

NBG5715

Simultaneous Dual-Band Wireless N Media Router

User's Guide



Default Login Details

| | |
|------------|---|
| IP Address | http://192.168.1.1 |
| Password | 1234 |

Firmware Version 1.0
Edition 1, 3/2011

www.zyxel.com

ZyXEL

Copyright © 2011
ZyXEL Communications Corporation

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the NBG5715 using the Web Configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

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 NBG5715 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.

Documentation Feedback

Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.



- **Download Library**
Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.
- **Knowledge Base**
If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.
- **Forum**
This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

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

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 NBG5715 may be referred to as the "NBG5715", 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 NBG5715 icon is not an exact representation of your device.

| | | |
|--|---|---|
| <p>NBG5715</p>  | <p>Computer</p>  | <p>Notebook computer</p>  |
| <p>Server</p>  | <p>DSLAM</p>  | <p>Firewall</p>  |
| <p>Telephone</p>  | <p>Switch</p>  | <p>Router</p>  |
| <p>Modem</p>  | | |

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.
- This product is for indoor use only (utilisation intérieure exclusivement).

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 | 19 |
| Introduction | 21 |
| The WPS Button | 25 |
| ZyXEL NetUSB Share Center Utility | 26 |
| Introducing the Web Configurator | 33 |
| Monitor and Summary | 37 |
| NBG5715 Modes | 43 |
| Easy Mode | 44 |
| Router Mode | 55 |
| Tutorials | 61 |
| Technical Reference | 69 |
| WAN | 71 |
| Wireless LAN | 79 |
| LAN | 95 |
| DHCP Server | 99 |
| NAT | 103 |
| Dynamic DNS | 113 |
| Static Route | 115 |
| Firewall | 119 |
| IPSec VPN | 124 |
| Bandwidth Management | 147 |
| Remote Management | 152 |
| Universal Plug-and-Play (UPnP) | 155 |
| Maintenance | 163 |
| Troubleshooting | 171 |

Table of Contents

| | |
|--|-----------|
| About This User's Guide | 3 |
| Document Conventions | 5 |
| Safety Warnings..... | 7 |
| Contents Overview | 9 |
| Table of Contents | 11 |
| | |
| Part I: User's Guide | 19 |
| | |
| Chapter 1 | |
| Introduction | 21 |
| 1.1 Overview | 21 |
| 1.2 Applications | 22 |
| 1.3 Ways to Manage the NBG5715 | 22 |
| 1.4 Good Habits for Managing the NBG5715 | 22 |
| 1.5 LEDs | 23 |
| | |
| Chapter 2 | |
| The WPS Button..... | 25 |
| 2.1 Overview | 25 |
| | |
| Chapter 3 | |
| ZyXEL NetUSB Share Center Utility | 26 |
| 3.1 Overview | 26 |
| 3.1.1 Quick Setup | 26 |
| 3.1.2 Installing ZyXEL NetUSB Share Center Utility | 26 |
| 3.2 The ZyXEL NetUSB Share Center Utility | 27 |
| 3.2.1 The Menus | 28 |
| 3.2.2 The Share Center Configuration Window | 29 |
| 3.2.3 The Auto-Connect Printer List Window | 29 |
| 3.3 Manually Connecting to USB Devices | 30 |
| 3.4 Automatically Connecting to a USB Printer | 31 |
| | |
| Chapter 4 | |
| Introducing the Web Configurator | 33 |
| 4.1 Overview | 33 |

| | |
|---|-----------|
| 4.2 Accessing the Web Configurator | 33 |
| 4.2.1 Login Screen | 33 |
| 4.2.2 Weather Edit | 34 |
| 4.2.3 Time/Date Edit | 35 |
| 4.3 Resetting the NBG5715 | 35 |
| 4.3.1 How to Use the RESET Button | 35 |
| Chapter 5 | |
| Monitor and Summary | 37 |
| 5.1 Overview | 37 |
| 5.2 What You Can Do in this Chapter | 37 |
| 5.3 The Log Screen | 38 |
| 5.3.1 View Log | 38 |
| 5.4 DHCP Table | 38 |
| 5.5 Packet Statistics | 40 |
| 5.6 VPN Monitor | 41 |
| 5.7 WLAN_2.4G/5G Station Status | 41 |
| Chapter 6 | |
| NBG5715 Modes | 43 |
| 6.1 Overview | 43 |
| 6.1.1 Web Configurator Modes | 43 |
| Chapter 7 | |
| Easy Mode | 44 |
| 7.1 Overview | 44 |
| 7.2 What You Can Do in this Chapter | 45 |
| 7.3 Navigation Panel | 45 |
| 7.4 Network Map | 46 |
| 7.5 Control Panel | 47 |
| 7.5.1 Game Engine | 48 |
| 7.5.2 Power Saving | 48 |
| 7.5.3 Content Filter | 49 |
| 7.5.4 Bandwidth MGMT | 50 |
| 7.5.5 Firewall | 51 |
| 7.5.6 Wireless Security | 51 |
| 7.5.7 WPS | 52 |
| 7.6 Status Screen in Easy Mode | 53 |
| Chapter 8 | |
| Router Mode | 55 |
| 8.1 Overview | 55 |
| 8.2 Router Mode Status Screen | 56 |

| | |
|---|-----------|
| 8.2.1 Navigation Panel | 58 |
| Chapter 9 | |
| Tutorials | 61 |
| 9.1 Overview | 61 |
| 9.2 Set Up a Wireless Network with WPS | 61 |
| 9.2.1 Push Button Configuration (PBC) | 61 |
| 9.2.2 PIN Configuration | 63 |
| 9.3 Configure Wireless Security without WPS | 64 |
| 9.3.1 Configure Your Notebook | 65 |
| | |
| Part II: Technical Reference | 69 |
| | |
| Chapter 10 | |
| WAN | 71 |
| 10.1 Overview | 71 |
| 10.2 What You Can Do in this Chapter | 71 |
| 10.3 What You Need To Know | 71 |
| 10.3.1 Configuring Your Internet Connection | 72 |
| 10.3.2 Multicast | 73 |
| 10.4 The Broadband Screen | 73 |
| 10.4.1 Ethernet Encapsulation | 73 |
| 10.4.2 PPPoE Encapsulation | 75 |
| 10.5 The Advanced Screen | 77 |
| | |
| Chapter 11 | |
| Wireless LAN | 79 |
| 11.1 Overview | 79 |
| 11.1.1 What You Can Do in this Chapter | 79 |
| 11.1.2 What You Should Know | 80 |
| 11.2 The General Wireless LAN Screen | 82 |
| 11.3 Wireless Security Modes | 84 |
| 11.3.1 No Security | 84 |
| 11.3.2 WEP Encryption | 85 |
| 11.3.3 WPA-PSK/WPA2-PSK | 86 |
| 11.3.4 WPA/WPA2 | 87 |
| 11.4 The MAC Filter Screen | 88 |
| 11.5 The Wireless LAN Advanced Screen | 90 |
| 11.6 The QoS Screen | 90 |
| 11.7 The WPS Screen | 91 |
| 11.8 The WPS Station Screen | 92 |

| | |
|--|------------|
| 11.9 The Scheduling Screen | 93 |
| Chapter 12 | |
| LAN | 95 |
| 12.1 Overview | 95 |
| 12.2 What You Can Do in this Chapter | 95 |
| 12.3 What You Need To Know | 96 |
| 12.3.1 IP Pool Setup | 96 |
| 12.3.2 LAN TCP/IP | 96 |
| 12.4 The LAN IP Screen | 97 |
| 12.5 The IP Alias Screen | 97 |
| Chapter 13 | |
| DHCP Server | 99 |
| 13.1 Overview | 99 |
| 13.1.1 What You Can Do in this Chapter | 99 |
| 13.1.2 What You Need To Know | 99 |
| 13.2 The DHCP Server General Screen | 99 |
| 13.3 The DHCP Server Advanced Screen | 100 |
| 13.4 The Client List Screen | 101 |
| Chapter 14 | |
| NAT | 103 |
| 14.1 Overview | 103 |
| 14.1.1 What You Can Do in this Chapter | 103 |
| 14.1.2 What You Need To Know | 104 |
| 14.2 The NAT General Screen | 105 |
| 14.3 The Port Forwarding Screen | 106 |
| 14.3.1 Port Forwarding Edit Screen | 108 |
| 14.4 The NAT Advance Screen | 109 |
| 14.5 Technical Reference | 110 |
| 14.5.1 NATPort Forwarding: Services and Port Numbers | 110 |
| 14.5.2 NAT Port Forwarding Example | 110 |
| 14.5.3 Trigger Port Forwarding | 110 |
| 14.5.4 Trigger Port Forwarding Example | 111 |
| 14.5.5 Two Points To Remember About Trigger Ports | 111 |
| Chapter 15 | |
| Dynamic DNS | 113 |
| 15.1 Overview | 113 |
| 15.1.1 What You Need To Know | 113 |
| 15.2 The Dynamic DNS Screen | 114 |

| | |
|--|------------|
| Chapter 16 | |
| Static Route | 115 |
| 16.1 Overview | 115 |
| 16.2 The Static Route Screen | 115 |
| 16.2.1 Add/Edit Static Route | 116 |
| Chapter 17 | |
| Firewall | 119 |
| 17.1 Overview | 119 |
| 17.1.1 What You Can Do in this Chapter | 119 |
| 17.1.2 What You Need To Know | 119 |
| 17.2 The Firewall General Screen | 121 |
| 17.3 The Firewall Services Screen | 121 |
| Chapter 18 | |
| IPSec VPN | 124 |
| 18.1 Overview | 124 |
| 18.2 What You Can Do in this Chapter | 124 |
| 18.3 What You Need To Know | 125 |
| 18.3.1 IKE SA (IKE Phase 1) Overview | 125 |
| 18.3.2 IPSec SA (IKE Phase 2) Overview | 126 |
| 18.4 The General Screen | 126 |
| 18.5 Edit VPN Rule | 128 |
| 18.5.1 IKEKey Setup | 129 |
| 18.5.2 Manual Key Setup | 134 |
| 18.5.3 Configuring Manual Key | 136 |
| 18.6 The SA Monitor Screen | 139 |
| 18.7 Technical Reference | 139 |
| 18.7.1 IPSec Architecture | 140 |
| 18.7.2 Encapsulation | 141 |
| 18.7.3 IKE Phases | 142 |
| 18.7.4 Negotiation Mode | 142 |
| 18.7.5 IPSec and NAT | 143 |
| 18.7.6 VPN, NAT, and NAT Traversal | 143 |
| 18.7.7 ID Type and Content | 144 |
| 18.7.8 Pre-Shared Key | 145 |
| 18.7.9 Diffie-Hellman (DH) Key Groups | 146 |
| Chapter 19 | |
| Bandwidth Management | 147 |
| 19.1 Overview | 147 |
| 19.2 What You Can Do this Chapter | 147 |
| 19.3 What You Need To Know | 147 |

| | |
|--|------------|
| 19.4 General Screen | 148 |
| 19.5 Advance Screen | 148 |
| 19.5.1 Rule Configuration: User Defined Service Rule Configuration | 151 |
| Chapter 20 | |
| Remote Management..... | 152 |
| 20.1 Overview | 152 |
| 20.2 What You Can Do in this Chapter | 152 |
| 20.3 What You Need to Know | 152 |
| 20.3.1 Remote Management and NAT | 152 |
| 20.3.2 System Timeout | 153 |
| 20.4 WWW Screen | 153 |
| 20.5 Telnet Screen | 154 |
| Chapter 21 | |
| Universal Plug-and-Play (UPnP)..... | 155 |
| 21.1 Overview | 155 |
| 21.2 What You Need to Know | 155 |
| 21.2.1 NAT Traversal | 155 |
| 21.2.2 Cautions with UPnP | 155 |
| 21.3 UPnP Screen | 156 |
| 21.4 Technical Reference | 156 |
| 21.4.1 Using UPnP in Windows XP Example | 156 |
| 21.4.2 Web Configurator Easy Access | 159 |
| Chapter 22 | |
| Maintenance | 163 |
| 22.1 Overview | 163 |
| 22.2 What You Can Do in this Chapter | 163 |
| 22.3 General Screen | 163 |
| 22.4 Password Screen | 164 |
| 22.5 Time Setting Screen | 165 |
| 22.6 Firmware Upgrade Screen | 166 |
| 22.7 Backup/Restore Screen | 167 |
| 22.8 The Language Screen | 169 |
| Chapter 23 | |
| Troubleshooting..... | 171 |
| 23.1 Overview | 171 |
| 23.2 Power, Hardware Connections, and LEDs | 171 |
| 23.3 NBG5715 Access and Login | 172 |
| 23.4 Internet Access | 174 |
| 23.5 Resetting the NBG5715 to Its Factory Defaults | 175 |

| | |
|--|------------|
| 23.6 Wireless Router Troubleshooting | 175 |
| 23.7 USB Device Problems | 176 |
| 23.8 ZyXEL NetUSB Share Center Utility Problems | 177 |
| Appendix A Product Specifications | 179 |
| 23.9 Wall-mounting Instructions | 181 |
| Appendix B Pop-up Windows, JavaScript and Java Permissions | 183 |
| Appendix C IP Addresses and Subnetting..... | 195 |
| Appendix D Setting Up Your Computer's IP Address | 205 |
| Appendix E Wireless LANs..... | 233 |
| Appendix F Common Services | 247 |
| Appendix G Open Software Announcements | 251 |
| Appendix H Legal Information | 281 |
| Index | 287 |

PART I

User's Guide

Introduction

1.1 Overview

This chapter introduces the main features and applications of the NBG5715.

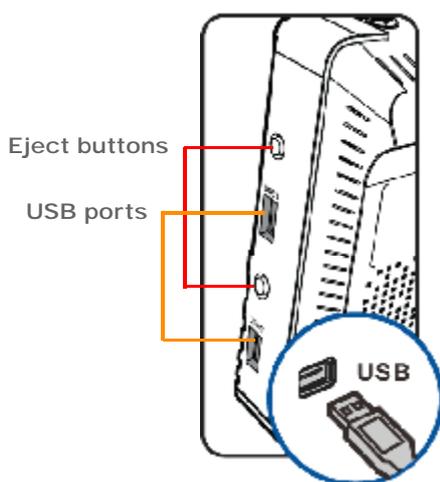
The NBG5715 extends the range of your existing wired network without additional wiring, providing easy network access to mobile users. You can set up a wireless network with other IEEE 802.11a/b/g/n compatible devices. The NBG5715 is able to function both 2.4G and 5G network at the same time.

A range of services such as a firewall and content filtering are also available for secure Internet computing. You can use media bandwidth management to efficiently manage traffic on your network. Bandwidth management features allow you to prioritize time-sensitive or highly important applications such as Voice over the Internet (VoIP).

There are two USB 2.0 ports on the side panel of your NBG5715. You can connect USB (version 2.0 or lower) memory sticks, USB hard drives, or USB devices for file sharing. The NBG5715 automatically detects the USB devices.

Two USB eject buttons are located above the USB ports. Push the eject button of the corresponding USB port for 2 seconds. Make sure the USB LED is off before removing your USB device. This will remove your USB device safely, preventing file or data loss if it is being transmitted through the USB device.

Figure 1 USB Ports and Eject Buttons



Note: For the USB function, it is strongly recommended to use version 2.0 or lower USB storage devices (such as memory sticks, USB hard drives) and/or USB devices (such as USB printers). Other USB products are not guaranteed to function properly with the NBG5715.

Note: Be sure to install the ZyXEL NetUSB™ Share Center Utility (for NetUSB functionality) from the included disc, or download the latest version from the zyxel.com website. See [Chapter 3 on page 26](#) for more information.

1.2 Applications

You can create the following networks using the NBG5715:

- **Wired.** You can connect network devices via the Ethernet ports of the NBG5715 so that they can communicate with each other and access the Internet.
- **Wireless.** Wireless clients can connect to the NBG5715 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.
- **NetUSB.** The NBG5715 allows you to connect a USB device (such as printer, scanner, or portable hard disk) directly to the USB port and then share that device over the Internet. You can also connect a USB to the NBG5715, which can then share up to 3 additional USB devices with the rest of your personal home network.

1.3 Ways to Manage the NBG5715

Use any of the following methods to manage the NBG5715.

- **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 NBG5715.
- **Web Configurator.** This is recommended for everyday management of the NBG5715 using a (supported) web browser.

1.4 Good Habits for Managing the NBG5715

Do the following things regularly to make the NBG5715 more secure and to manage the NBG5715 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 NBG5715 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG5715. You could simply restore your last configuration.

1.5 LEDs

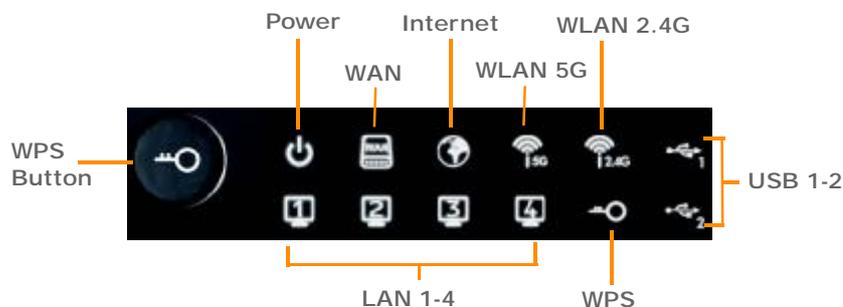
Look at the LED lights on the front panel to determine the status of the NBG5715. Use the LED button at the side panel of the device to turn the LED lights on or off. If you have already pushed the LED button to the ON position but none of the LEDs are on, make sure the NBG5715 is receiving power and the power is turned on.

Note: The **Power LED** will be on even if you push the LED button to the **OFF** position. This is for you to determine whether the NBG5715 is powered on.

Figure 2 LED Button



Figure 3 Front Panel



The following table describes the LEDs and the WPS button.

Table 1 Front panel LEDs and WPS button

| LED | STATUS | DESCRIPTION |
|-------------|----------|--|
| WPS Button | | Press this button for 1 second to set up a wireless connection via WiFi Protected Setup with another WPS-enabled client. You must press the WPS button on the client side within 120 seconds for a successful connection. See Chapter 2 on page 25 and Chapter 9 on page 61 for more information on WPS. |
| Power | On | The NBG5715 is receiving power and functioning properly. |
| | Off | The NBG5715 is not receiving power. |
| WAN | On | The NBG5715's WAN connection is ready. |
| | Blinking | The NBG5715 is sending/receiving data through the WAN with a 1000Mbps transmission rate. |
| | Off | The WAN connection is not ready, or has failed. |
| Internet | On | The NBG5715 has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the connection is up. |
| | Blinking | The NBG5715 is sending or receiving IP traffic. |
| | Off | The NBG5715 does not have an IP connection. |
| WLAN 2.4/5G | On | The NBG5715 is ready, but is not sending/receiving data through the 5G wireless LAN. |
| | Blinking | The NBG5715 is sending/receiving data through the 5G wireless LAN. The NBG5715 is negotiating a WPS connection with a wireless client. |
| | Off | The wireless LAN is not ready or has failed. |
| LAN 1-4 | On | The NBG5715's LAN connection is ready. |
| | Blinking | The NBG5715 is sending/receiving data through the LAN with a 1000Mbps transmission rate. |
| | Off | The LAN connection is not ready, or has failed. |
| USB 1-2 | On | The NBG5715 has a USB device installed. |
| | Blinking | The NBG5715 is transmitting and/or receiving data from routers through an installed USB device. |
| | Off | There is no USB device connected to the NBG5715. |

The WPS Button

2.1 Overview

Your NBG5715 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 [Chapter 9 on page 61](#).

Figure 4 The WPS Button



ZyXEL NetUSB Share Center Utility

3.1 Overview

The ZyXEL NetUSB Share Center Utility allows you to work with the USB devices that are connected directly to the NBG5715 as if they are connected directly to your computer. This allows you to easily share USB-based devices such as printers, scanners, portable hard disks, MP3 players, faxes, and digital cameras (to name a few) with all the other people in your home or office as long as they are connected to the NBG5715 and have the ZyXEL NetUSB Share Center Utility installed.

Note: Be sure to install the ZyXEL NetUSB Share Center Utility (for NetUSB functionality) from the included disc, or download the latest version from the zyxel.com website's Download Library.

3.1.1 Quick Setup

This section shows you how to get started using the ZyXEL NetUSB Share Center Utility.

- 1 Install the ZyXEL NetUSB Share Center Utility on each computer connected to the NBG5715.
- 2 Connect a USB device to the USB port on the NBG5715.

Note: If you are connecting multiple devices to the NBG5715, first connect a USB hub to the NBG5715 then connect your other USB devices to it.

- 3 Run the ZyXEL NetUSB Share Center Utility to display a list of all connected USB devices, then use it to connect your computer to them.

3.1.2 Installing ZyXEL NetUSB Share Center Utility

Before you can access USB devices connected to the NBG5715, you must first install the ZyXEL NetUSB Share Center Utility on any computer on your LAN to which you want to allow access to these devices.

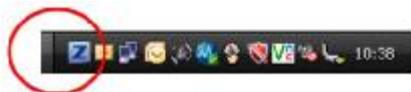
Note: In order to properly use the utility with your NBG5715, ensure that the NBG5715 firmware is version v1.00(BWQ.0) or higher. See [Chapter 22 on page 166](#) for information on updating your device's firmware.

To install the ZyXEL NetUSB Share Center Utility:

- 1 Insert the disc that came with your NBG5715 into your computer's disc drive.
- 2 Run the **Setup** program by double-clicking it and then follow the on-screen instructions for installing it on your computer.

Note: The following operating systems are supported: Windows XP/Vista/7 (32 and 64-bit versions).

- To open the ZyXEL NetUSB Share Center Utility, double-click its system tray icon.



3.2 The ZyXEL NetUSB Share Center Utility

This section describes the ZyXEL NetUSB Share Center Utility main window.

Figure 5 ZyXEL NetUSB Share Center Utility Main Window



The following table describes the icons in this window.

Table 2 ZyXEL NetUSB Share Center Utility Main Window Icons

| ICON | DESCRIPTION |
|---|--|
|  | <p>Configure Server</p> <p>Click to open the NBG5715's built-in Web Configurator, which you can use to set up the NBG5715 (see Chapter 4 on page 33 for details).</p> |
|  | <p>Auto-Connect Printer</p> <p>Click this if you want to automatically connect to the printer each time you start your computer.</p> <p>Note: You must first install the appropriate print driver on each computer for which you intend to use this feature. See the documentation that came with your printer for instructions on how to do this.</p> |
|  | <p>Connect</p> <p>Select a USB device and then click this button to connect to it. Your computer can connect to as many USB devices as are connected to the NBG5715.</p> |
|  | <p>Disconnect</p> <p>Select a device to which your computer is connected and then click this button to disconnect from it.</p> |

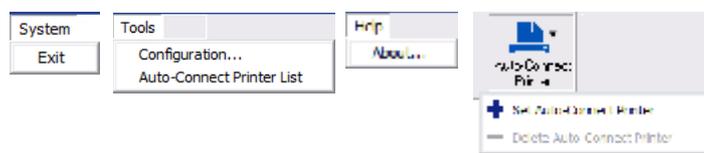
Table 2 ZyXEL NetUSB Share Center Utility Main Window Icons (continued)

| ICON | DESCRIPTION |
|---|--|
|  | Request to Connect Some USB devices may not allow automatic connections over the network. If so, select the device in question and click this button to issue a request to connect to it. |
|  | Network Scanner Click this to open the scanner options on your computer for working with a scanner connected to the network. |

3.2.1 The Menus

This section describes the utility’s menus.

Figure 6 ZyXEL NetUSB Share Center Utility Menus



The following table describes the menus in this screen.

Table 3 ZyXEL NetUSB Share Center Utility Main Screen Menus

| MENU | ITEM | DESCRIPTION |
|----------------------|-----------------------------|--|
| System | Exit | This closes the ZyXEL NetUSB Share Center Utility. |
| Tools | Configuration | This opens the ZyXEL NetUSB Share Center Utility configuration window. |
| | Auto-Connect Printer List | This opens the list window that displays all of the printing devices connected to the NBG5715. |
| Help | About | This opens the about window, which provides information of the utility software and driver versions. |
| Auto-Connect Printer | Set Auto-Connect Printer | This sets the selected printer to 'auto-connect', meaning your computer will always connect to the printer over the network. Note: You first must install the appropriate drivers for the printer that you intend to use. |
| | Delete Auto-Connect Printer | This removes the auto-connect option from the selected printer. |

3.2.2 The Share Center Configuration Window

This section describes the utility's configuration window, which allows you to set certain options for the utility. These options do not apply to the USB devices connected to the NBG5715.

You can open it by clicking the **Tools > Configuration** menu command.

Figure 7 ZyXEL NetUSB Share Center Utility Configuration Window



The following table describes the labels in this window.

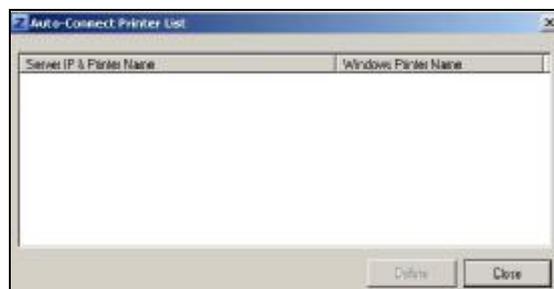
Table 4 ZyXEL NetUSB Share Center Utility Configuration Window

| LABEL | DESCRIPTION |
|----------|--|
| Basic | Select this to run the utility automatically when you log into or start up Windows. |
| Language | Select a language for the ZyXEL NetUSB Share Center Utility. You must restart the utility for the change to take effect. |
| OK | Click this to save your changes and close the window. |
| Cancel | Click this cancel to close the window without saving. |
| Apply | Click this to save your changes without closing the window. |

3.2.3 The Auto-Connect Printer List Window

This section describes the utility's auto-connect printer list window. You can open it by clicking the **Tools > Auto-Connect Printer List** menu command.

Figure 8 ZyXEL NetUSB Share Center Utility Auto-Connect Printer List Window



The following table describes the labels in this screen.

Table 5 ZyXEL NetUSB Share Center Utility Auto-Connect Printer List Window

| LABEL | DESCRIPTION |
|--------------------------|--|
| Server IP & Printer Name | Displays a list of print server IPs and printer names connected to this NBG5715. |
| Windows Printer Name | Displays a corresponding list of Windows printer names connected to this devices listed in the other list. |
| Delete | Select an printer from the list and click this to remove it. |
| Close | Click this to close the window. |

3.3 Manually Connecting to USB Devices

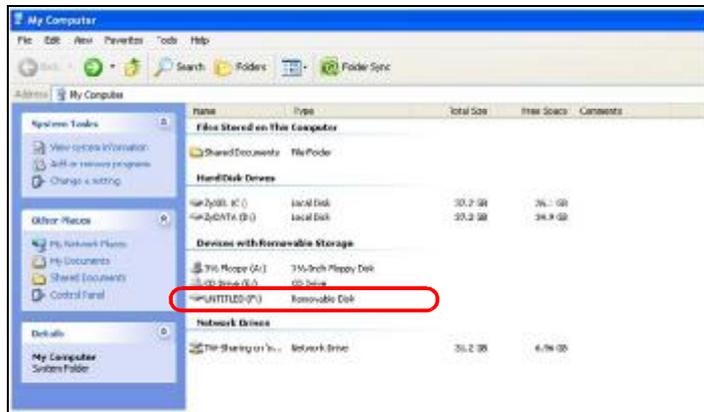
This example shows you how to connect to a USB device over your NBG5715 network. Makes sure that you have first installed the ZyXEL NetUSB Share Center Utility on the computer to which you want to connect the USB devices.

Note: If you do this with a USB printer but do not yet have the print driver installed you will be prompted to install one by the Windows New Hardware Wizard.

- 1 Connect a USB device to the NBG5715.
- 2 In the ZyXEL NetUSB Share Center Utility, select the device and click **Connect**.



- 3 The device mounts on your system.



3.4 Automatically Connecting to a USB Printer

This example shows you how to set your computer to automatically connect to a shared USB printer over your NBG5715 network each time you log into your computer. Makes sure that you have first installed the ZyXEL NetUSB Share Center Utility.

- 1 Connect a USB printer to the NBG5715.
- 2 Open the ZyXEL NetUSB Sharing Center Utility on the computer that you want to use to connect to the printer.



Click the **Connect** button. You may be prompted to install a printer driver or to configure other settings.

- 3 Finally, click the **Auto-Connect Printer** menu and select **Set Auto-Connect Printer** from the menu.

Introducing the Web Configurator

4.1 Overview

This chapter describes how to access the NBG5715 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 NBG5715 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 23 on page 171](#)) to see how to make sure these functions are allowed in Internet Explorer.

4.2 Accessing the Web Configurator

- 1 Make sure your NBG5715 hardware is properly connected and prepare your computer or computer network to connect to the NBG5715 (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "<http://192.168.1.1>" as the website address.

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

4.2.1 Login Screen

Note: If this is the first time you are accessing the Web Configurator, you may be redirected to the Wizard. Refer to [Chapter 4 on page 33](#) for the Connection Wizard screens.

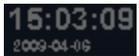
The Web Configurator initially displays the following login screen.

Figure 9 Login screen



The following table describes the labels in this screen.

Table 6 Login screen

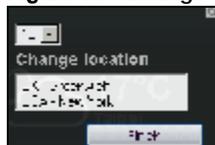
| LABEL | DESCRIPTION |
|---|--|
| Language | Select the language you want to use to configure the Web Configurator. Click Login . |
| Password | Type "1234" (default) as the password. |
|  | This shows the current weather, either in celsius or fahrenheit, of the city you specify in Section 4.2.2 on page 34 . |
|  | This shows the time (hh:mm:ss) and date (yyyy:mm:dd) of the timezone you select in Section 4.2.3 on page 35 or Section 22.5 on page 165 . The time is in 24-hour format, for example 15:00 is 3:00 PM. |

4.2.2 Weather Edit

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

Click the  icon to change the Weather display.

Figure 10 Change Weather



The following table describes the labels in this screen.

Table 7 Change Weather

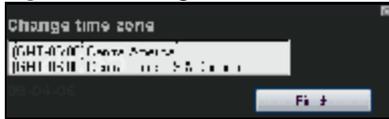
| LABEL | DESCRIPTION |
|-----------------|---|
| °C or °F | Choose which temperature unit you want the NBG5715 to display. |
| Change Location | Select the location for which you want to know the weather. If the city you want is not listed, choose one that is closest to it. |
| Finish | Click this to apply the settings and refresh the date and time display. |

4.2.3 Time/Date Edit

One timezone can cover more than one country. You can choose a particular country in which the NBG5715 is located and have the NBG5715 display and use the current time and date for its logs.

Click the  icon to change the Weather display.

Figure 11 Change Password Screen



The following table describes the labels in this screen.

Table 8 Change Password Screen

| LABEL | DESCRIPTION |
|------------------|--|
| Change time zone | Select the specific country whose current time and date you want the NBG5715 to display. |
| Finish | Click this to apply the settings and refresh the weather display. |

Note: You can also edit the timezone in [Section 22.5 on page 165](#).

4.3 Resetting the NBG5715

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 NBG5715 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".

4.3.1 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 NBG5715.
- 3 Press the **RESET** button for longer than 5 seconds to set the NBG5715 back to its factory-default configurations.

Monitor and Summary

5.1 Overview

This chapter discusses read-only information related to the device state of the NBG5715.

To access the **Monitor** screens, go to **Expert Mode** after login, then click .



You can also click the **Details** 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 NBG5715.

| Summary | |
|--------------------------|------------------------------|
| Packet Statistics | (Details...) |
| WLAN_2.4G Station Status | (Details...) |
| WLAN_5G Station Status | (Details...) |
| IPSec VPN Status | (Details...) |

5.2 What You Can Do in this Chapter

- Use the **Log** screens to see the logs for the activity on the NBG5715 ([Section 5.3 on page 38](#)).
- Use the **DHCP Table** screen to view information related to your DHCP status ([Section 5.4 on page 38](#)).
- use the **Packet Statistics** screen to view port status, packet specific statistics, the "system up time" and so on ([Section 5.5 on page 40](#)).
- Use the **VPN Monitor** screen to view the active VPN connections ([Section 5.6 on page 41](#)).
- Use the **WLAN_2.4G/5G Station Status** screen to view the 2.4G wireless stations that are currently associated to the NBG5715 ([Section 5.7 on page 41](#)).

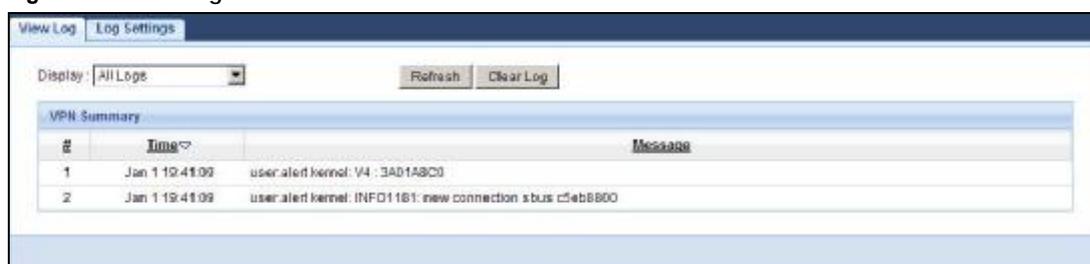
5.3 The Log Screen

The Web Configurator allows you to look at all of the NBG5715's logs in one location.

5.3.1 View Log

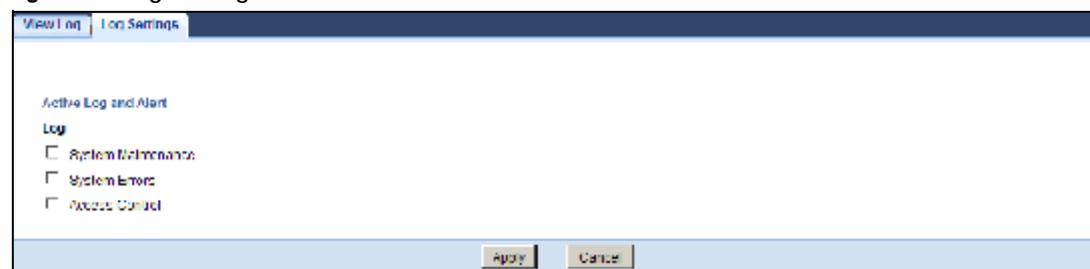
Use the **View Log** screen to see the logged messages for the NBG5715. The log wraps around and deletes the old entries after it fills. Select what logs you want to see from the **Display** drop list. The log choices depend on your settings in the **Log Settings** screen. Click **Refresh** to renew the log screen. Click **Clear** to delete all the logs.

Figure 12 View Log



You can configure which logs to display in the **View Log** screen. Go to the **Log Settings** screen and select the logs you wish to display. Click **Apply** to save your settings. Click **Refresh** to start the screen afresh.

Figure 13 Log Settings



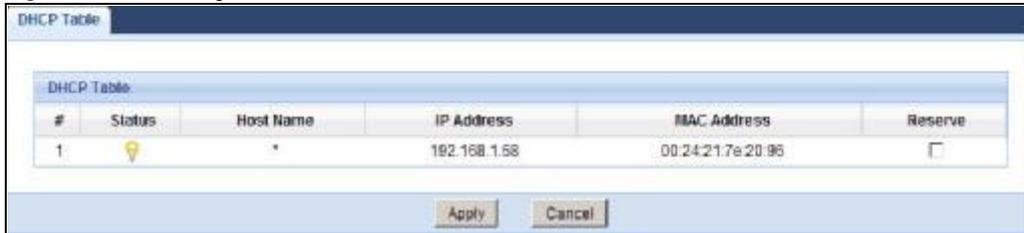
5.4 DHCP Table

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 NBG5715's LAN as a DHCP server or disable it. When configured as a server, the NBG5715 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 **Monitor > DHCP Table** or the **DHCP Table (Details...)** hyperlink in the **Status** screen. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client

information (including MAC Address, IP Address, and Expiration time) of all network clients using the NBG5715's DHCP server.

Figure 14 Summary: DHCP Table



The screenshot shows a window titled "DHCP Table" containing a table with the following data:

| # | Status | Host Name | IP Address | MAC Address | Reserve |
|---|---|-----------|--------------|-------------------|--------------------------|
| 1 |  | * | 192.168.1.58 | 00:24:21:7e:20:96 | <input type="checkbox"/> |

At the bottom of the window are "Apply" and "Cancel" buttons.

The following table describes the labels in this screen.

Table 9 Summary: DHCP Table

| LABEL | DESCRIPTION |
|-------------|---|
| # | This is the index number of the host computer. |
| Status | This field displays whether the connection to the host computer is up (a yellow bulb) or down (a gray bulb). |
| Host Name | This field displays the computer host name. |
| IP Address | This field displays the IP address relative to the # field listed above. |
| 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. |
| Reserve | Select this if you want to reserve the IP address for this specific MAC address. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Reset | Click Cancel to reload the previous configuration for this screen. |

5.5 Packet Statistics

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

Figure 15 Summary: Packet Statistics



The following table describes the labels in this screen.

Table 10 Summary: Packet Statistics

| LABEL | DESCRIPTION |
|------------------|---|
| Port | This is the NBG5715's port type. |
| Status | For the LAN ports, this displays the port speed and duplex setting or Down when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and Idle (line (ppp) idle), Dial (starting to trigger a call) and Drop (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays Down when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and Down when the WLAN is disabled. |
| TxPkts | This is the number of transmitted packets on this port. |
| RxPkts | This is the number of received packets on this port. |
| Collisions | This is the number of collisions on this port. |
| Tx B/s | This displays the transmission speed in bytes per second on this port. |
| Rx B/s | This displays the reception speed in bytes per second on this port. |
| Up Time | This is the total time the NBG5715 has been for each session. |
| System Up Time | This is the total time the NBG5715 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. |

5.6 VPN Monitor

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

Figure 16 Summary: Security Associations



The following table describes the labels in this screen.

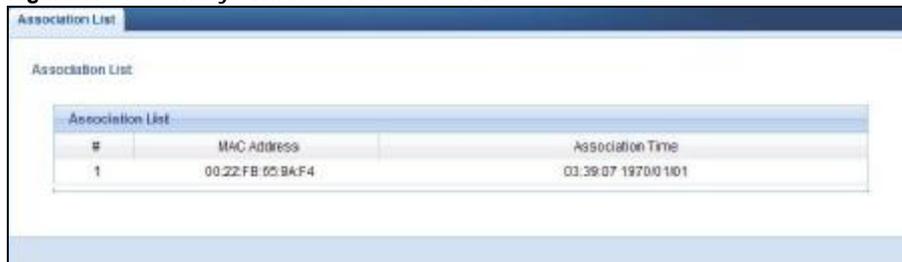
Table 11 Summary: Security Associations

| LABEL | DESCRIPTION |
|-----------------|---|
| Status | This field displays whether the VPN connection is up (a yellow bulb) or down (a gray bulb). |
| Connection Name | This field displays the identification name for this VPN policy. |
| Remote Gateway | This is the static WAN IP address or URL of the remote IPsec router. |
| Local Address | This is the IP address of computer(s) on your local network behind your NBG5715. |
| Remote Address | This is the IP address of computer(s) on the remote network behind the remote IPsec router. |
| Refresh | Click this button to update the screen's statistics immediately. |

5.7 WLAN_2.4G/5G Station Status

Click **Monitor > WLAN_2.4G/5G Station Status** or the **WLAN 2.4G/5G WLAN Station Status (Details...)** hyperlink in the **Status** screen. View the wireless stations that are currently associated to the NBG5715 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 17 Summary: Wireless Association List



The following table describes the labels in this screen.

Table 12 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 NBG5715's WLAN network. |

NBG5715 Modes

6.1 Overview

This chapter introduces the different modes available on your NBG5715. First, the term “mode” refers to two things in this User’s Guide.

- **Web Configurator mode.** This refers to the Web Configurator interface you want to use for editing NBG5715 features.
- **Router mode:** This is the device mode of the NBG5715. Use this mode to connect the local network to another network, like the Internet. Go to [Section 8.2 on page 56](#) to view the Status screen in this mode.

6.1.1 Web Configurator Modes

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

- **Easy:** The Web Configurator shows this mode by default. Refer to [Chapter 7 on page 44](#) for more information on the screens in this mode. This interface may be sufficient for users who just want to use the device.
- **Expert:** Advanced users can change to this mode to customize all the functions of the NBG5715. Click **Expert Mode** after logging into the Web Configurator. The User’s Guide [Chapter 4 on page 33](#) discusses the screens in this mode.

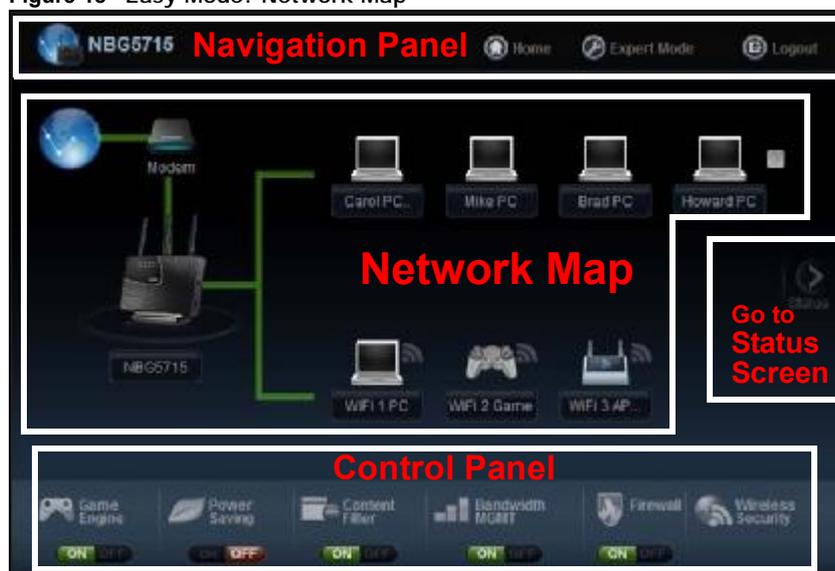
Easy Mode

7.1 Overview

The Web Configurator is set to **Easy Mode** by default. You can configure several key features of the NBG5715 in this mode. This mode is useful to users who are not fully familiar with some features that are usually intended for network administrators.

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

Figure 18 Easy Mode: Network Map



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

Figure 19 Easy Mode: Status Screen



7.2 What You Can Do in this Chapter

You can do the following in this mode:

- Use this Navigation Panel to opt out of the Easy mode ([Section 7.3 on page 45](#)).
- Use the Network Map screen to check if your NBG5715 can ping the gateway and whether it is connected to the Internet ([Section 7.4 on page 46](#)).
- Use the Control Panel to configure and enable NBG5715 features, including wireless security, wireless scheduling and bandwidth management and so on ([Section 7.5 on page 47](#)).
- Use the Status Screen to view read-only information about the NBG5715, including the WAN IP, MAC Address of the NBG5715 and the firmware version ([Section 7.6 on page 53](#)).

7.3 Navigation Panel

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

Figure 20 Control Panel



The following table describes the labels in this screen.

Table 13 Control Panel

| ITEM | DESCRIPTION |
|-------------|--|
| Home | Click this to go to the Login page. |
| Expert Mode | Click this to change to Expert mode and customize features of the NBG5715. |
| Logout | Click this to end the Web Configurator session. |

7.4 Network Map

Note: The Network MAP is viewable by Windows XP (need to install patch), Windows Vista and Windows 7 users only. For Windows XP (Service Pack 2) users, you can see the network devices connected to the NBG5715 by downloading the LLTD (Link Layer Topology Discovery) patch from the Microsoft Website.

Note: Don't worry if the Network Map does not display in your web browser. This feature may not be supported by your system. You can still configure the Control Panel (Section 7.5 on page 47) in the Easy Mode and the NBG5715 features that you want to use in the Expert Mode.

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

Figure 21 Network Map



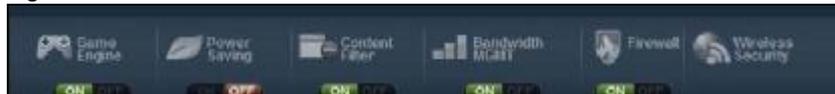
The line connecting the NBG5715 to the gateway becomes green when the NBG5715 is able to ping the gateway. It becomes red when the ping initiating from the NBG5715 does not get a response from the gateway. The same rule applies to the line connecting the gateway to the Internet.

You can also view the devices (represented by icons indicating the kind of network device) connected to the NBG5715, including those connecting wirelessly. Right-click on the NBG5715 icon to refresh the network map and go to the Wizard. Right click on the other icons to view information about the device.

7.5 Control Panel

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

Figure 22 Control Panel



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

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

The following table describes the labels in this screen.

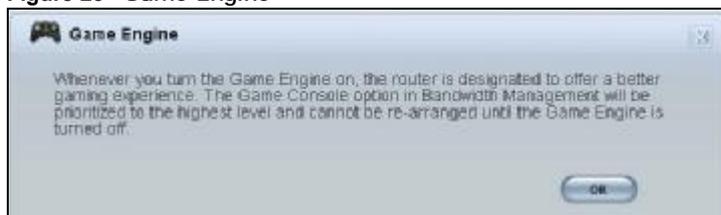
Table 14 Control Panel

| ITEM | DESCRIPTION |
|-------------------|---|
| Game Engine | Switch ON to maximize bandwidth for gaming traffic in your network. Otherwise, switch OFF . Refer to Section 7.5.1 on page 48 to see this screen. |
| Power Saving | Click this to schedule the wireless feature of the NBG5715. Disabling the wireless function helps lower the energy consumption of the NBG5715. Switch ON to apply wireless scheduling. Otherwise, switch OFF . Refer to Section 7.5.2 on page 48 to see this screen. |
| Content Filter | Click this to restrict access to certain websites, based on keywords contained in URLs, to which you do not want users in your network to open. Switch ON to apply website filtering. Otherwise, switch OFF . Refer to Section 7.5.3 on page 49 to see this screen. |
| Bandwidth MGMT | Click this to edit bandwidth management for predefined applications. Switch ON to have the NBG5715 management bandwidth for uplink and downlink traffic according to an application or service. Otherwise, switch OFF . Refer to Section 7.5.4 on page 50 to see this screen. |
| Firewall | Switch ON to ensure that your network is protected from Denial of Service (DoS) attacks. Otherwise, switch OFF . Refer to Section 7.5.5 on page 51 to see this screen. |
| Wireless Security | Click this to configure the wireless security, such as SSID, security mode and WPS key on your NBG5715. Refer to Section 7.5.6 on page 51 to see this screen. |

7.5.1 Game Engine

When this feature is enabled, the NBG5715 maximizes the bandwidth for gaming traffic that it forwards out through an interface.

Figure 23 Game Engine



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

Turn this off if your network is not using gaming.

Click OK to close this screen.

7.5.2 Power Saving

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

Disabling the wireless capability lowers the energy consumption of the of the NBG5715.

Figure 24 Power Saving



The following table describes the labels in this screen.

Table 15 Power Saving

| LABEL | DESCRIPTION |
|---|---|
| Wireless Radio | Choose whether you want to apply the power saving schedule to 2.4G hz or 5G hz wireless radio. |
| WLAN Status | Select On or Off to specify whether the Wireless LAN is turned on or off (depending on what you selected in the WLAN Status field). 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. |
| Except for the following times (24-Hour Format) | Select a begin time using the first set of hour and minute (min) drop down boxes and select an end time using the second set of hour and minute (min) drop down boxes. If you have chosen On earlier for the WLAN Status the Wireless LAN will turn 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. In this time format, midnight is 00:00 and progresses up to 24:00. For example, 6:00 PM is 18:00. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Reset | Click Reset to begin configuring this screen afresh. |

7.5.3 Content Filter

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

Figure 25 Content Filter



The following table describes the labels in this screen.

Table 16 Content Filter

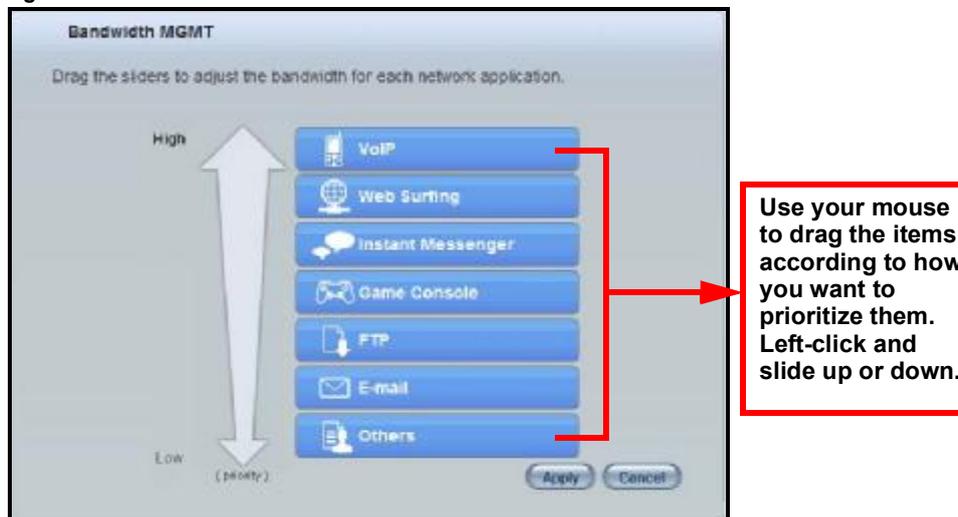
| LABEL | DESCRIPTION |
|--------|--|
| Add | Click Add after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. Note: The NBG5715 does not recognize wildcard characters as keywords. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request. |
| Delete | Highlight a keyword in the text box and click Delete to remove it. The keyword disappears from the text box after you click Apply . |
| Apply | Click Apply to save your changes. |
| Cancel | Click Cancel to close this screen without saving any changes. |

7.5.4 Bandwidth MGMT

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

The NBG5715 uses bandwidth management for incoming and outgoing traffic. Rank the services and applications by dragging them accordingly from **High** to **Low** and click **Apply**. Click **Cancel** to close the screen.

Figure 26 Bandwidth MGMT



7.5.5 Firewall

Enable this feature to protect the network from Denial of Service (DoS) attacks. The NBG5715 blocks repetitive pings from the WAN that can otherwise cause systems to slow down or hang.

Figure 27 Firewall



Click OK to close this screen.

7.5.6 Wireless Security

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

Note: You can enable the Wireless function of your NBG5715 by first turning on the switch in the side panel.

Figure 28 Wireless Security



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

Table 17 Wireless Security

| LABEL | DESCRIPTION |
|------------------------------|---|
| Wireless Radio | Choose whether you want to apply the wireless security to 2.4G hz or 5G hz wireless radio. |
| Wireless Network Name (SSID) | (Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 keyboard characters) for the wireless LAN. |

Table 17 Wireless Security (continued)

| LABEL | DESCRIPTION |
|-------------------|--|
| Security mode | Select WPA-PSK or WPA2-PSK to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. Select No Security to allow any client to connect to this network without authentication. |
| Wireless password | This field appears when you choose wither WPA-PSK or WPA2-PSK as the security mode. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters. |
| Verify password | Type the password again to confirm. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to close this screen. |
| WPS | Click this to configure the WPS screen. You can transfer the wireless settings configured here (Wireless Security screen) to another wireless device that supports WPS. |

7.5.7 WPS

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

Figure 29 Wireless Security: WPS



The following table describes the labels in this screen.

Table 18 Wireless Security: WPS

| LABEL | DESCRIPTION |
|-------------------|--|
| Wireless Security | Click this to go back to the Wireless Security screen. |
| WPS | <p>Create a secure wireless network simply by pressing a button.</p> <p>The NBG5715 scans for a WPS-enabled device within the range and performs wireless security information synchronization.</p> <p>Note: After you click the WPS button on this screen, you have to press a similar button in the wireless station utility within 2 minutes. To add the second wireless station, you have to press these buttons on both device and the wireless station again after the first 2 minutes.</p> |
| Register | <p>Create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the NBG5715's interface and pushing this button.</p> <p>Type the same PIN number generated in the wireless station's utility. Then click Register to associate to each other and perform the wireless security information synchronization.</p> |
| Exit | Click Exit to close this screen. |

7.6 Status Screen in Easy Mode

In the Network Map screen, click **Status** to view read-only information about the NBG5715.

Figure 30 Status Screen in Easy Mode



| | |
|-------------------------------------|-------------------------|
| Name : | ZyXEL NBG5715 |
| Time : | 1970-01-01/09:14:47 |
| WAN IP : | |
| MAC Address : | 00-AA-BB-CC-DD-EE |
| Firmware Version : | NBG5715_1.00(AAAG 0)tr1 |
| <hr/> | |
| Wireless_2.4G Network Name (SSID) : | ZyXEL |
| Security : | No security |
| Wireless_5G Network Name (SSID) : | ZyXEL |
| Security : | No security |

The following table describes the labels in this screen.

Table 19 Status Screen in Easy Mode

| ITEM | DESCRIPTION |
|-------------|---|
| Name | This is the name of the NBG5715 in the network. You can change this in the Maintenance > General screen in Section 22.3 on page 163 . |
| Time | <p>This is the current system date and time.</p> <p>The date is in YYYY:MM:DD (Year-Month-Day) format. The time is in HH:MM:SS (Hour:Minutes:Seconds) format.</p> |
| WAN IP | This is the IP address of the WAN port. |
| MAC Address | This is the MAC address of the NBG5715. |

Table 19 Status Screen in Easy Mode (continued)

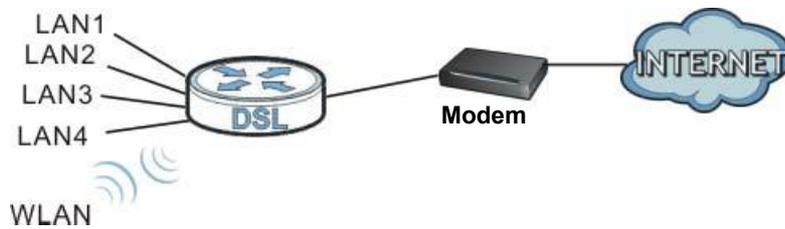
| ITEM | DESCRIPTION |
|--------------------------------------|---|
| Firmware Version | This shows the firmware version of the NBG5715. The firmware version format shows the trunk version, model code and release number. |
| Wireless_2.4G/5G Network Name (SSID) | This shows the SSID of the wireless network. You can configure this in the Wireless Security screen (Section 7.5.6 on page 51 ; Section 11.2 on page 82). |
| Security | This shows the wireless security used by the NBG5715. |

Router Mode

8.1 Overview

The NBG5715 operates as a router. Routers are used to connect the local network to another network (for example, the Internet). In the figure below, the NBG5715 connects the local network (LAN1 ~ LAN4) to the Internet.

Figure 31 NBG5715 Network

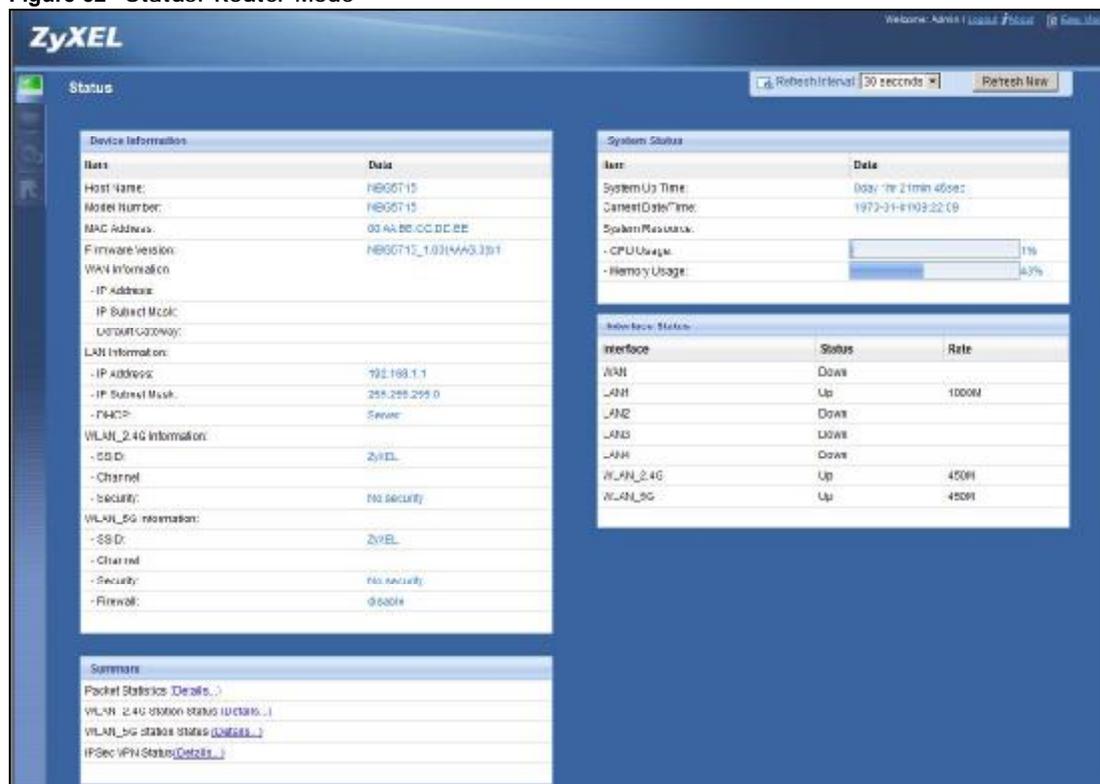


Note: The **Status** screen is shown after changing to the **Expert** mode of the Web Configurator. It varies depending on the device mode of your NBG5715.

8.2 Router Mode Status Screen

Click  to open the status screen.

Figure 32 Status: Router Mode



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

Table 20 Status: Router Mode

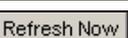
| ICON | DESCRIPTION |
|---|--|
|  | Click this icon to logout of the web configurator. |
|  | Click this icon to view copyright and a link for related product information. |
|  | Click this icon to go to Easy Mode. See Chapter 7 on page 44 . |
|  | Select a number of seconds or None from the drop-down 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. |

Table 20 Status: Router Mode (continued)

| ICON | DESCRIPTION |
|---|--|
|  | 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 21 Status Screen: Router Mode

| LABEL | DESCRIPTION |
|-----------------------|---|
| Device Information | |
| Host Name | This is the System Name you enter in the Maintenance > General screen. It is for identification purposes. |
| Model Number | This is the model name of your device. |
| MAC Address | This shows the WAN Ethernet adapter MAC Address of your device. |
| Firmware Version | This is the firmware version and the date created. |
| WAN Information | |
| - IP Address | This shows the WAN port's IP address. |
| - IP Subnet Mask | This shows the WAN port's subnet mask. |
| - Default Gateway | This shows the WAN port's gateway IP address. |
| LAN Information | |
| - 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_2.4G Information | |
| - SSID | This shows a descriptive name used to identify the NBG5715 in the wireless LAN. |
| - Channel | This shows the channel number which the NBG5715 is currently using over the wireless LAN. |
| - Security | This shows the level of wireless security the NBG5715 is using. |
| WLAN_5G Information | |
| - SSID | This shows a descriptive name used to identify the NBG5715 in the wireless LAN. |
| - Channel | This shows the channel number which the NBG5715 is currently using over the wireless LAN. |
| - Security | This shows the level of wireless security the NBG5715 is using. |
| - Firewall | This shows whether the firewall is enabled or not. |
| System Status | |
| Item | This column shows the type of data the NBG5715 is recording. |
| Data | This column shows the actual data recorded by the NBG5715. |
| System Up Time | This is the total time the NBG5715 has been on. |
| Current Date/Time | This field displays your NBG5715's present date and time. |
| System Resource | |
| - CPU Usage | This displays what percentage of the NBG5715's processing ability is currently used. When this percentage is close to 100%, the NBG5715 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.) |

Table 21 Status Screen: Router Mode (continued)

| LABEL | DESCRIPTION |
|--------------------------|--|
| - Memory Usage | This shows what percentage of the heap memory the NBG5715 is using. |
| Interface Status | |
| Interface | This displays the NBG5715 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 2.4G/5G, it displays the maximum transmission rate when the WLAN 2.4G/5G is enabled and N/A when the WLAN is disabled. |
| Summary | |
| Packet Statistics | Click Details... to go to the Monitor > Packet Statistics screen (Section 5.5 on page 40). Use this screen to view port status and packet specific statistics. |
| WLAN_2.4G Station Status | Click Details... to go to the Monitor > WLAN_2.4G Station Status screen (Section 5.7 on page 41). Use this screen to view the wireless stations that are currently associated to the NBG5715. |
| WLAN_5G Station Status | Click Details... to go to the Monitor > WLAN_5G Station Status screen (Section 5.7 on page 41). Use this screen to view the wireless stations that are currently associated to the NBG5715. |
| IPSec VPN Status | Click Details... to go to the Monitor > VPN Monitor screen (Section 5.4 on page 38). Use this screen to view the active VPN connections. |

8.2.1 Navigation Panel

Use the sub-menus on the navigation panel to configure NBG5715 features.

Figure 33 Navigation Panel: Router Mode

The following table describes the sub-menus.

Table 22 Navigation Panel: Router Mode

| LINK | TAB | FUNCTION |
|--------------------------|-------------|--|
| Status | | This screen shows the NBG5715's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables. |
| MONITOR | | |
| Log | | Use this screen to view the list of activities recorded by your NBG5715. |
| DHCP Table | | Use this screen to view current DHCP client information. |
| Packet Statistics | | Use this screen to view port status and packet specific statistics. |
| VPN Monitor | | Use this screen to view the active VPN connections. |
| WLAN_2.4G Station Status | | Use this screen to view the 2.4G wireless stations that are currently associated to the NBG5715. |
| WLAN_5G Station Status | | Use this screen to view the 5G wireless stations that are currently associated to the NBG5715. |
| CONFIGURATION | | |
| Network | | |
| WAN | Broadband | This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address. |
| | Advanced | Use this screen to configure other advanced properties. |
| Wireless LAN 2.4G | General | Use this screen to enable the 2.4G wireless LAN network, configure its SSID, channel, and the wireless security level. |
| | MAC Filter | Use the MAC filter screen to configure the NBG5715 to block access to devices or block the devices from accessing the NBG5715. |
| | Advanced | This screen allows you to configure advanced wireless settings. |
| | QoS | Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services. |
| | WPS | Use this screen to configure WPS. |
| | WPS Station | Use this screen to add a wireless station using WPS. |
| | Scheduling | Use this screen to schedule the times the Wireless LAN is enabled. |
| Wireless LAN 5G | General | Use this screen to enable the 5G wireless LAN network, configure its SSID, channel, and the wireless security level. |
| | MAC Filter | Use the MAC filter screen to configure the NBG5715 to block access to devices or block the devices from accessing the NBG5715. |
| | Advanced | This screen allows you to configure advanced wireless settings. |
| | QoS | Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services. |
| | WPS | Use this screen to configure WPS. |
| | WPS Station | Use this screen to add a wireless station using WPS. |
| | Scheduling | Use this screen to schedule the times the Wireless LAN is enabled. |
| LAN | IP | Use this screen to configure LAN IP address and subnet mask. |
| | IP Alias | Use this screen to have the NBG5715 apply IP alias to create LAN subnets. |

Table 22 Navigation Panel: Router Mode (continued)

| LINK | TAB | FUNCTION |
|--------------------|------------------|---|
| DHCP Server | General | Use this screen to enable the NBG5715's DHCP server. |
| | Advanced | Use this screen to assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server. |
| | Client List | Use this screen to view information related to your DHCP status. |
| NAT | General | Use this screen to enable NAT. |
| | Port Forwarding | Use this screen to configure forward incoming service requests to the server(s) on your local network. |
| | NAT Advanced | Use this screen to change your NBG5715's port triggering settings. |
| Dynamic DNS | Dynamic DNS | Use this screen to set up dynamic DNS. |
| Static Route | Static Route | Use this screen to configure IP static routes. |
| Security | | |
| Firewall | General | Use this screen to activate/deactivate the firewall. |
| | Services | This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule. |
| IPSec VPN | General | Use this screen to display and manage the NBG5715's VPN rules (tunnels). |
| | SA Monitor | Use this screen to display and manage active VPN connections. |
| Management | | |
| Bandwidth MGMT | General | Use this screen to enable bandwidth management. |
| | Advance | Use this screen to set the upstream bandwidth and edit a bandwidth management rule. |
| Remote MGMT | WWW | Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the NBG5715. |
| | Telnet | Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the NBG5715. |
| UPnP | UPnP | Use this screen to enable UPnP on the NBG5715. |
| 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 NBG5715. |
| Time | Time Setting | Use this screen to change your NBG5715's time and date. |
| Firmware Upgrade | Firmware Upgrade | Use this screen to upload firmware to your NBG5715. |
| Backup/Restore | Backup/Restore | Use this screen to backup and restore the configuration or reset the factory defaults to your NBG5715. |
| Language | Language | This screen allows you to select the language you prefer. |

9.1 Overview

This chapter provides tutorials for setting up your NBG5715.

- [Set Up a Wireless Network with WPS](#)
- [Configure Wireless Security without WPS](#)

9.2 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 NBG5715 as the AP and NWD210N as the wireless client which connects to a notebook. Wireless LAN 2.4G is used as the wireless mode in this example.

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

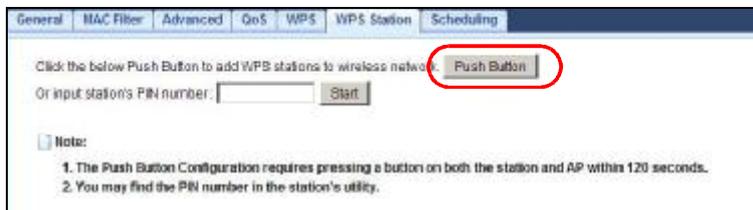
There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See [Section 9.2.1 on page 61](#). 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 NBG5715's interface. See [Section 9.2.2 on page 63](#). This is the more secure method, since one device can authenticate the other.

9.2.1 Push Button Configuration (PBC)

- 1 Make sure that your NBG5715 is turned on. The wireless LAN is enabled by default. Check if WLAN 2.4G LED is on. If not, you can enable wireless LAN by pressing the **WLAN On/Off** button on the device's side panel or in the **Network > Wireless LAN 2.4G** screen. Make sure that 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 NBG5715's Web Configurator and press the **Push Button** in the **Configuration > Network > Wireless LAN 2.4G > WPS Station** screen.



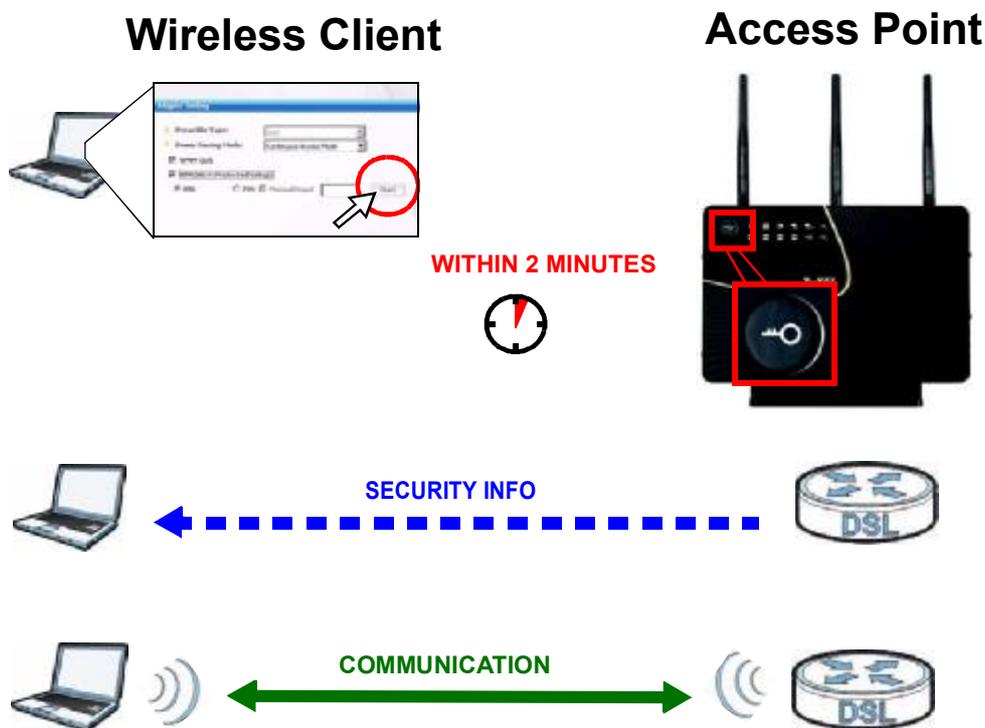
Note: Your NBG5715 has a WPS button located on its front panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

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 NBG5715 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 NBG5715 securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both NBG5715 and wireless client (the NWD210N in this example).

Figure 34 Example WPS Process: PBC Method



9.2.2 PIN Configuration

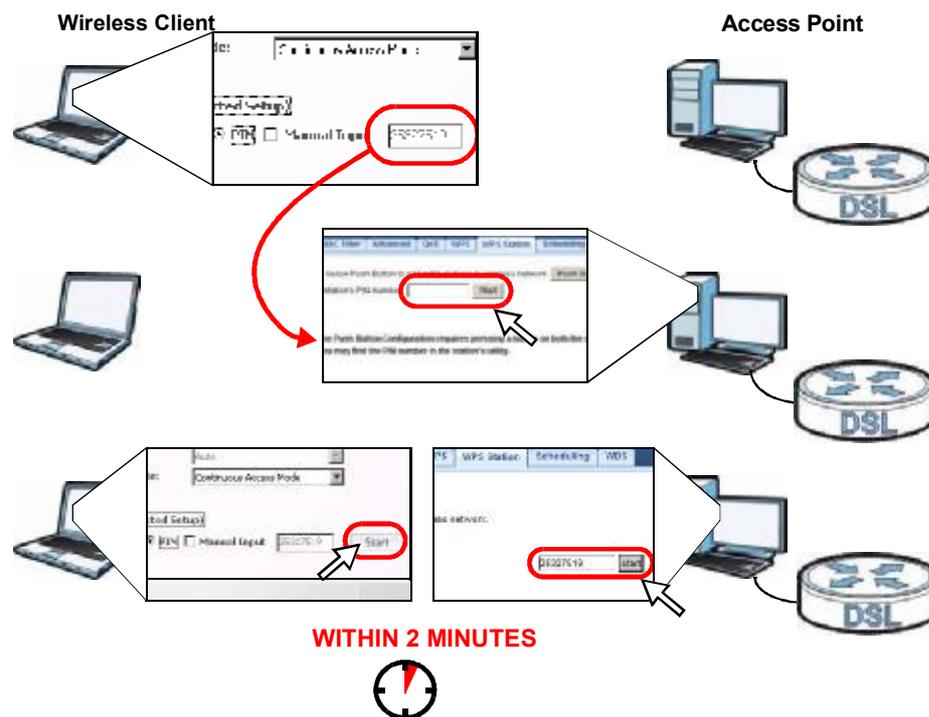
When you use the PIN configuration method, you need to use both NBG5715's configuration interface and the client's utilities.

- 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 > Network > Wireless LAN 2.4G > WPS Station** screen on the NBG5715.
- 3 Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the NBG5715's **WPS Station** screen within two minutes.

The NBG5715 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 NBG5715 securely.

The following figure shows you the example to set up wireless network and security on NBG5715 and wireless client (ex. NWD210N in this example) by using PIN method.

Figure 35 Example WPS Process: PIN Method



9.3 Configure Wireless Security without WPS

This example shows you how to configure wireless security settings with the following parameters on your NBG5715.

| | |
|-------------------|---|
| Wireless LAN Mode | 2.4G |
| SSID | SSID_Example3 |
| Channel | 6 |
| Security | WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey) |

Follow the steps below to configure the wireless settings on your NBG5715.

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 4.2 on page 33](#)).

- 1 Open the **Configuration > Wireless LAN 2.4G > General** screen in the AP's Web Configurator.
- 2 Confirm that the status of wireless LAN is enabled.
- 3 Enter **SSID_Example3** as the SSID and select **Channel-06** as the channel.
- 4 Set security mode to **WPA-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

The screenshot shows the 'Wireless Setup' configuration page. The 'Wireless LAN' option is enabled. The SSID is 'SSID_Example3'. The channel is set to 'Channel-06 2437MHz'. The security mode is 'WPA-PSK' and the pre-shared key is 'ThisismyWPA-PSKpre-sharedkey'. The group key update timer is 3600 seconds. There are 'Apply' and 'Cancel' buttons at the bottom.

- 5 Open the Status screen. Verify your WLAN 2.4G wireless and wireless security settings under Device Information and check if the WLAN 2.4G connection is up under Interface Status.

The screenshot displays the ZyXEL Status page with the following sections:

- Device Information:**

| Item | Data |
|----------------------------|----------------------|
| Host Name | NBG5715 |
| Model Number | NR04781 |
| MAC Address | ED:AA:9B:C2:00:0E |
| Firmware Version | NR04781_V1.00000.001 |
| LAN Information: | |
| - IP Address: | |
| - IP Subnet Mask: | |
| - Default Gateway: | |
| LAN Information: | |
| - IP Address: | 192.168.1.1 |
| - IP Subnet Mask: | 255.255.255.0 |
| - DHCP: | Enable |
| WLAN_2.4G Information: | |
| - SSID: | SSID_Example3 |
| - Channel: | 6 |
| - Security: | WPA/PSK |
| WLAN_Security Information: | |
| - SSID: | ZyXEL |
| - Channel: | |
| - Security: | No security |
| - Firewall: | Disable |
- System Status:**

| Item | Data |
|--------------------|------------------------|
| System Up Time: | 5:09:11.379 (2594) |
| Current Date/Time: | 1803-11-18 10:08:37:00 |
| System Resource: | |
| - CPU Usage: | 1% |
| - Memory Usage: | 14% |
- Interface Status:**

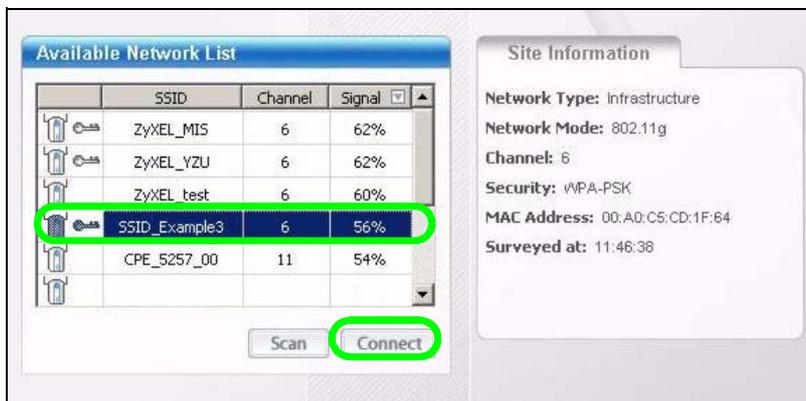
| Interface | Status | Rate |
|-----------|--------|-------|
| WAN | Down | |
| LAN1 | Up | 1000M |
| LAN2 | Down | |
| LAN3 | Down | |
| LAN4 | Down | |
| WLAN_2.4G | Up | 450M |
| WLAN_5G | Up | 450M |

9.3.1 Configure Your Notebook

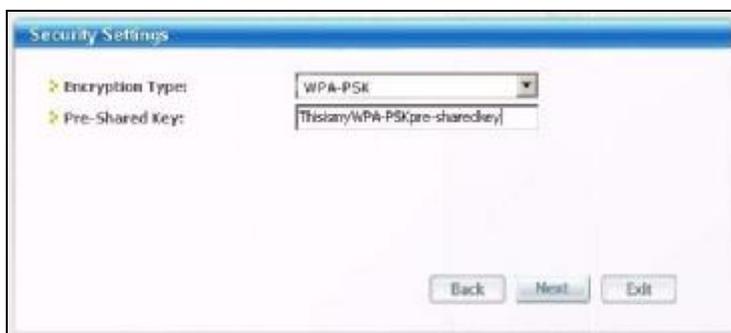
Note: We use the ZyXEL M-302 wireless adapter utility screens as an example for the wireless client. The screens may vary for different models.

- 1 The NBG5715 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.

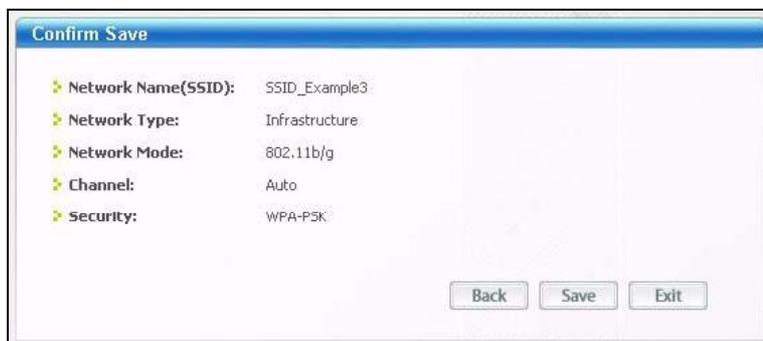
- 4 Select SSID_Example3 and click Connect.



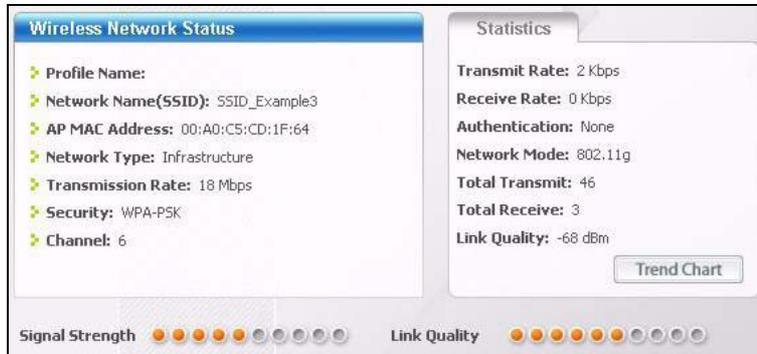
- 5 Select WPA-PSK and type the security key in the following screen. Click Next.



- 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 the 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.

PART II

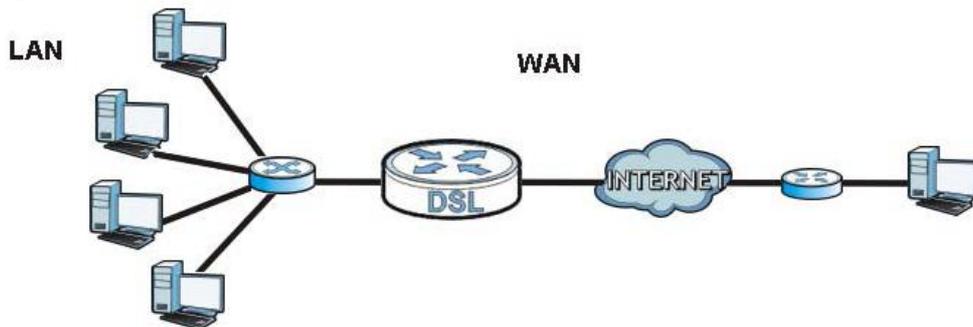
Technical Reference

10.1 Overview

This chapter discusses the NBG5715's WAN screens. Use these screens to configure your NBG5715 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 36 LAN and WAN



10.2 What You Can Do in this Chapter

- Use the **Broadband** screen to enter your ISP information and set how the computer acquires its IP, DNS and WAN MAC addresses ([Section 10.4 on page 73](#)).
- Use the **Advanced** screen to enable multicasting ([Section 10.5 on page 77](#)).

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 NBG5715.

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 NBG5715, which makes it accessible from an outside network. It is used by the NBG5715 to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the NBG5715 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 NBG5715 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 NBG5715's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

WAN MAC Address

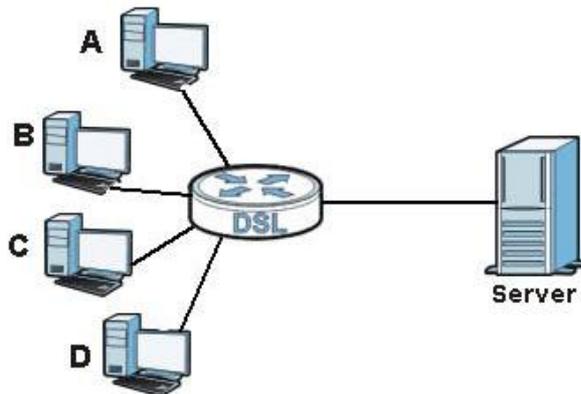
The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

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.

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 37 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 NBG5715 supports both IGMP version 1 (IGMP-v1) and IGMP version 2 (IGMP-v2).

At start up, the NBG5715 queries all directly connected networks to gather group membership. After that, the NBG5715 periodically updates this information. IP multicasting can be enabled/disabled on the NBG5715 LAN and/or WAN interfaces in the Web Configurator (LAN; WAN). Select None to disable IP multicasting on these interfaces.

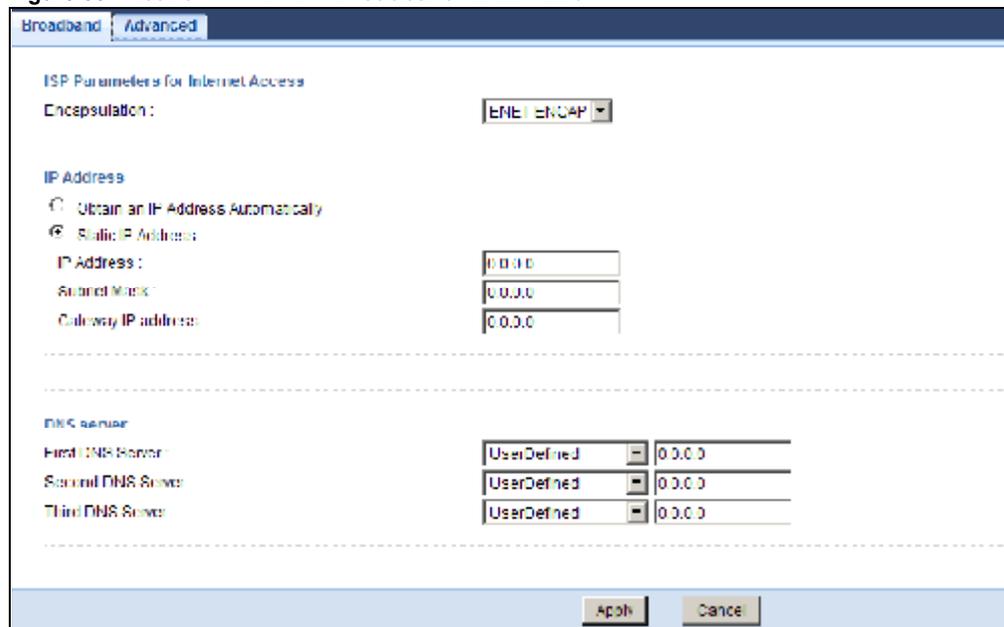
10.4 The Broadband Screen

Use this screen to change your NBG5715's Internet access settings. Click **Configuration > Network > WAN** to open the **Broadband** screen. The screen differs according to the encapsulation you choose.

10.4.1 Ethernet Encapsulation

This screen displays when you select ENET ENCAP (Ethernet encapsulation).

Figure 38 Network > WAN > Broadband: ENET ENCAP



The following table describes the labels in this screen.

Table 23 Network > WAN > Broadband: ENET ENCAP

| LABEL | DESCRIPTION |
|------------------------------------|--|
| ISP Parameters for Internet Access | |
| Encapsulation | Choose the ENET ENCAP (Ethernet encapsulation) option when the WAN port is used as a regular Ethernet. |
| Obtain an IP Address Automatically | Select this option if your ISP did not assign you a fixed IP address. This is the default selection. |
| Static 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 Static IP Address. |
| Subnet Mask | Enter the Subnet Mask in this field. |
| Gateway IP Address | Enter a Gateway IP Address (if your ISP gave you one) in this field. |
| First DNS Server | Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the NBG5715'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. |
| Second DNS Server | |
| Third DNS Server | |

Table 23 Network > WAN > Broadband: ENET ENCAP (continued)

| LABEL | DESCRIPTION |
|--------|--|
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

10.4.2 PPPoE Encapsulation

The NBG5715 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 NBG5715 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG5715 does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

This screen displays when you select PPPoE encapsulation.

Figure 39 Network > WAN > Broadband: PPPoE

The screenshot shows the 'Broadband' configuration page with the 'Advanced' tab selected. The 'ISP Parameters for Internet Access' section has 'Encapsulation' set to 'PPPoE'. The 'PPP Information' section includes fields for 'PPP Username', 'PPP Password', 'PPP Auto Connect' (checked), and 'IDLE Timeout (seconds)' set to '300'. The 'WAN IP Address Assignment' section has 'Get automatically from ISP' selected. The 'DNS server' section has three fields for 'First DNS Server', 'Second DNS Server', and 'Third DNS Server', each with a dropdown menu set to 'Obtained From ISP'. 'Apply' and 'Cancel' buttons are at the bottom.

The following table describes the labels in this screen.

Table 24 Network > WAN > Broadband: PPPoE

| LABEL | DESCRIPTION |
|------------------------------------|---|
| ISP Parameters for Internet Access | |
| Encapsulation | Select PPPoE if you connect to your Internet via dial-up. |
| PPP Information | |
| PPP Username | Type the user name given to you by your ISP. |
| PPP Password | Type the password associated with the user name above. |
| PPP Auto Connect | Select this option if you do not want the connection to time out. |
| IDLE Timeout | This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server. |
| PPPoE Service Name | Enter the name of your PPPoE service here. |
| WAN IP Address Assignment | |
| Get automatically from ISP | Select this option if your ISP did not assign you a fixed IP address. This is the default selection. |
| Use Fixed IP Address | Select this option if the ISP assigned a fixed IP address. |
| My WAN IP Address | Enter your WAN IP address in this field if you selected Use Fixed IP Address . |
| DNS Server | |
| First DNS Server | Select From ISP if your ISP dynamically assigns DNS server information (and the NBG5715's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. |
| Second DNS Server | Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined , but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply . If you set a second choice to User-Defined , and enter the same IP address, the second User-Defined changes to None after you click Apply . |
| | Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

10.5 The Advanced Screen

To change your NBG5715's advanced WAN settings, click **Network > WAN > Advanced**. The screen appears as shown. You can use this screen to enable multicast.

Figure 40 Network > WAN > Advanced

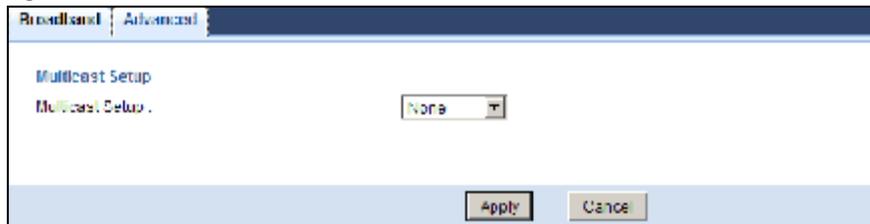


Table 25 Network > WAN > Advance

| LABEL | DESCRIPTION |
|-----------------|---|
| Multicast Setup | Select IGMPv1/v2 to enable multicasting. This applies to traffic routed from the WAN to the LAN. Select None to disable this feature. This may cause incoming traffic to be dropped or sent to all connected network devices. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

Wireless LAN

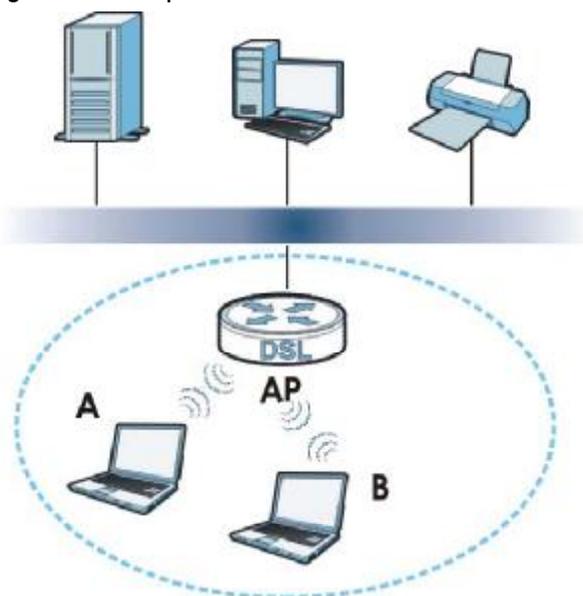
11.1 Overview

This chapter discusses how to configure the wireless network settings in your NBG5715. The NBG5715 is able to function both 2.4G and 5G network at the same time. You can have different wireless settings for 2.4G and 5G. Click **Configuration > Network > Wireless LAN 2.4G** or **Wireless LAN 5G** to configure to do so.

See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 41 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 NBG5715 is the AP.

11.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable or disable wireless LAN, configure SSID, operating channel, and wireless security ([Section 11.2 on page 82](#)).
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the NBG5715 ([Section 11.4 on page 88](#)).

- Use the **Advanced** screen to allow intra-BSS networking and set the RTS/CTS Threshold ([Section 11.5 on page 90](#)).
- Use the **QoS** screen to ensure Quality of Service (QoS) in your wireless network ([Section 11.6 on page 90](#)).
- Use the **WPS** screen to quickly set up a wireless network with strong security, without having to configure security settings manually ([Section 11.7 on page 91](#)).
- Use the **WPS Station** screen to add a wireless station using WPS ([Section 11.8 on page 92](#)).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off ([Section 11.9 on page 93](#)).

11.1.2 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.

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.

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

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

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 81](#) for information about this.)

Table 26 Types of Encryption for Each Type of Authentication

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

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

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

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

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

When you select **WPA2 or WPA2-PSK** in your NBG5715, you can also select an option (**WPA Compatible**) to support WPA as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK or WPA2** (depending on the type of wireless network login) and select the **WPA Compatible** option in the NBG5715.

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 9.2 on page 61](#).

WDS

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

11.2 The General Wireless LAN Screen

Use this screen to configure the SSIDs of the wireless LAN.

Note: If you are configuring the NBG5715 from a computer connected to the wireless LAN and you change the NBG5715'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 NBG5715's new settings.

Click **Network > Wireless LAN 2.4G/5G** to open the **General** screen.

Figure 42 Network > Wireless LAN 2.4G/5G > General

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

Table 27 Network > Wireless LAN 2.4G/5G > General

| LABEL | DESCRIPTION |
|------------------------|---|
| Wireless LAN | Select Enable to activate the 2.4G and/or 5G wireless LAN. Select Disable to turn it off. |
| 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. |
| Hide SSID | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool. |
| Channel Selection | Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Refer to the Connection Wizard chapter for more information on channels. This option is only available if Auto Channel Selection is disabled. |
| Auto Channel Selection | Select this check box for the NBG5715 to automatically choose the channel with the least interference. Deselect this check box if you wish to manually select the channel using the Channel Section field. |
| Operating Channel | This displays the channel the NBG5715 is currently using. |
| Channel Width | Select the wireless channel width used by NBG5715. A standard 20 MHz channel offers transfer speeds of up to 216.7 Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 450 Mbps. Because not all devices support 40 MHz channels, select Auto 20/40MHz to allow the NBG5715 to adjust the channel bandwidth automatically. Select 20 MHz to lessen radio interference with other wireless devices in your neighborhood. |

Table 27 Network > Wireless LAN 2.4G/5G > General (continued)

| LABEL | DESCRIPTION |
|---------------|---|
| Wireless Mode | <p>If you are in the Wireless LAN 2.4G > General screen, you can select from the following:</p> <ul style="list-style-type: none"> • 802.11b: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the NBG5715. In this mode, all wireless devices can only transmit at the data rates supported by IEEE 802.11b. • 802.11g: allows IEEE 802.11g compliant WLAN devices to associate with the Device. IEEE 802.11b compliant WLAN devices can associate with the NBG5715 only when they use the short preamble type. • 802.11bg: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the NBG5715. The NBG5715 adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. • 802.11n: allows IEEE 802.11n compliant WLAN devices to associate with the NBG5715. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the NBG5715. I • 802.11gn: allows either IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the NBG5715. The transmission rate of your NBG5715 might be reduced. • 802.11 bgn: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the NBG5715. The transmission rate of your NBG5715 might be reduced. <p>If you are in the Wireless LAN 5G > General screen, you can select from the following:</p> <ul style="list-style-type: none"> • 802.11a: allows only IEEE 802.11a compliant WLAN devices to associate with the NBG5715. • 802.11an: allows both IEEE802.11n and IEEE802.11a compliant WLAN devices to associate with the NBG5715. The transmission rate of your NBG5715 might be reduced. |
| Security Mode | <p>Select Static WEP, WPA-PSK, WPA, WPA2-PSK or WPA2 to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See Section 11.3 on page 84 for detailed information on different security modes. Or you can select No Security to allow any client to associate this network without authentication.</p> <p>Note: If the WPS function is enabled (default), only No Security, WPA-PSK and WPA2-PSK are available in this field.</p> |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to reload the previous configuration for this screen. |

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

11.3 Wireless Security Modes

11.3.1 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 NBG5715, your network is accessible to any wireless networking device that is within range.

Figure 43 Network > Wireless LAN 2.4G/5G > Security: No Security

Security
Security Mode :

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

Apply Cancel

The following table describes the labels in this screen.

Table 28 Network > Wireless LAN > Security: No Security

| LABEL | DESCRIPTION |
|---------------|---|
| Security Mode | Choose No Security from the drop-down list box. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to reload the previous configuration for this screen. |

11.3.2 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 NBG5715 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 44 Network > Wireless LAN 2.4G/5G > Security: Static WEP

Security
Security Mode :

PassPhrase :

WEP Encryption :

Authentication Method :

Note:
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)

ASCII Hex

Key 1

Key 2

Key 3

Key 4

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

Apply Cancel

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

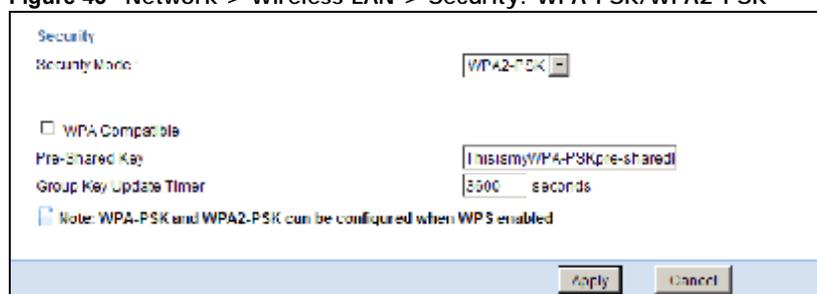
Table 29 Network > Wireless LAN 2.4G/5G > Security: Static WEP

| LABEL | DESCRIPTION |
|-----------------------|---|
| Security Mode | Select Static WEP to enable data encryption. |
| PassPhrase | Enter a Passphrase (up to 26 printable characters) and click Generate . A passphrase functions like a password. In WEP security mode, it is further converted by the NBG5715 into a complicated string that is referred to as the "key". This key is requested from all devices wishing to connect to a wireless network. |
| WEP Encryption | Select 64-bits or 128-bits . This dictates the length of the security key that the network is going to use. |
| Authentication Method | Select Auto or Shared Key from the drop-down list box. This field specifies whether the wireless clients have to provide the WEP key to login to the wireless client. Keep this setting at Auto unless you want to force a key verification before communication between the wireless client and the NBG5715 occurs. Select Shared Key to force the clients to provide the WEP key prior to communication. |
| ASCII | Select this option in order to enter ASCII characters as WEP key. |
| Hex | Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically. |
| Key 1 to Key 4 | The WEP keys are used to encrypt data. Both the NBG5715 and the wireless stations must use the same WEP key for data transmission. If you chose 64-bit WEP , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128-bit WEP , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to reload the previous configuration for this screen. |

11.3.3 WPA-PSK/WPA2-PSK

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

Figure 45 Network > Wireless LAN > Security: WPA-PSK/WPA2-PSK



The following table describes the labels in this screen.

Table 30 Network > Wireless LAN > Security: WPA-PSK/WPA2-PSK

| LABEL | DESCRIPTION |
|------------------------|---|
| 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 NBG5715. |
| Pre-Shared Key | WPA-PSK/WPA2-PSK uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters. |
| Group Key Update Timer | The Group Key Update Timer is the rate at which the AP sends a new group key out to all clients. The default is 3600 seconds (60 minutes). |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to reload the previous configuration for this screen. |

11.3.4 WPA/WPA2

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

Figure 46 Network > Wireless LAN 2.4G/5G > General: WPA/WPA2

The screenshot shows the configuration interface for WPA/WPA2 security. The 'Security Mode' dropdown is set to 'WPA2'. Below it, the 'WPA Compatible' checkbox is unchecked. The 'Group Key Update Timer' is set to 3600 seconds. The 'PMK Cache Period' is set to 10 seconds. The 'Pre-Authentication' radio buttons have 'Disable' selected. The 'Authentication Server' section includes an IP address of 192.168.2.3, a port number of 1012, and a shared secret of 12345678. The 'Session Timeout' is set to 0. A note at the bottom indicates that WPA PSK and WPA2 PSK can be configured when WPA is enabled. 'Apply' and 'Cancel' buttons are located at the bottom right.

The following table describes the labels in this screen.

Table 31 Network > Wireless LAN > General: WPA/WPA2

| LABEL | DESCRIPTION |
|----------------|---|
| Security Mode | Select WPA or WPA2 to enable data encryption. |
| WPA Compatible | This check box is available only when you select WPA2-PSK or WPA2 in the Security Mode field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the NBG5715 even when the NBG5715 is using WPA2-PSK or WPA2 . |

Table 31 Network > Wireless LAN > General: WPA/WPA2 (continued)

| LABEL | DESCRIPTION |
|------------------------|---|
| Group Key Update Timer | The Group Key Update Timer is the rate at which the AP (if using WPA-PSK/WPA2-PSK key management) or RADIUS server (if using WPA/WPA2 key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the Group Key Update Timer is also supported in WPA-PSK/WPA2-PSK mode. |
| PMK Cache Period | This field is available only when you select WPA2 . Specify how often wireless clients have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 99999 minutes. Note: If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority. |
| Pre-Authentication | This field is available only when you select WPA2 . 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. Select Enable to turn on preauthentication in WAP2. Otherwise, select Disable . |
| Authentication Server | |
| IP Address | Enter the IP address of the external authentication server in dotted decimal notation. |
| Port Number | Enter the port number of the external authentication server. You need not change this value unless your network administrator instructs you to do so with additional information. |
| Shared Secret | Enter a password (up to 127 alphanumeric characters) as the key to be shared between the external authentication server and the NBG5715. The key must be the same on the external authentication server and your NBG5715. The key is not sent over the network. |
| Session Timeout | The NBG5715 automatically disconnects a wireless client from the wireless and wired networks after a period of inactivity. The wireless client needs to send the username and password again before it can use the wireless and wired networks again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. Enter the time in seconds from 0 to 999999. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Reset | Click Reset to reload the previous configuration for this screen. |

11.4 The MAC Filter Screen

The MAC filter screen allows you to configure the NBG5715 to give exclusive access to devices (**Allow**) or exclude devices from accessing the NBG5715 (**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 NBG5715's MAC filter settings, click **Network > Wireless LAN 2.4G/5G > MAC Filter**. The screen appears as shown.

Figure 47 Network > Wireless LAN 2.4G/5G > MAC Filter

The following table describes the labels in this menu.

Table 32 Network > Wireless LAN 2.4G/5G > MAC Filter

| LABEL | DESCRIPTION |
|--------------------|---|
| MAC Address Filter | Select to turn on (Enable) or off (Disable) MAC address filtering. |
| Filter Action | Define the filter action for the list of MAC addresses in the MAC Filter Summary table. This field is configurable only when you select Enable in the MAC Address Filter field. Select Allow to permit access to the NBG5715, MAC addresses not listed will be denied access to the NBG5715. Select Deny to block access to the NBG5715, MAC addresses not listed will be allowed to access the NBG5715. |
| MAC Filter Summary | |
| Set | This is the index number of the MAC address. |
| MAC Address | Enter the MAC address of the wireless station that are allowed or denied access to the NBG5715. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to reload the previous configuration for this screen. |

11.5 The 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 **Network > Wireless LAN 2.4G/5G > Advanced**. The screen appears as shown.

Figure 48 Network > Wireless LAN 2.4G/5G > Advanced

| Setting | Value | Range |
|---------------------------|---|--------------|
| RTS/CTS Threshold : | 2345 | (256 ~ 2346) |
| Fragmentation Threshold : | 2344 | (256 ~ 2346) |
| Intra-BSS Traffic : | <input type="radio"/> Enable <input checked="" type="radio"/> Disable | |
| advance tx power : | 100% | |

The following table describes the labels in this screen.

Table 33 Network > Wireless LAN 2.4G/5G > Advanced

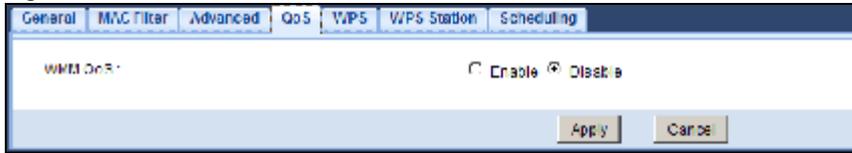
| LABEL | DESCRIPTION |
|-------------------------|--|
| RTS/CTS Threshold | Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. |
| Fragmentation Threshold | The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. |
| 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 clients can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless clients can still access the wired network but cannot communicate with each other. |
| advance tx power | Set the output power of the NBG5715 in this field. If there is a high density of APs in an area, decrease the output power of the NBG5715 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 NBG5715's output power. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to reload the previous configuration for this screen. |

11.6 The QoS Screen

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

Click **Network > Wireless LAN 2.4G/5G > QoS**. The following screen appears.

Figure 49 Network > Wireless LAN 2.4G/5G > QoS



The following table describes the labels in this screen.

Table 34 Network > Wireless LAN 2.4G/5G > QoS

| LABEL | DESCRIPTION |
|----------------|--|
| Enable WMM QoS | Check this to have the NBG5715 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 NBG5715. |
| Cancel | Click Cancel to reload the previous configuration for this screen. |

11.7 The WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. To open this screen, click **Network > Wireless LAN 2.4G/5G > WPS** tab.

Note: With WPS, wireless clients can only connect to the wireless network using the first SSID on the NBG5715.

Figure 50 Network > Wireless LAN 2.4G/5G > WPS



The following table describes the labels in this screen.

Table 35 Network > Wireless LAN 2.4G/5G > WPS

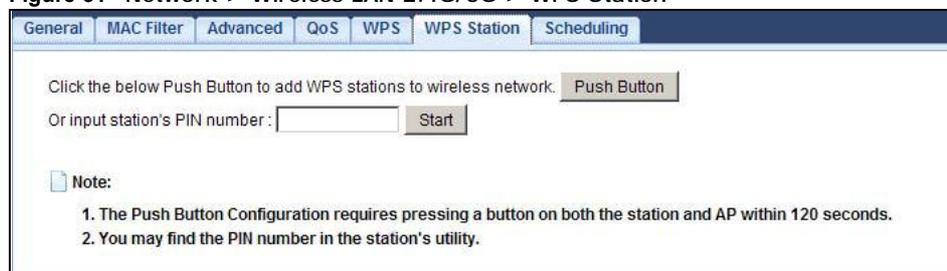
| LABEL | DESCRIPTION |
|-----------------------|---|
| WPS Setup | |
| WPS | Select Enable to activate the WPS feature. Select Disable to turn it off. |
| PIN Number | This displays a PIN number last time system generated. Click Generate to generate a new PIN number. |
| WPS Status | |
| Status | This displays Configured when the NBG5715 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 NBG5715 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 NBG5715. |
| 802.11 Mode | This is the 802.11 mode used. Only compliant WLAN devices can associate with the NBG5715. |
| SSID | This is the name of the wireless network (the NBG5715'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 NBG5715. |
| Cancel | Click Cancel to reload the previous configuration for this screen. |

11.8 The WPS Station Screen

Use this screen when you want to add a wireless station using WPS. To open this screen, click **Network > Wireless LAN 2.4G/5G > 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 51 Network > Wireless LAN 2.4G/5G > WPS Station



The following table describes the labels in this screen.

Table 36 Network > Wireless LAN 2.4G/5G > WPS Station

| LABEL | DESCRIPTION |
|-------------------------------|--|
| Push Button | Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. See Section 9.2.1 on page 61 . Click this to start WPS-aware wireless station scanning and the wireless security information synchronization. |
| Or input station's PIN number | Use this button when you use the PIN Configuration method to configure wireless station's wireless settings. See Section 9.2.2 on page 63 . Type the same PIN number generated in the wireless station's utility. Then click Start to associate to each other and perform the wireless security information synchronization. |

11.9 The Scheduling Screen

Use this screen to set the times your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default. The wireless LAN can be scheduled to turn on or off on certain days and at certain times. To open this screen, click **Network > Wireless LAN 2.4G/5G > Scheduling** tab.

Figure 52 Network > Wireless LAN 2.4G/5G > Scheduling

The following table describes the labels in this screen.

Table 37 Network > Wireless LAN 2.4G/5G > Scheduling

| LABEL | DESCRIPTION |
|-------------------------|--|
| Wireless LAN Scheduling | Select Enable to activate the scheduling feature. Select Disable to turn it off. |
| 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. |

Table 37 Network > Wireless LAN 2.4G/5G > Scheduling (continued)

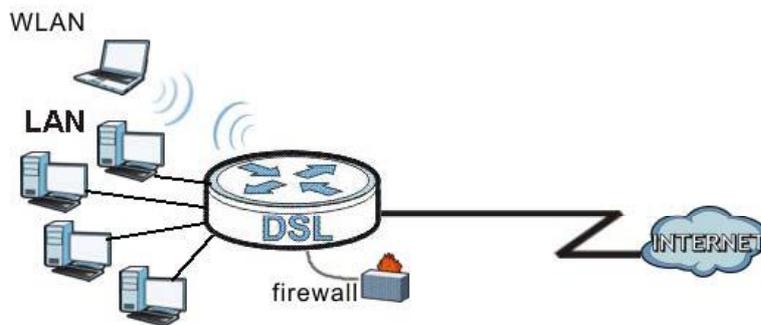
| LABEL | DESCRIPTION |
|---|--|
| Day | Select Everyday or the specific days to turn the Wireless LAN on or off. If you select Everyday you can not select any specific days. This field works in conjunction with the For the following times field. |
| Except for the following times (24-Hour Format) | Select a begin time using the first set of hour and minute (min) drop down boxes and select an end time using the second set of hour and minute (min) drop down boxes. If you have chosen On earlier for the WLAN Status the Wireless LAN will turn 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 NBG5715. |
| Cancel | Click Cancel to reload the previous configuration for this screen. |

12.1 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 53 LAN Example



The LAN screens can help you manage IP addresses.

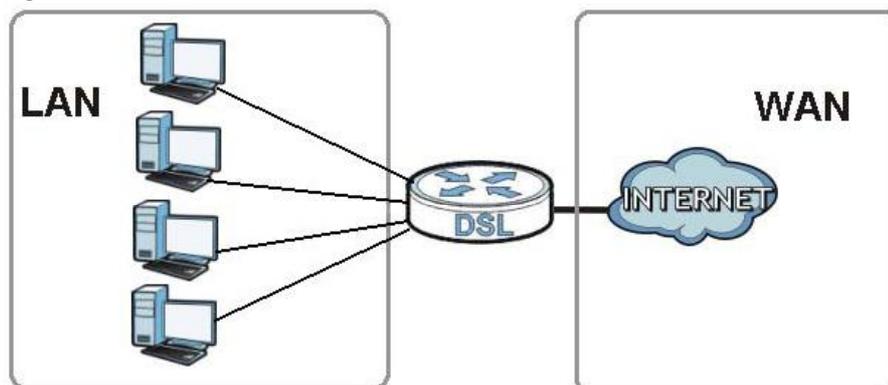
12.2 What You Can Do in this Chapter

- Use the IP screen to change the IP address for your NBG5715 ([Section 12.4 on page 97](#)).
- Use the IP Alias screen to have the NBG5715 apply IP alias to create LAN subnets ([Section 12.5 on page 97](#)).

12.3 What You Need To Know

The actual physical connection determines whether the NBG5715 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 54 LAN and WAN IP Addresses



The LAN parameters of the NBG5715 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.

12.3.1 IP Pool Setup

The NBG5715 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 NBG5715 itself) in the lower range (192.168.1.2 to 192.168.1.32) for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

12.3.2 LAN TCP/IP

The NBG5715 has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

12.4 The LAN IP Screen

Use this screen to change the IP address for your NBG5715. Click **Network > LAN > IP**.

Figure 55 Network > LAN > IP

The screenshot shows a web-based configuration interface for the LAN IP settings. At the top, there are two tabs: 'IP' and 'IP Alias', with 'IP' selected. Below the tabs, there are two input fields: 'IP Address' with the value '192.168.1.1' and 'IP Subnet Mask' with the value '255.255.255.0'. At the bottom right, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 38 Network > LAN > IP

| LABEL | DESCRIPTION |
|----------------|--|
| IP Address | Type the IP address of your NBG5715 in dotted decimal notation. |
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. Your NBG5715 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 NBG5715. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

12.5 The IP Alias Screen

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The NBG5715 supports three logical LAN interfaces via its single physical Ethernet interface with the NBG5715 itself as the gateway for each LAN network.

To change your NBG5715's IP alias settings, click **Network > LAN > IP Alias**. The screen appears as shown.

Figure 56 Network > LAN > IP Alias

The screenshot shows a web-based configuration interface for IP Alias settings. At the top, there are two tabs: 'IP' and 'IP Alias', with 'IP Alias' selected. Below the tabs, there are two sections for IP Alias 1 and IP Alias 2. Each section has a checkbox for 'IP Alias', and fields for 'IP Address' and 'IP Subnet Mask'. The values for IP Alias 1 are 0.0.0.0 and 0.0.0.0, and for IP Alias 2 are 0.0.0.0 and 0.0.0.0. At the bottom right, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 39 Network > LAN > IP Alias

| LABEL | DESCRIPTION |
|----------------|--|
| IP Alias 1, 2 | Select the check box to configure another LAN network for the NBG5715. |
| IP Address | Type the IP alias address of your NBG5715 in dotted decimal notation. |
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. Your NBG5715 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 NBG5715. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

DHCP Server

13.1 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 NBG5715's LAN as a DHCP server or disable it. When configured as a server, the NBG5715 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.

13.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable the DHCP server ([Section 13.2 on page 99](#)).
- Use the **Advanced** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses ([Section 13.3 on page 100](#)).
- Use the **Client List** screen to view the current DHCP client information ([Section 13.4 on page 101](#)).

13.1.2 What You Need To Know

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

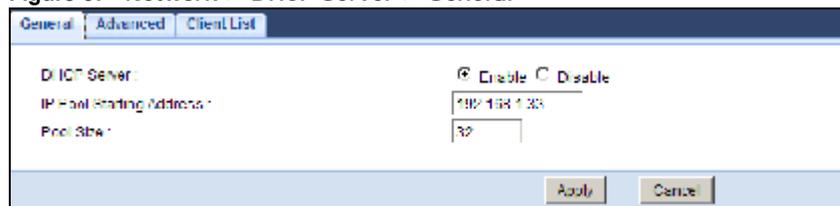
MAC Addresses

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.

13.2 The DHCP Server General Screen

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

Figure 57 Network > DHCP Server > General



The following table describes the labels in this screen.

Table 40 Network > DHCP Server > General

| LABEL | DESCRIPTION |
|--------------------------|---|
| DHCP Server | Select Enable to activate 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. Enable the DHCP server unless your ISP instructs you to do otherwise. Select Disable to stop the NBG5715 acting as a DHCP server. When configured as a server, the NBG5715 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 NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

13.3 The DHCP Server 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 NBG5715 sends to the DHCP clients.

To change your NBG5715's static DHCP settings, click **Network > DHCP Server > Advanced**. The following screen displays.

Figure 58 Network > DHCP Server > Advanced

The screenshot shows the 'Advanced' tab of the DHCP Server configuration. At the top, there are three tabs: 'General', 'Advanced', and 'Client List'. The main area is titled 'Static DHCP Table' and contains a table with three columns: '#', 'MAC Address', and 'IP Address'. The table has 8 rows, each with a MAC address field (all containing '00:00:00:00:00:00') and an IP address field (all containing '0.0.0.0'). Below the table, there is a section for 'DNS Server' configuration. It includes the text 'DNS Servers Assigned by DHCP Server' and three rows for 'First DNS Server', 'Second DNS Server', and 'Third DNS Server'. Each row has a dropdown menu set to 'From ISP' and an IP address field containing '0.0.0.0'. At the bottom of the screen, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 41 Network > DHCP Server > Advanced

| LABEL | DESCRIPTION |
|-------------------------------------|---|
| Static DHCP Table | |
| # | This is the index number of the static IP table entry (row). |
| MAC Address | Type the MAC address (with colons) of a computer on your LAN. |
| IP Address | Type the LAN IP address of a computer on your LAN. |
| DNS Server | |
| DNS Servers Assigned by DHCP Server | The NBG5715 passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The NBG5715 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. |
| First DNS Server | Select From ISP if your ISP dynamically assigns DNS server information (and the NBG5715's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. |
| Second DNS Server | |
| Third DNS Server | |
| | Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined , but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply . If you set a second choice to User-Defined , and enter the same IP address, the second User-Defined changes to None after you click Apply . |
| | Select DNS Relay to have the NBG5715 act as a DNS proxy. The NBG5715's LAN IP address displays in the field to the right (read-only). The NBG5715 tells the DHCP clients on the LAN that the NBG5715 itself is the DNS server. When a computer on the LAN sends a DNS query to the NBG5715, the NBG5715 forwards the query to the NBG5715'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 . |
| | 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. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

13.4 The Client List Screen

The DHCP table shows current DHCP client information (including IP Address, Host Name and MAC Address) of network clients using the NBG5715's DHCP servers.

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

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

Figure 59 Network > DHCP Server > Client List



The following table describes the labels in this screen.

Table 42 Network > DHCP Server > Client List

| LABEL | DESCRIPTION |
|-------------|--|
| # | This is the index number of the host computer. |
| Status | This field displays whether the connection to the host computer is up (a yellow bulb) or down (a gray bulb). |
| Host Name | This field displays the computer host name. |
| IP Address | This field displays the IP address relative to the # field listed above. |
| 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. |
| Reserve | Select this if you want to reserve the IP address for this specific MAC address. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Reset | Click Cancel to reload the previous configuration for this screen. |

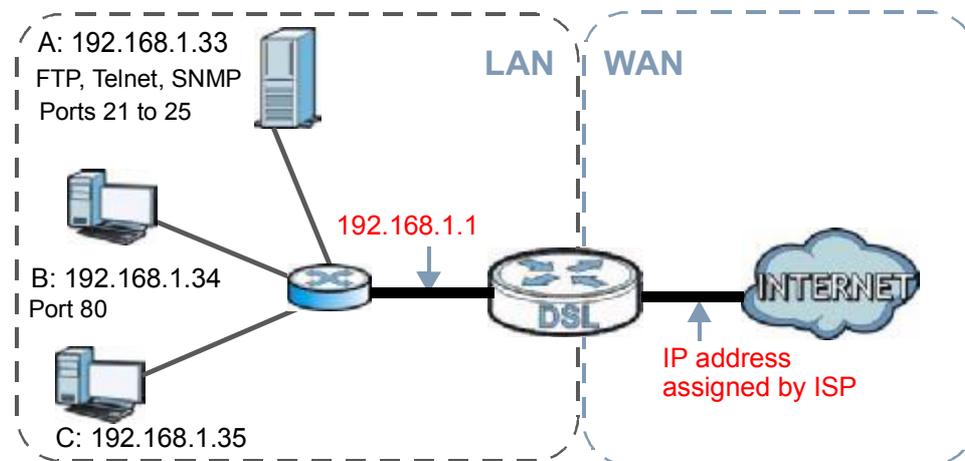
14.1 Overview

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

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

You assign the LAN IP addresses to the devices (A to D) connected to your NBG5715. 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 NBG5715, which is 192.168.1.1.

Figure 60 NAT Example



This chapter discusses how to configure NAT on the NBG5715.

Note: You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the NBG5715.

14.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable NAT and set a default server ([Section 14.2 on page 105](#)).
- Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network ([Section 14.3 on page 106](#)).

- Use the NAT Advance screen to change your NBG5715's trigger port settings ([Section 14.4 on page 109](#)).

14.1.2 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 NBG5715, 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 43 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.

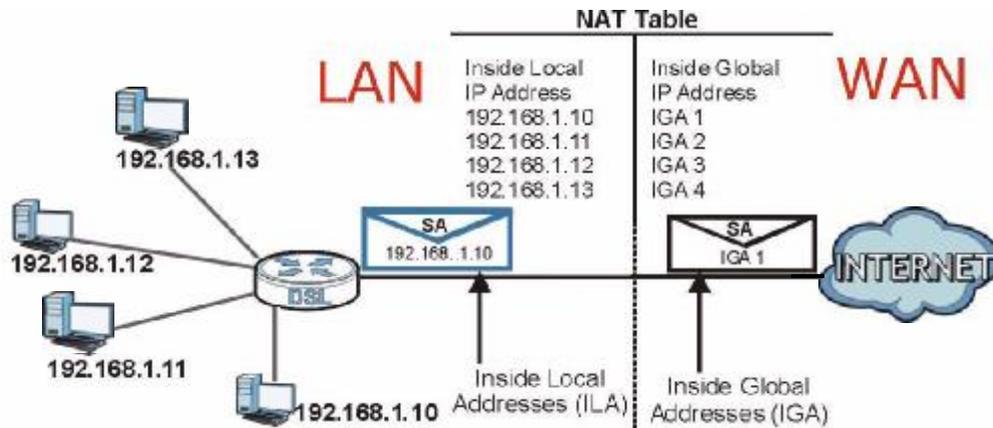
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your NBG5715 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 NBG5715 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 61 How NAT Works



14.2 The NAT General Screen

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

Figure 62 Network > NAT > General

| General | Port Forwarding | NAT Advance |
|--|-----------------|-------------|
| Network Address Translation(NAT) : <input checked="" type="radio"/> Enable <input type="radio"/> Disable | | |
| Max NAT/Firewall Session Per User <input type="text" value="512"/> | | |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | | |

The following table describes the labels in this screen.

Table 44 Network > NAT > General

| LABEL | DESCRIPTION |
|-----------------------------------|---|
| Network Address Translation (NAT) | 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 Enable to activate NAT. Select Disable to turn it off. |
| Max NAT/Firewall Session Per User | Specify the highest number of NAT sessions that the NBG5715 will permit a host to have at one time. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

14.3 The Port Forwarding Screen

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

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

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

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your NBG5715's port forwarding settings, click **Network > NAT > Port Forwarding**. The screen appears as shown.

Note: If you do not assign a **Default Server**, the NBG5715 discards all packets received for ports that are not specified in this screen or remote management.

Refer to [Appendix F on page 247](#) for port numbers commonly used for particular services.

Figure 63 Network > NAT > Port Forwarding

The following table describes the labels in this screen.

Table 45 Network > NAT > Port Forwarding

| LABEL | DESCRIPTION |
|-------------------------|---|
| Default Server Setup | |
| Default Server | 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 Port Forwarding screen. You can decide whether you want to use the default server or specify a server manually. Select this to use the default server. |
| Change to Server | Select this and manually enter the server's IP address. |
| Port Forwarding | |
| Service Name | Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will be displayed in the Port Forwarding Summary section. Otherwise, select User define to manually enter the port number(s) and select the IP protocol. |
| Service Protocol | Select the transport layer protocol supported by this virtual server. Choices are TCP , UDP , or TCP&UDP . If you have chosen a pre-defined service in the Service Name field, the protocol will be configured automatically. |
| Server IP Address | Enter the inside IP address of the virtual server here and click Add to add it in the Port Forwarding Summary section. |
| Port Forwarding Summary | |
| # | This is the number of an individual port forwarding server entry. |
| Status | This icon is turned on when the rule is enabled. |
| Name | This field displays a name to identify this rule. |
| Protocol | This is the transport layer protocol used for the service. |
| Port | This field displays the port number(s). |
| Server IP Address | This field displays the inside IP address of the server. |
| Modify | Click the Edit icon to open the edit screen where you can modify an existing rule. Click the Remove icon to delete a rule. |

Table 45 Network > NAT > Port Forwarding (continued)

| LABEL | DESCRIPTION |
|--------|--|
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

14.3.1 Port Forwarding Edit Screen

This screen lets you create or edit a port forwarding rule. Click the **Add Port Forward** button or a rule's **Edit** icon in the **Port Forwarding** screen to open the following screen.

Figure 64 NAT > Port Forwarding Edit

The following table describes the labels in this screen.

Table 46 NAT > Port Forwarding Edit

| LABEL | DESCRIPTION |
|-------------------|---|
| Port Forwarding | Select Enable to turn on this rule and the requested service can be forwarded to the host with a specified internal IP address. Select Disable to disallow forwarding of these ports to an inside server without having to delete the entry. |
| Service Name | Type a name (of up to 31 printable characters) to identify this rule in the first field next to Service Name . Otherwise, select a predefined service in the second field next to Service Name . The predefined service name and port number(s) will display in the Service Name and Port fields. |
| Protocol | Select the transport layer protocol supported by this virtual server. Choices are TCP, UDP, or TCP&UDP. If you have chosen a pre-defined service in the Service Name field, the protocol will be configured automatically. |
| Port | Type a port number(s) to define the service to be forwarded to the specified server. To specify a range of ports, enter a hyphen (-) between the first port and the last port, such as 10-20. |
| Server IP Address | Type the IP address of the server on your LAN that receives packets from the port(s) specified in the Port field. |
| Back | Click Back to return to the previous screen. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

14.4 The NAT Advance Screen

To change your NBG5715's trigger port settings, click **Network > NAT > NAT Advance**. The screen appears as shown.

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

Figure 65 Network > NAT > NAT Advance

| # | Name | Incoming | | Trigger | |
|----|------|----------|----------|---------|----------|
| | | Port | End Port | Port | End Port |
| 1 | | 0 | 0 | 0 | 0 |
| 2 | | 0 | 0 | 0 | 0 |
| 3 | | 0 | 0 | 0 | 0 |
| 4 | | 0 | 0 | 0 | 0 |
| 5 | | 0 | 0 | 0 | 0 |
| 6 | | 0 | 0 | 0 | 0 |
| 7 | | 0 | 0 | 0 | 0 |
| 8 | | 0 | 0 | 0 | 0 |
| 9 | | 0 | 0 | 0 | 0 |
| 10 | | 0 | 0 | 0 | 0 |
| 11 | | 0 | 0 | 0 | 0 |
| 12 | | 0 | 0 | 0 | 0 |

The following table describes the labels in this screen.

Table 47 Network > NAT > NAT Advance

| LABEL | DESCRIPTION |
|-----------------------|--|
| Port Triggering Rules | |
| # | This is the rule index number (read-only). |
| Name | Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces. |
| Incoming | Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The NBG5715 forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. |
| Port | Type a port number or the starting port number in a range of port numbers. |
| End Port | Type a port number or the ending port number in a range of port numbers. |
| Trigger | The trigger port is a port (or a range of ports) that causes (or triggers) the NBG5715 to record the IP address of the LAN computer that sent the traffic to a server on the WAN. |
| Port | Type a port number or the starting port number in a range of port numbers. |
| End Port | Type a port number or the ending port number in a range of port numbers. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Reset | Click Reset to begin configuring this screen afresh. |

14.5 Technical Reference

The following section contains additional technical information about the NBG5715 features described in this chapter.

14.5.1 NATPort Forwarding: Services and Port Numbers

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

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

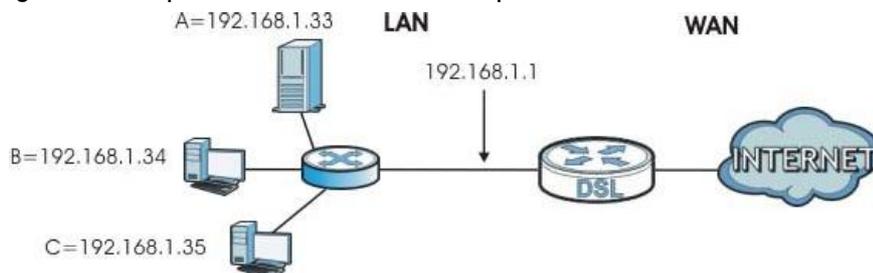
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

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

14.5.2 NAT Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), port 80 to another (B in the example) and assign a default server IP address of 192.168.1.35 to a third (C in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 66 Multiple Servers Behind NAT Example



14.5.3 Trigger Port Forwarding

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN).

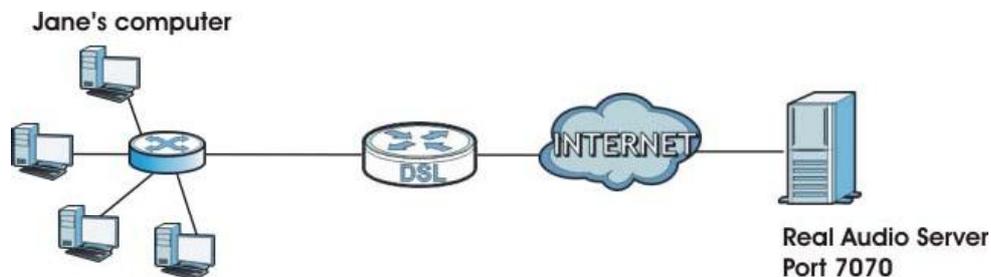
The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The NBG5715 records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the NBG5715's WAN port receives a response with a specific port number and protocol ("incoming" port), the NBG5715 forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

14.5.4 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 67 Trigger Port Forwarding Process: Example



- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the NBG5715 to record Jane's computer IP address. The NBG5715 associates Jane's computer IP address with the "incoming" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The NBG5715 forwards the traffic to Jane's computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The NBG5715 times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

14.5.5 Two Points To Remember About Trigger Ports

- 1 Trigger events only happen on data that is going coming from inside the NBG5715 and going to the outside.
- 2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

Dynamic DNS

15.1 Overview

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

15.1.1 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 FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

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.

15.2 The Dynamic DNS Screen

To change your NBG5715's DDNS, click **Network > DDNS**. The screen appears as shown.

Figure 68 Dynamic DNS

The following table describes the labels in this screen.

Table 48 Dynamic DNS

| LABEL | DESCRIPTION |
|------------------|---|
| Dynamic DNS | Select Enable to use dynamic DNS. Select Disable to turn this feature off. |
| Service Provider | Select the name of your Dynamic DNS service provider. |
| Host Name | Enter a host names in the field provided. You can specify up to two host names in the field separated by a comma (","). |
| Username | Enter your user name. |
| Password | Enter the password assigned to you. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

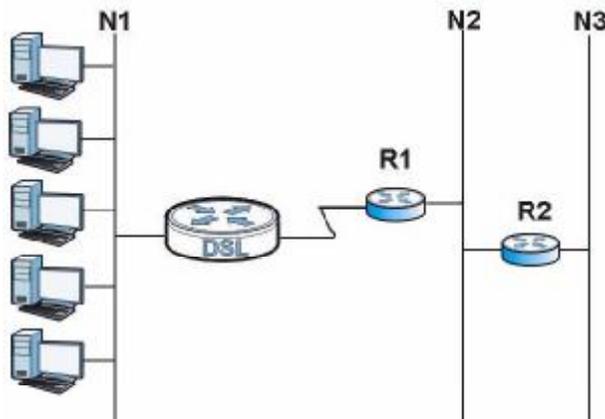
Static Route

16.1 Overview

This chapter shows you how to configure static routes for your NBG5715.

Each remote node specifies only the network to which the gateway is directly connected, and the NBG5715 has no knowledge of the networks beyond. For instance, the NBG5715 knows about network N2 in the following figure through remote node Router 1. However, the NBG5715 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 NBG5715 about the networks beyond the remote nodes.

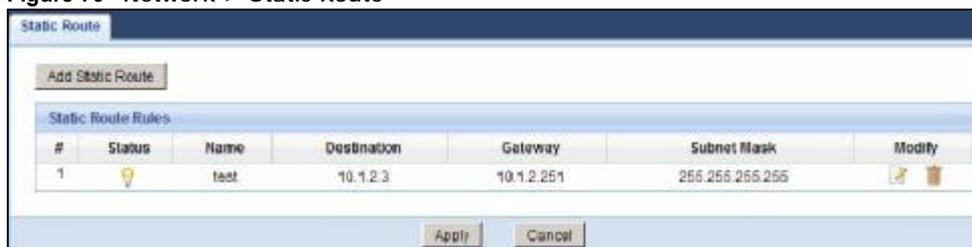
Figure 69 Example of Static Routing Topology



16.2 The Static Route Screen

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

Figure 70 Network > Static Route



The following table describes the labels in this screen.

Table 49 Network > Static Route

| LABEL | DESCRIPTION |
|------------------|--|
| Add Static Route | Click this to create a new rule. |
| # | This is the number of an individual static route. |
| Status | This field indicates whether the rule is active (yellow bulb) or not (gray bulb). |
| Name | This field displays a name to identify this rule. |
| Destination | This parameter specifies the IP network address of the final destination. Routing is always based on network number. |
| Subnet Mask | This parameter specifies the IP network subnet mask of the final destination. |
| 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. |
| Modify | Click the Edit icon to open a screen where you can modify an existing rule. Click the Remove icon to delete a rule from the NBG5715. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

16.2.1 Add/Edit Static Route

Click the **Add Static Route** button or a rule's **Edit** icon in the **Static Route** screen. Use this screen to configure the required information for a static route.

Figure 71 Static Route: Add/Edit

The following table describes the labels in this screen.

Table 50 Static Route: Add/Edit

| LABEL | DESCRIPTION |
|------------------------|---|
| Static Route | Select to enable or disable this rule. |
| Route Name | Type a name to identify this rule. You can use up to 20 printable English keyboard characters, including spaces. |
| Destination IP Address | This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. |
| IP Subnet Mask | Enter the IP subnet mask here. |
| Gateway IP Address | Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your NBG5715's interface(s). The gateway helps forward packets to their destinations. |

Table 50 Static Route: Add/Edit

| LABEL | DESCRIPTION |
|--------|--|
| Back | Click Back to return to the previous screen without saving. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to set every field in this screen to its last-saved value. |

Firewall

17.1 Overview

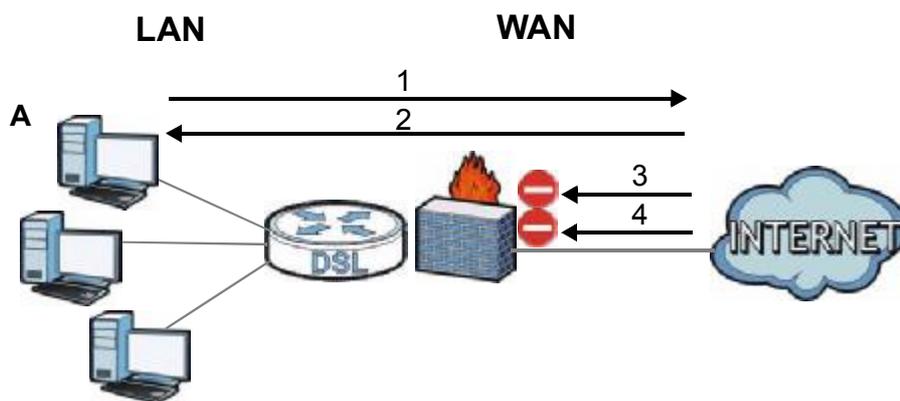
Use these screens to enable and configure the firewall that protects your NBG5715 and your LAN from unwanted or malicious traffic.

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 72 Default Firewall Action



17.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable or disable the NBG5715's firewall ([Section 17.2 on page 121](#)).
- Use the **Services** screen enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them ([Section 17.3 on page 121](#)).

17.1.2 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 NBG5715 Firewall

The NBG5715'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 NBG5715's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG5715 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 NBG5715 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 NBG5715 has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas. The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

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

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.

17.2 The Firewall General Screen

Use this screen to enable or disable the NBG5715's firewall, and set up firewall logs. Click **Security > Firewall** to open the **General** screen.

Figure 73 Security > Firewall > General I



The following table describes the labels in this screen.

Table 51 Security > Firewall > General

| LABEL | DESCRIPTION |
|-----------------|--|
| Enable Firewall | Select this check box to activate the firewall. The NBG5715 performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated. |
| Apply | Click Apply to save the settings. |
| Reset | Click Reset to start configuring this screen again. |

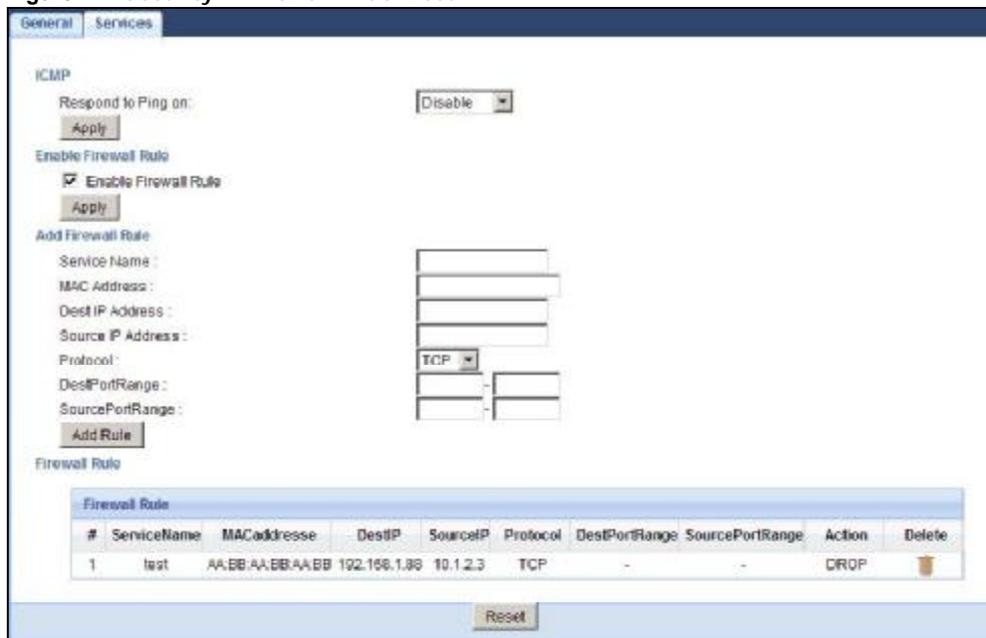
17.3 The Firewall Services Screen

If an outside user attempts to probe an unsupported port on your NBG5715, an ICMP response packet is automatically returned. This allows the outside user to know the NBG5715 exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your NBG5715 when unsupported ports are probed.

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

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

Figure 74 Security > Firewall > Services I



The following table describes the labels in this screen.

Table 52 Security > Firewall > Services

| LABEL | DESCRIPTION |
|----------------------|---|
| 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 NBG5715 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. |
| Enable Firewall Rule | |
| Enable Firewall Rule | Select this check box to activate the firewall rules that you define (see Add Firewall Rule below). |
| Apply | Click Apply to save the settings. |
| Add Firewall Rule | |
| Service Name | Enter a name that identifies or describes the firewall rule. |
| MAC Address | Enter the MAC address of the computer for which the firewall rule applies. |
| Dest IP Address | Enter the IP address of the computer to which traffic for the application or service is entering. The NBG5715 applies the firewall rule to traffic initiating from this computer. |

Table 52 Security > Firewall > Services (continued)

| LABEL | DESCRIPTION |
|-------------------|--|
| Source IP Address | Enter the IP address of the computer that initializes traffic for the application or service. The NBG5715 applies the firewall rule to traffic initiating from this computer. |
| Protocol | Select the protocol (ALL , TCP , UDP or BOTH) used to transport the packets for which you want to apply the firewall rule. |
| Dest Port Range | Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic. |
| Source Port Range | Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic. |
| Add Rule | Click Add to save the firewall rule. |
| Firewall Rule | |
| # | This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. |
| Service Name | This is a name that identifies or describes the firewall rule. |
| MAC address | This is the MAC address of the computer for which the firewall rule applies. |
| Dest IP | This is the IP address of the computer to which traffic for the application or service is entering. |
| Source IP | This is the IP address of the computer from which traffic for the application or service is initialized. |
| Protocol | This is the protocol (ALL , TCP , UDP or BOTH) used to transport the packets for which you want to apply the firewall rule. |
| Dest Port Range | This is the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic. |
| Source Port Range | This is the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic. |
| Action | DROP - Traffic matching the conditions of the firewall rule are stopped. |
| Delete | Click Delete to remove the firewall rule. |
| Reset | Click Reset to start configuring this screen again. |

See [Appendix F on page 247](#) for commonly used services and port numbers.

IPSec VPN

18.1 Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

The following figure provides one perspective of a VPN tunnel.

Figure 75 IPSec VPN: Overview



The VPN tunnel connects the NBG5715 (X) and the remote IPSec router (Y). These routers then connect the local network (A) and remote network (B).

18.2 What You Can Do in this Chapter

- Use the **General** screen to display and manage the NBG5715's VPN rules (tunnels) ([Section 18.4 on page 126](#)).
- Use the **SA Monitor** screen to display and manage active VPN connections ([Section 18.6 on page 139](#)).

18.3 What You Need To Know

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the NBG5715 and the remote IPsec router will use.

The first phase establishes an Internet Key Exchange (IKE) SA between the NBG5715 and remote IPsec router. The second phase uses the IKE SA to securely establish an IPsec SA through which the NBG5715 and remote IPsec router can send data between computers on the local network and remote network. The following figure illustrates this.

Figure 76 VPN: IKE SA and IPsec SA



In this example, a computer in network A is exchanging data with a computer in network B. Inside networks A and B, the data is transmitted the same way data is normally transmitted in the networks. Between routers X and Y, the data is protected by tunneling, encryption, authentication, and other security features of the IPsec SA. The IPsec SA is established securely using the IKE SA that routers X and Y established first.

18.3.1 IKE SA (IKE Phase 1) Overview

The IKE SA provides a secure connection between the NBG5715 and remote IPsec router.

It takes several steps to establish an IKE SA. The negotiation mode determines the number of steps to use. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Both routers must use the same negotiation mode.

These modes are discussed in more detail in [Section 18.7.4 on page 142](#). Main mode is used in various examples in the rest of this section.

IP Addresses of the NBG5715 and Remote IPsec Router

In the NBG5715, you have to specify the IP addresses of the NBG5715 and the remote IPsec router to establish an IKE SA.

You can usually provide a static IP address or a domain name for the NBG5715. Sometimes, your NBG5715 might also offer another alternative, such as using the IP address of a port or interface.

You can usually provide a static IP address or a domain name for the remote IPsec router as well. Sometimes, you might not know the IP address of the remote IPsec router (for example, telecommuters). In this case, you can still set up the IKE SA, but only the remote IPsec router can initiate an IKE SA.

18.3.2 IPsec SA (IKE Phase 2) Overview

Once the NBG5715 and remote IPsec router have established the IKE SA, they can securely negotiate an IPsec SA through which to send data between computers on the networks.

Note: The IPsec SA stays connected even if the underlying IKE SA is not available anymore.

Local Network and Remote Network

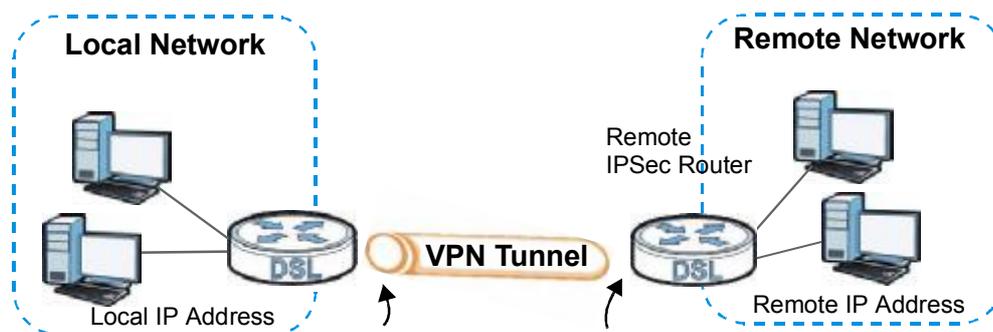
In an IPsec SA, the local network consists of devices connected to the NBG5715 and may be called the local policy. Similarly, the remote network consists of the devices connected to the remote IPsec router and may be called the remote policy.

Note: It is not recommended to set a VPN rule's local and remote network settings both to 0.0.0.0 (any). This causes the NBG5715 to try to forward all access attempts (to the local network, the Internet or even the NBG5715) to the remote IPsec router. In this case, you can no longer manage the NBG5715.

18.4 The General Screen

The following figure helps explain the main fields in the web configurator.

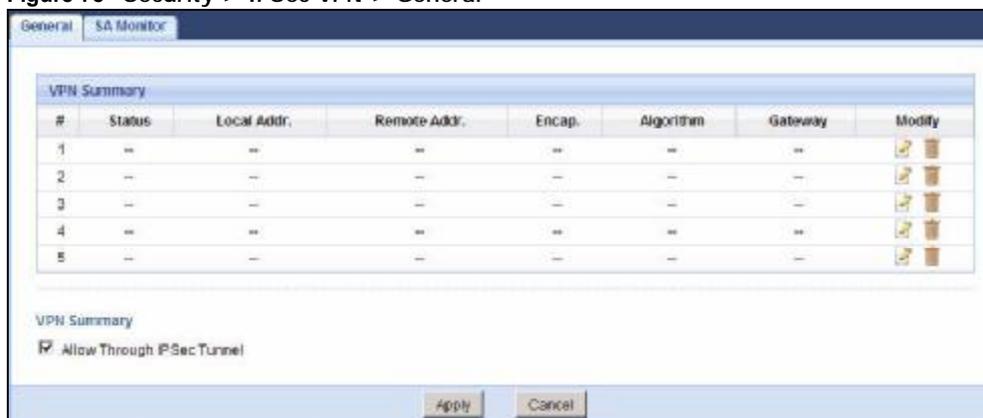
Figure 77 IPsec Fields Summary



Local and remote IP addresses must be static.

Click **Security > IPsec VPN** to display the **Summary** screen. This is a read-only menu of your VPN rules (tunnels). Edit a VPN rule by clicking the **Edit** icon.

Figure 78 Security > IPsec VPN > General



The following table describes the fields in this screen.

Table 53 Security > IPsec VPN > General

| LABEL | DESCRIPTION |
|----------------------------|--|
| # | This is the VPN policy index number. |
| Status | This field displays whether the VPN policy is active or not. This icon is turned on when the rule is enabled. |
| Local Addr. | This displays the beginning and ending (static) IP addresses or a (static) IP address and a subnet mask of computer(s) on your local network behind your NBG5715. |
| Remote Addr. | This displays the beginning and ending (static) IP addresses or a (static) IP address and a subnet mask of computer(s) on the remote network behind the remote IPsec router. This field displays 0.0.0.0 when the Secure Gateway Address field displays 0.0.0.0. In this case only the remote IPsec router can initiate the VPN. |
| Encap. | This field displays Tunnel or Transport mode (Tunnel is the default selection). |
| Algorithm | This field displays the security protocol, encryption algorithm and authentication algorithm used for an SA. |
| Gateway | This is the static WAN IP address or URL of the remote IPsec router. This field displays 0.0.0.0 when you configure the Secure Gateway Address field in the Rule Setup screen to 0.0.0.0. |
| Modify | Click the Edit icon to go to the screen where you can edit the VPN rule. Click the Remove icon to remove an existing VPN rule. |
| Allow Through IPsec Tunnel | Select this check box to send NetBIOS packets through the VPN connection. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

18.5 Edit VPN Rule

Click on a policy's **Edit** icon in the **IPsec VPN > General** screen to edit the VPN policy.

Note: The NBG5715 uses the system default gateway interface's WAN IP address as its WAN IP address to set up a VPN tunnel.

18.5.1 IKEKey Setup

IKE provides more protection so it is generally recommended. You only configure VPN manual key when you select IKE in the IPsec Keying Mode field on the IPsec VPN > General > Edit screen.

Figure 79 Security > IPsec VPN > General > Edit: IKE

| | |
|--|---|
| Property | |
| Property: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| <input type="checkbox"/> Keep Alive | |
| <input type="checkbox"/> NAT Traversal | |
| IPsec Keying Mode: | IKE |
| DNS Server (for IPsec VPN) | 0.0.0.0 |
| Local Policy | |
| Local Address: | 0.0.0.0 |
| Local Address End/Mask: | 255.255.255.0 |
| Remote Policy | |
| Remote Address Start: | 0.0.0.0 |
| Remote Address End/Mask: | 255.255.255.0 |
| Authentication Method | |
| My IP Address: | 0.0.0.0 |
| Local ID Type: | IP |
| Local Content: | |
| Secure Gateway Address: | 0.0.0.0 |
| Peer ID Type: | IP |
| Peer Content: | |
| IPsec Algorithm | |
| Phase 1 | |
| Pre-Shared Key: | |
| Mode: | Main |
| Encryption Algorithm: | DES |
| Authentication Algorithm: | MD5 |
| SA Life Time: | 3600 (seconds) |
| Key Group: | DM1 |
| Phase 2 | |
| Encapsulation Mode: | Tunnel |
| IPsec Protocol: | ESP |
| Encryption Algorithm: | DES |
| Authentication Algorithm: | MD5 |
| SA Life Time: | 3600 (seconds) |
| Key Group: | DM1 |
| <input type="button" value="Back"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

The following table describes the labels in this screen.

Table 54 Security > IPsec VPN > General > Edit: IKE

| LABEL | DESCRIPTION |
|----------------------------|---|
| Property | |
| Propert | Select Enable to activate this VPN policy. |
| Keep Alive | Select this check box to have the NBG5715 automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPsec router must also have keep alive enabled in order for this feature to work. |
| NAT Traversal | Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPsec routers. The remote IPsec router must also have NAT traversal enabled. You can use NAT traversal with ESP protocol using Transport or Tunnel mode, but not with AH protocol nor with manual key management. In order for an IPsec router behind a NAT router to receive an initiating IPsec packet, set the NAT router to forward UDP ports 500 and 4500 to the IPsec router behind the NAT router. |
| IPsec Keying Mode | Select IKE from the drop-down list box. IKE provides more protection so it is generally recommended. |
| DNS Server (for IPsec VPN) | If there is a private DNS server that services the VPN, type its IP address here. The NBG5715 assigns this additional DNS server to the NBG5715's DHCP clients that have IP addresses in this IPsec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names. |
| Local Policy | Local IP addresses must be static and correspond to the remote IPsec router's configured remote IP addresses. Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. In order to have more than one active rule with the Secure Gateway Address field set to 0.0.0.0 , the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with 0.0.0.0 in the Secure Gateway Address field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the Secure Gateway Address field set to 0.0.0.0 . |
| Local Address | For a single IP address, enter a (static) IP address on the LAN behind your NBG5715. For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on your LAN behind your NBG5715. To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the LAN behind your NBG5715. |
| Local Address End /Mask | When the local IP address is a single address, type it a second time here. When the local IP address is a range, enter the end (static) IP address, in a range of computers on the LAN behind your NBG5715. When the local IP address is a subnet address, enter a subnet mask on the LAN behind your NBG5715. |

Table 54 Security > IPsec VPN > General > Edit: IKE (continued)

| LABEL | DESCRIPTION |
|------------------------------|---|
| Remote Policy | <p>Remote IP addresses must be static and correspond to the remote IPsec router's configured local IP addresses. The remote fields do not apply when the Secure Gateway IP Address field is configured to 0.0.0.0. In this case only the remote IPsec router can initiate the VPN.</p> <p>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p> |
| Remote Address Start | <p>For a single IP address, enter a (static) IP address on the network behind the remote IPsec router.</p> <p>For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPsec router.</p> <p>To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the network behind the remote IPsec router.</p> |
| Remote Address End /Mask | <p>When the remote IP address is a single address, type it a second time here.</p> <p>When the remote IP address is a range, enter the end (static) IP address, in a range of computers on the network behind the remote IPsec router.</p> <p>When the remote IP address is a subnet address, enter a subnet mask on the network behind the remote IPsec router.</p> |
| Authentication Method | |
| My IP Address | <p>Enter the NBG5715's static WAN IP address (if it has one) or leave the field set to 0.0.0.0.</p> <p>The NBG5715 uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as 0.0.0.0. If the WAN connection goes down, the NBG5715 uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect.</p> <p>Otherwise, you can enter one of the dynamic domain names that you have configured (in the DDNS screen) to have the NBG5715 use that dynamic domain name's IP address.</p> <p>The VPN tunnel has to be rebuilt if My IP Address changes after setup.</p> |
| Local ID Type | <p>Select IP to identify this NBG5715 by its IP address.</p> <p>Select Domain Name to identify this NBG5715 by a domain name.</p> <p>Select E-mail to identify this NBG5715 by an e-mail address.</p> |

Table 54 Security > IPsec VPN > General > Edit: IKE (continued)

| LABEL | DESCRIPTION |
|------------------------|---|
| Local Content | <p>When you select IP in the Local ID Type field, type the IP address of your computer in the Local Content field. The NBG5715 automatically uses the IP address in the My IP Address field (refer to the My IP Address field description) if you configure the Local Content field to 0.0.0.0 or leave it blank.</p> <p>It is recommended that you type an IP address other than 0.0.0.0 in the Local Content field or use the Domain Name or E-mail ID type in the following situations.</p> <p>When there is a NAT router between the two IPsec routers.</p> <p>When you want the remote IPsec router to be able to distinguish between VPN connection requests that come in from IPsec routers with dynamic WAN IP addresses.</p> <p>When you select Domain Name or E-mail in the Local ID Type field, type a domain name or e-mail address by which to identify this NBG5715 in the Local Content field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.</p> |
| Secure Gateway Address | <p>Type the WAN IP address or the domain name (up to 31 characters) of the IPsec router with which you're making the VPN connection. Set this field to 0.0.0.0 if the remote IPsec router has a dynamic WAN IP address (the IPsec Keying Mode field must be set to IKE).</p> <p>In order to have more than one active rule with the Secure Gateway Address field set to 0.0.0.0, the ranges of the local IP addresses cannot overlap between rules.</p> <p>If you configure an active rule with 0.0.0.0 in the Secure Gateway Address field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the Secure Gateway Address field set to 0.0.0.0.</p> <p>You can also enter a remote secure gateway's domain name in the Secure Gateway Address field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The NBG5715 has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).</p> |
| Peer ID Type | <p>Select IP to identify the remote IPsec router by its IP address.</p> <p>Select Domain Name to identify the remote IPsec router by a domain name.</p> <p>Select E-mail to identify the remote IPsec router by an e-mail address.</p> |

Table 54 Security > IPsec VPN > General > Edit: IKE (continued)

| LABEL | DESCRIPTION |
|--------------------------|---|
| Peer Content | <p>The configuration of the peer content depends on the peer ID type.</p> <p>For IP, type the IP address of the computer with which you will make the VPN connection. If you configure this field to 0.0.0.0 or leave it blank, the NBG5715 will use the address in the Secure Gateway Address field (refer to the Secure Gateway Address field description).</p> <p>For Domain Name or E-mail, type a domain name or e-mail address by which to identify the remote IPsec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.</p> <p>It is recommended that you type an IP address other than 0.0.0.0 or use the Domain Name or E-mail ID type in the following situations:</p> <p>When there is a NAT router between the two IPsec routers.</p> <p>When you want the NBG5715 to distinguish between VPN connection requests that come in from remote IPsec routers with dynamic WAN IP addresses.</p> |
| IPsec Algorithm | |
| Phase 1 | |
| Pre-Shared Key | <p>Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.</p> <p>Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself.</p> <p>Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.</p> |
| Mode | Select Main or Aggressive from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode. |
| Encryption Algorithm | <p>Select which key size and encryption algorithm to use for data communications. Choices are:</p> <p>DES - a 56-bit key with the DES encryption algorithm</p> <p>3DES - a 168-bit key with the DES encryption algorithm</p> <p>The NBG5715 and the remote IPsec router must use the same algorithms and key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. Longer keys require more processing power, resulting in increased latency and decreased throughput.</p> |
| Authentication Algorithm | Select which hash algorithm to use to authenticate packet data. Choices are SHA1 and MD5 . SHA1 is generally considered stronger than MD5 , but it is also slower. |
| SA Life Time | <p>Define the length of time before an IKE or IPsec SA automatically renegotiates in this field. It may range from 1 to 2,000,000,000 seconds.</p> <p>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.</p> |

Table 54 Security > IPsec VPN > General > Edit: IKE (continued)

| LABEL | DESCRIPTION |
|--------------------------|--|
| Key Group | You must choose a key group for phase 1 IKE setup. DH1 refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. |
| Phase 2 | |
| Encapsulation Mode | Select Tunnel mode or Transport mode from the drop-down list box. |
| IPsec Protocol | Select the security protocols used for an SA. Both AH and ESP increase processing requirements and communications latency (delay). If you select ESP here, you must select options from the Encryption Algorithm and Authentication Algorithm fields (described below). |
| Encryption Algorithm | Select which key size and encryption algorithm to use for data communications. Choices are: DES - a 56-bit key with the DES encryption algorithm 3DES - a 168-bit key with the DES encryption algorithm The NBG5715 and the remote IPsec router must use the same algorithms and key , which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. Longer keys require more processing power, resulting in increased latency and decreased throughput. |
| Authentication Algorithm | Select which hash algorithm to use to authenticate packet data. Choices are SHA1 and MD5 . SHA1 is generally considered stronger than MD5 , but it is also slower. |
| SA Life Time | Define the length of time before an IKE or IPsec SA automatically renegotiates in this field. It may range from 1 to 2,000,000,000 seconds. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| Key Group | You must choose a key group for phase 1 IKE setup. DH1 refers to Diffie-Hellman Group 1 a 768 bit random number. DH2 refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. |
| Back | Click Back to return to the previous screen. |
| Apply | Click Apply to save your changes back to the NBG5715 . |
| Cancel | Click Cancel to restore your previous settings. |

18.5.2 Manual Key Setup

Manual key management is useful if you have problems with IKE key management.

18.5.2.1 Security Parameter Index (SPI)

An SPI is used to distinguish different SAs terminating at the same destination and using the same IPsec protocol. This data allows for the multiplexing of SAs to a single gateway. The **SPI** (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association (SA). The **SPI** is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

18.5.2.2 IPsec SA Using Manual Keys

You might set up an IPsec SA using manual keys when you want to establish a VPN tunnel quickly, for example, for troubleshooting. You should only do this as a temporary solution, however, because it is not as secure as a regular IPsec SA.

In IPsec SAs using manual keys, the NBG5715 and remote IPsec router do not establish an IKE SA. They only establish an IPsec SA. As a result, an IPsec SA using manual keys has some characteristics of IKE SA and some characteristics of IPsec SA. There are also some differences between IPsec SA using manual keys and other types of SA.

18.5.2.3 IPsec SA Proposal Using Manual Keys

In IPsec SA using manual keys, you can only specify one encryption algorithm and one authentication algorithm. There is no DH key exchange, so you have to provide the encryption key and the authentication key the NBG5715 and remote IPsec router use.

Note: The NBG5715 and remote IPsec router must use the same encryption key and authentication key.

18.5.3 Configuring Manual Key

You only configure VPN manual key when you select **Manual** in the **IPsec Keying Mode** field on the **IPsec VPN > General > Edit** screen.

Figure 80 Security > IPsec VPN > General > Edit: Manual

The screenshot shows the configuration interface for an IPsec VPN policy. It is divided into several sections:

- Property:** Includes radio buttons for 'Enable' and 'Disable', and a dropdown menu for 'IPsec Keying Mode' set to 'Manual'.
- DNS Server (for IPsec VPN):** A text input field containing '0.0.0.0'.
- Local Policy:** Includes 'Local Address' (0.0.0.0) and 'Local Address End/Mask' (255.255.255.0).
- Remote Policy:** Includes 'Remote Address Start' (0.0.0.0) and 'Remote Address End/Mask' (255.255.255.0).
- Authentication Method:** Includes 'My IP Address' (0.0.0.0) and 'Secure Gateway Address' (0.0.0.0).
- IPsec Algorithm:** Includes 'SPI' (101), 'Encryption Algorithm' (DES), 'Encryption Key' (Hex), 'Authentication Algorithms' (MD5), 'Authentication Key' (Hex), 'Encapsulation Mode' (Tunnel), and 'IPsec Protocol' (ESP).

At the bottom, there are 'Back', 'Apply', and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 55 Security > IPsec VPN > General > Edit: Manual

| LABEL | DESCRIPTION |
|----------------------------|--|
| Property | |
| Property | Select Enable to activate this VPN policy. |
| IPsec Keying Mode | Select Manual from the drop-down list box. Manual is a useful option for troubleshooting if you have problems using IKE key management. |
| DNS Server (for IPsec VPN) | If there is a private DNS server that services the VPN, type its IP address here. The NBG5715 assigns this additional DNS server to the NBG5715's DHCP clients that have IP addresses in this IPsec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names. |

Table 55 Security > IPSec VPN > General > Edit: Manual (continued)

| LABEL | DESCRIPTION |
|--------------------------|---|
| Local Policy | <p>Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses.</p> <p>Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p> <p>In order to have more than one active rule with the Secure Gateway Address field set to 0.0.0.0, the ranges of the local IP addresses cannot overlap between rules.</p> <p>If you configure an active rule with 0.0.0.0 in the Secure Gateway Address field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the Secure Gateway Address field set to 0.0.0.0.</p> |
| Local Address | <p>For a single IP address, enter a (static) IP address on the LAN behind your NBG5715.</p> <p>For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on your LAN behind your NBG5715.</p> <p>To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the LAN behind your NBG5715.</p> |
| Local Address End /Mask | <p>When the local IP address is a single address, type it a second time here.</p> <p>When the local IP address is a range, enter the end (static) IP address, in a range of computers on the LAN behind your NBG5715.</p> <p>When the local IP address is a subnet address, enter a subnet mask on the LAN behind your NBG5715.</p> |
| Remote Policy | <p>Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the Secure Gateway IP Address field is configured to 0.0.0.0. In this case only the remote IPSec router can initiate the VPN.</p> <p>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p> |
| Remote Address Start | <p>For a single IP address, enter a (static) IP address on the network behind the remote IPSec router.</p> <p>For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router.</p> <p>To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the network behind the remote IPSec router.</p> |
| Remote Address End /Mask | <p>When the remote IP address is a single address, type it a second time here.</p> <p>When the remote IP address is a range, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router.</p> <p>When the remote IP address is a subnet address, enter a subnet mask on the network behind the remote IPSec router.</p> |
| Authentication Method | |

Table 55 Security > IPSec VPN > General > Edit: Manual (continued)

| LABEL | DESCRIPTION |
|--------------------------|--|
| My IP Address | <p>Enter the NBG5715's static WAN IP address (if it has one) or leave the field set to 0.0.0.0.</p> <p>The NBG5715 uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as 0.0.0.0. If the WAN connection goes down, the NBG5715 uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect.</p> <p>Otherwise, you can enter one of the dynamic domain names that you have configured (in the DDNS screen) to have the NBG5715 use that dynamic domain name's IP address.</p> <p>The VPN tunnel has to be rebuilt if My IP Address changes after setup.</p> |
| Secure Gateway Address | <p>Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address (the IPSec Keying Mode field must be set to IKE).</p> <p>In order to have more than one active rule with the Secure Gateway Address field set to 0.0.0.0, the ranges of the local IP addresses cannot overlap between rules.</p> <p>If you configure an active rule with 0.0.0.0 in the Secure Gateway Address field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the Secure Gateway Address field set to 0.0.0.0.</p> <p>You can also enter a remote secure gateway's domain name in the Secure Gateway Address field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The NBG5715 has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).</p> |
| IPSec Algorithm | |
| SPI | Type a unique SPI (Security Parameter Index) from one to four characters long. Valid Characters are "0, 1, 2, 3, 4, 5, 6, 7, 8, and 9". |
| Encryption Algorithm | <p>Select which key size and encryption algorithm to use in the IKE SA. Choices are:</p> <p>DES - a 56-bit key with the DES encryption algorithm</p> <p>3DES - a 168-bit key with the DES encryption algorithm</p> <p>The NBG5715 and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.</p> |
| Encryption Key | <p>This field is applicable when you select ESP in the IPSec Protocol field above.</p> <p>With DES, type a unique key 8 characters long. With 3DES, type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.</p> |
| Authentication Algorithm | Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are SHA1 and MD5 . SHA1 is generally considered stronger than MD5 , but it is also slower. |
| Authentication Key | Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for MD5 authentication or 20 characters for SHA-1 authentication. Any characters may be used, including spaces, but trailing spaces are truncated. |
| Encapsulation Mode | Select Tunnel mode or Transport mode from the drop-down list box. |

Table 55 Security > IPsec VPN > General > Edit: Manual (continued)

| LABEL | DESCRIPTION |
|----------------|---|
| IPsec Protocol | Select the security protocols used for an SA. Both AH and ESP increase processing requirements and communications latency (delay). If you select ESP here, you must select options from the Encryption Algorithm and Authentication Algorithm fields (described below). |
| Back | Click Back to return to the previous screen. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to restore your previous settings. |

18.6 The SA Monitor Screen

In the Web Configurator, click **Security > IPsec VPN > SA Monitor**. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections.

Figure 81 Security > IPsec VPN > SA Monitor

The following table describes the labels in this screen.

Table 56 Security > VPN > SA Monitor

| LABEL | DESCRIPTION |
|-----------------|---|
| Status | This field displays whether the VPN connection is up (yellow bulb) or down (gray bulb). |
| Connection Name | This field displays the identification name for this VPN policy. |
| Remote Gateway | This is the static WAN IP address or URL of the remote IPsec router. |
| Local Address | This is the IP address of computer(s) on your local network behind your NBG5715. |
| Remote Address | This is the IP address of computer(s) on the remote network behind the remote IPsec router. |
| Refresh | Click Refresh to display the current active VPN connection(s). |

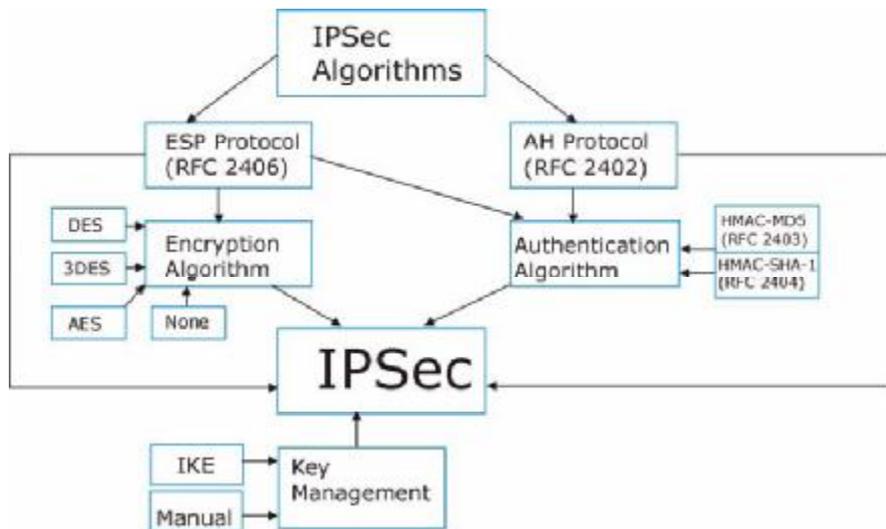
18.7 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

18.7.1 IPsec Architecture

The overall IPsec architecture is shown as follows.

Figure 82 IPsec Architecture



IPsec Algorithms

The ESP (Encapsulating Security Payload) Protocol (RFC 2406) and AH (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404), provide an authentication mechanism for the AH and ESP protocols.

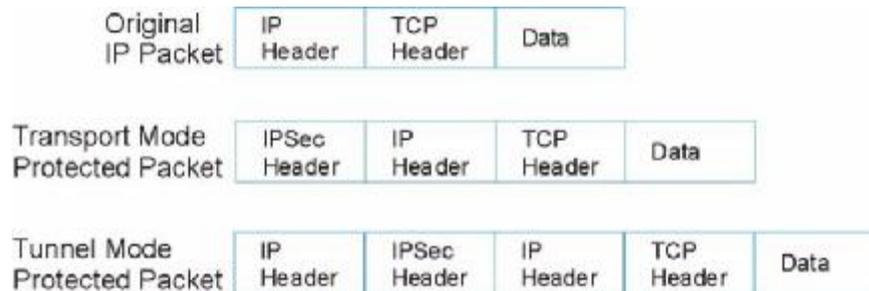
Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

18.7.2 Encapsulation

The two modes of operation for IPSec VPNs are **Transport mode** and **Tunnel mode**. At the time of writing, the NBG5715 supports **Tunnel mode** only.

Figure 83 Transport and Tunnel Mode IPSec Encapsulation



Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport mode**, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP**, protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

Tunnel Mode

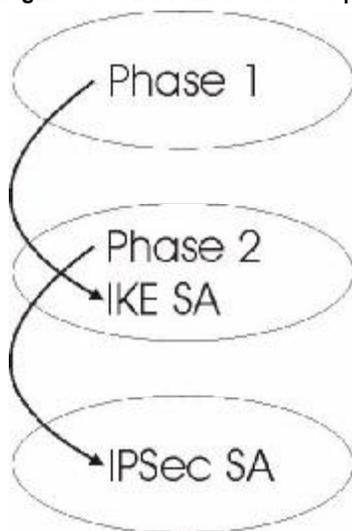
Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel mode** is required for gateway services to provide access to internal systems. **Tunnel mode** is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel mode** is required for gateway to gateway and host to gateway communications. **Tunnel mode** communications have two sets of IP headers:

- **Outside header:** The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header:** The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

18.7.3 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 84 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (DH1 or DH2).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The NBG5715 automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

18.7.4 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not known by the responder and both parties want to use pre-shared key authentication.

18.7.5 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the NBG5715.

NAT is incompatible with the AH protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using AH protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode ESP with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode ESP with authentication is not compatible with NAT.

Table 57 VPN and NAT

| SECURITY PROTOCOL | MODE | NAT |
|-------------------|-----------|-----|
| AH | Transport | N |
| AH | Tunnel | N |
| ESP | Transport | N |
| ESP | Tunnel | Y |

18.7.6 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both **transport** and **tunnel** mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the NBG5715's **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPsec routers.

Figure 85 NAT Router Between IPsec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPsec routers because the NAT router changes the header of the IPsec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPsec packet. The NAT router forwards the IPsec packet with the UDP port 500 header unchanged. In the above figure, when IPsec router A tries to establish an IKE SA, IPsec router B checks the UDP port 500 header, and IPsec routers A and B build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPsec endpoints.
- Set the NAT router to forward UDP port 500 to IPsec router A.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

Table 58 VPN and NAT

| SECURITY PROTOCOL | MODE | NAT |
|-------------------|-----------|-----|
| AH | Transport | N |
| AH | Tunnel | N |
| ESP | Transport | Y* |
| ESP | Tunnel | Y |

Y* - This is supported in the NBG5715 if you enable NAT traversal.

18.7.7 ID Type and Content

With aggressive negotiation mode (see [Section 18.7.4 on page 142](#)), the NBG5715 identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the NBG5715 to distinguish between multiple rules for SAs that connect from remote IPsec routers that have dynamic WAN IP addresses.

Regardless of the ID type and content configuration, the NBG5715 does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see [Section 18.7.4 on page 142](#)), the ID type and content are encrypted to provide identity protection. In this case the NBG5715 can only distinguish between up to 12 different incoming SAs that connect from remote IPsec routers that have dynamic WAN IP

addresses. The NBG5715 can distinguish up to 48 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and eight key groups when you configure a VPN rule (see [Section 18.4 on page 126](#)). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 59 Local ID Type and Content Fields

| LOCAL ID TYPE= | CONTENT= |
|----------------|--|
| IP | Type the IP address of your computer. |
| DNS | Type a domain name (up to 31 characters) by which to identify this NBG5715. |
| E-mail | Type an e-mail address (up to 31 characters) by which to identify this NBG5715. |
| | The domain name or e-mail address that you use in the Local ID Content field is used for identification purposes only and does not need to be a real domain name or e-mail address. |

18.7.7.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two NBG5715s in this example can complete negotiation and establish a VPN tunnel.

Table 60 Matching ID Type and Content Configuration Example

| NBG5715 A | NBG5715 B |
|--|---|
| Local ID type: E-mail | Local ID type: IP |
| Local ID content: <u>tom@yourcompany.com</u> | Local ID content: 1.1.1.2 |
| Remote ID type: IP | Remote ID type: E-mail |
| Remote ID content: 1.1.1.2 | Remote ID content: <u>tom@yourcompany.com</u> |

The two NBG5715s in this example cannot complete their negotiation because NBG5715 B's **Local ID type** is IP, but NBG5715 A's **Remote ID type** is set to E-mail. An "ID mismatched" message displays in the IPSEC LOG.

Table 61 Mismatching ID Type and Content Configuration Example

| NBG5715 A | NBG5715 B |
|--|----------------------------|
| Local ID type: IP | Local ID type: IP |
| Local ID content: 1.1.1.10 | Local ID content: 1.1.1.2 |
| Remote ID type: E-mail | Remote ID type: IP |
| Remote ID content: <u>aa@yahoo.com</u> | Remote ID content: 1.1.1.0 |

18.7.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see [Section 18.7.3 on page 142](#) for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

18.7.9 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit, 1024-bit, 1536-bit, 2048-bit, and 3072-bit Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

Bandwidth Management

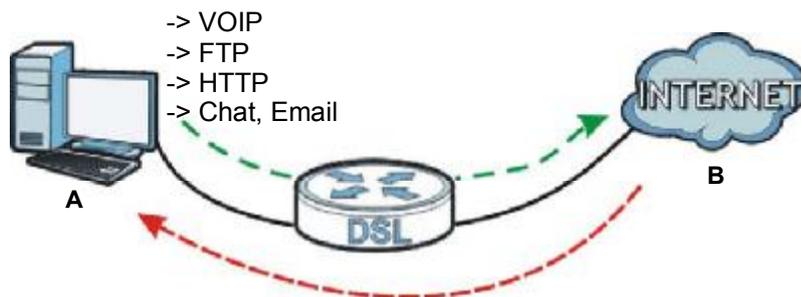
19.1 Overview

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

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

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

Figure 86 Bandwidth Management Example



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

19.2 What You Can Do this Chapter

- Use the **General** screen to enable bandwidth management ([Section 19.4 on page 148](#)).
- Use the **Advanced** screen to configure bandwidth managements rule for the pre-defined services and applications ([Section 19.5 on page 148](#)).

19.3 What You Need To Know

The sum of the bandwidth allotments that apply to the WAN interface (LAN to WAN, WLAN to WAN) must be less than or equal to the **Upstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen ([Section 19.5 on page 148](#)).

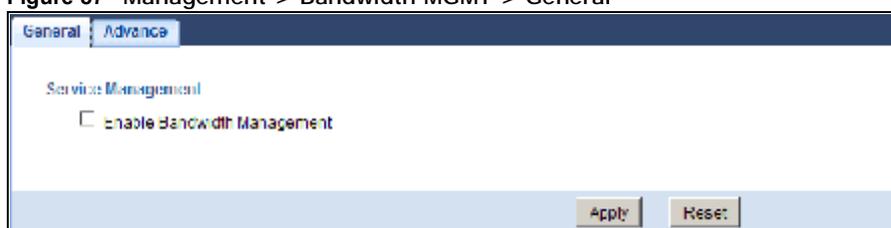
The sum of the bandwidth allotments that apply to the LAN interface (WAN to LAN, WAN to WLAN) must be less than or equal to the **Downstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen [Section 19.5 on page 148](#).

19.4 General Screen

Use this screen to have the NBG5715 apply bandwidth management.

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

Figure 87 Management > Bandwidth MGMT > General



The following table describes the labels in this screen.

Table 62 Management > Bandwidth MGMT > General

| LABEL | DESCRIPTION |
|-----------------------------|---|
| Enable Bandwidth Management | This field allows you to have NBG5715 apply bandwidth management. Enable bandwidth management to give traffic that matches a bandwidth rule priority over traffic that does not match a bandwidth rule. 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. |
| Apply | Click Apply to save your customized settings. |
| Reset | Click Reset to begin configuring this screen afresh. |

19.5 Advance Screen

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

You can also use this screen to configure bandwidth management rule for other services or applications that are not on the pre-defined list of NBG5715. Additionally, you can define the source and destination IP addresses and port for a service or application.

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

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

Figure 88 Management > Bandwidth MGMT > Advance

The following table describes the labels in this screen.

Table 63 Management > Bandwidth MGMT > Advance

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

Table 63 Management > Bandwidth MGMT > Advance (continued)

| LABEL | DESCRIPTION |
|----------------------|--|
| Priority | Select a priority from the drop down list box. The lower the number, the higher the priority. <ul style="list-style-type: none"> Select higher priority for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay). Select medium priority for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay. Select lower priority for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users. |
| Category | This is the category where a service belongs. |
| Service | This is the name of the service. Select the check box to have the NBG5715 apply this bandwidth management rule. |
| User-defined Service | |
| User-defined Service | Use this table to allocate specific amounts of bandwidth to specific applications or services you specify. |
| # | This is the number of an individual bandwidth management rule. |
| Enable | Select this check box to have the NBG5715 apply this bandwidth management rule. |
| Direction | From WAN applies bandwidth management to traffic from LAN/WLAN to WAN (i.e., uplink). From LAN&WLAN applies bandwidth management to traffic that the NBG5715 forwards to both the LAN and the WLAN. |
| Service Name | Enter a descriptive name for the bandwidth management rule. |
| Category | Select a the category where a service belongs. |
| Modify | Click the Edit icon to open the Rule Configuration screen. Modify an existing rule or create a new rule in the Rule Configuration screen. See Section 19.5.1 on page 151 for more information. Click the Remove icon to delete a rule. |
| Direction | Select To LAN&WLAN to apply bandwidth management to traffic from WAN to LAN and WLAN. Select To WAN to apply bandwidth management to traffic from LAN/WLAN to WAN. |
| Service Name | Enter a descriptive name for the bandwidth management rule. |
| Category | This is the category where a service belongs. |
| Modify | Click the Edit icon to open the Rule Configuration screen. Modify an existing rule or create a new rule in the Rule Configuration screen. See Section 19.5.1 on page 151 for more information. Click the Remove icon to delete a rule. |
| Apply | Click Apply to save your customized settings. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

19.5.1 Rule Configuration: User Defined Service Rule Configuration

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

Figure 89 Bandwidth MGMT Rule Configuration: User-defined Service

The following table describes the labels in this screen.

Table 64 Bandwidth MGMT Rule Configuration: User-defined Service

| LABEL | DESCRIPTION |
|----------------------------|--|
| Destination Address | Enter the IP address of the destination computer. The NBG5715 applies bandwidth management to the service or application that is entering this computer. |
| Destination Subnet Netmask | Enter the subnet netmask of the destination of the traffic for which the bandwidth management rule applies. |
| Destination Port | This is the port number of the destination that define the traffic type, for example TCP port 80 defines web traffic. |
| Source Address | Enter the IP address of the computer that initializes traffic for the application or service. The NBG5715 applies bandwidth management to traffic initiating from this computer. |
| Source Subnet Netmask | Enter the subnet netmask of the computer initiating the traffic for which the bandwidth management rule applies. |
| Source Port | This is the port number of the source that define the traffic type, for example TCP port 80 defines web traffic. |
| Protocol | Select the protocol (TCP, UDP) for which the bandwidth management rule applies. |
| Apply | Click Apply to save your customized settings. |
| Cancel | Click Cancel to exit this screen without saving. |

See [Appendix F on page 247](#) for commonly used services and port numbers

Remote Management

20.1 Overview

This chapter provides information on the Remote Management screens.

Remote Management allows you to manage your NBG5715 from a remote location through the following interfaces:

- LAN and WAN
- LAN only
- WAN only

Note: The NBG5715 is managed using the Web Configurator.

20.2 What You Can Do in this Chapter

- Use the **WWW** screen to define the interface/s from which the NBG5715 can be managed remotely using the web and specify a secure client that can manage the NBG5715 ([Section 20.4 on page 153](#)) .
- Use the **TELNET** screen to define the interface/s from which the NBG5715 can be managed remotely using Telnet service and specify a secure client that can manage the NBG5715 ([Section 20.5 on page 154](#)).

20.3 What You Need to Know

Remote management over LAN or WAN will not work when:

- 1 The IP address in the **Secured Client IP Address** field ([Section 20.4 on page 153](#)) does not match the client IP address. If it does not match, the NBG5715 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.

20.3.1 Remote Management and NAT

When NAT is enabled:

- Use the NBG5715's WAN IP address when configuring from the WAN.
- Use the NBG5715's LAN IP address when configuring from the LAN.

20.3.2 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The NBG5715 automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the System screen

20.4 WWW Screen

To change your NBG5715's remote management settings, click **Management > Remote MGMT** to open the **WWW** screen.

Figure 90 Management > Remote MGMT > WWW

The following table describes the labels in this screen.

Table 65 Management > Remote MGMT > WWW

| LABEL | DESCRIPTION |
|---------------------------|---|
| 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. |
| Access Status | Select the interface(s) through which a computer may access the NBG5715 using this service. |
| Secured Client IP Address | Select All to allow all computers to access the NBG5715. Otherwise, check Selected and specify the IP address of the computer that can access the NBG5715. |
| Apply | Click Apply to save your customized settings and exit this screen. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

20.5 Telnet Screen

To change your NBG5715's remote management settings, click **Management > Remote MGMT > Telnet** to open the Telnet screen.

Figure 91 Management > Remote MGMT > Telnet

The screenshot shows the 'Telnet' configuration page. At the top, there are tabs for 'WWW' and 'Telnet'. The 'Port' field is set to '23'. The 'Access Status' dropdown menu is set to 'LAN & WAN'. Under 'Secured Client IP Address', the 'All' radio button is selected, and the 'Selected' radio button is unselected. Below these fields is a 'Note' box with a blue icon and text: 'You may also need to create a [Firewall](#) rule'. At the bottom of the page, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 66 Management > Remote MGMT > Telnet

| LABEL | DESCRIPTION |
|---------------------------|---|
| 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. |
| Access Status | Select the interface(s) through which a computer may access the NBG5715 using this service. |
| Secured Client IP Address | Select All to allow all computers to access the NBG5715. Otherwise, check Selected and specify the IP address of the computer that can access the NBG5715. |
| Apply | Click Apply to save your customized settings and exit this screen. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

Universal Plug-and-Play (UPnP)

21.1 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.

21.2 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.

21.2.1 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.

21.2.2 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 NBG5715 allows multicast messages on the LAN only.

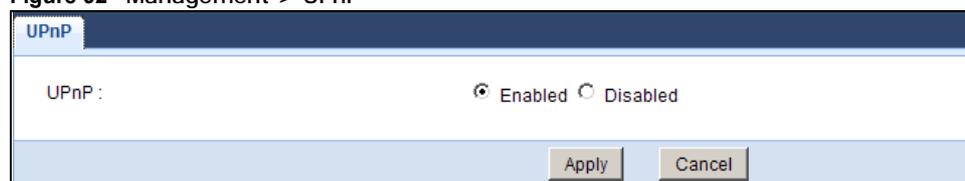
All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

21.3 UPnP Screen

Use this screen to enable UPnP on your NBG5715.

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

Figure 92 Management > UPnP



The following table describes the fields in this screen.

Table 67 Management > UPnP

| LABEL | DESCRIPTION |
|--------|---|
| UPnP | Select Enable to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the NBG5715's IP address (although you must still enter the password to access the web configurator). |
| Apply | Click Apply to save the setting to the NBG5715. |
| Cancel | Click Cancel to return to the previously saved settings. |

21.4 Technical Reference

The sections show examples of using UPnP.

21.4.1 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 NBG5715.

Make sure the computer is connected to a LAN port of the NBG5715. Turn on your computer and the NBG5715.

21.4.1.1 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 93 Network Connections



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

Figure 94 Internet Connection Properties



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

Figure 95 Internet Connection Properties: Advanced Settings

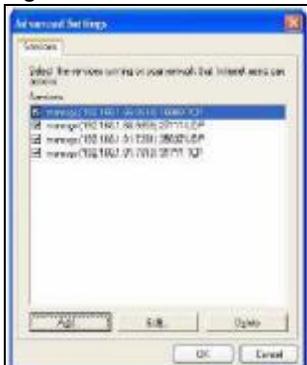


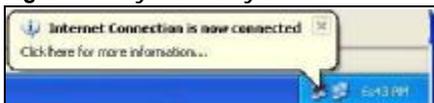
Figure 96 Internet Connection Properties: Advanced Settings: Add



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

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

Figure 97 System Tray Icon



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

Figure 98 Internet Connection Status



21.4.2 Web Configurator Easy Access

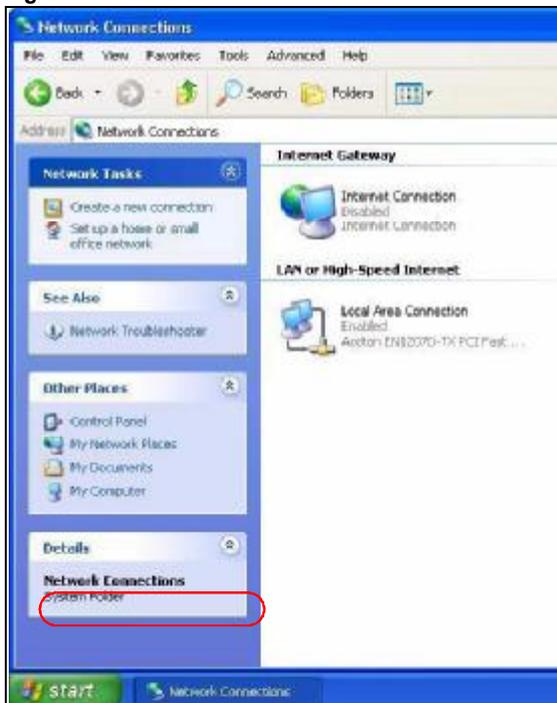
With UPnP, you can access the web-based configurator on the NBG5715 without finding out the IP address of the NBG5715 first. This comes helpful if you do not know the IP address of the NBG5715.

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 99 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 NBG5715 and select Invoke. The web configurator login screen displays.

Figure 100 Network Connections: My Network Places



- 6 Right-click on the icon for your NBG5715 and select **Properties**. A properties window displays with basic information about the NBG5715.

Figure 101 Network Connections: My Network Places: Properties: Example



Maintenance

22.1 Overview

This chapter provides information on the Maintenance screens.

22.2 What You Can Do in this Chapter

- Use the **General** screen to set the timeout period of the management session ([Section 22.3 on page 163](#)).
- Use the **Password** screen to change your NBG5715's system password ([Section 22.4 on page 164](#)).
- Use the **Time** screen to change your NBG5715's time and date ([Section 22.5 on page 165](#)).
- Use the **Firmware Upgrade** screen to upload firmware to your NBG5715 ([Section 22.6 on page 166](#)).
- Use the **Backup/Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration ([Section 22.7 on page 167](#)).
- Use the **Language** screen to change the language for the Web Configurator ([Section 22.8 on page 169](#)).

22.3 General Screen

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

Figure 102 Maintenance > General

The screenshot shows a web interface for the 'General' maintenance screen. It has a title bar 'General' and three input fields: 'System Name' with the value 'OpenWrt', 'Domain Name' with the value 'zyxel.com', and 'Administrator Inactivity Timer' with the value '60' and a note '(minutes, 0 means no timeout)'. At the bottom, there are 'Apply' and 'Cancel' buttons.

| | |
|----------------------------------|---|
| System Name : | <input type="text" value="OpenWrt"/> |
| Domain Name : | <input type="text" value="zyxel.com"/> |
| Administrator Inactivity Timer : | <input type="text" value="60"/> (minutes, 0 means no timeout) |

The following table describes the labels in this screen.

Table 68 Maintenance > General

| LABEL | DESCRIPTION |
|--------------------------------|---|
| System Name | System Name is a unique name to identify the NBG5715 in an Ethernet network. |
| Domain Name | Enter the domain name you want to give to the NBG5715. |
| Administrator Inactivity Timer | Type how many minutes a management session can be left idle before the session times out. 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 NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

22.4 Password Screen

It is strongly recommended that you change your NBG5715's password.

If you forget your NBG5715's password (or IP address), you will need to reset the device. See [Section 22.7 on page 167](#) for details.

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

Figure 103 Maintenance > Password

The following table describes the labels in this screen.

Table 69 Maintenance > Password

| LABEL | DESCRIPTION |
|-------------------|---|
| Password Setup | Change your NBG5715's password (recommended) using the fields as shown. |
| Old Password | Type the default password or the existing password you use to access the system in this field. |
| New Password | Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type. |
| Retype to Confirm | Type the new password again in this field. |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

22.5 Time Setting Screen

Use this screen to configure the NBG5715's time based on your local time zone. To change your NBG5715's time and date, click **Maintenance > Time**. The screen appears as shown.

Figure 104 Maintenance > Time

The following table describes the labels in this screen.

Table 70 Maintenance > Time

| LABEL | DESCRIPTION |
|--------------------------|---|
| Current Time and Date | |
| Current Time | This field displays the time of your NBG5715. Each time you reload this page, the NBG5715 synchronizes the time with the time server. |
| Current Date | This field displays the date of your NBG5715. Each time you reload this page, the NBG5715 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 . |

Table 70 Maintenance > Time (continued)

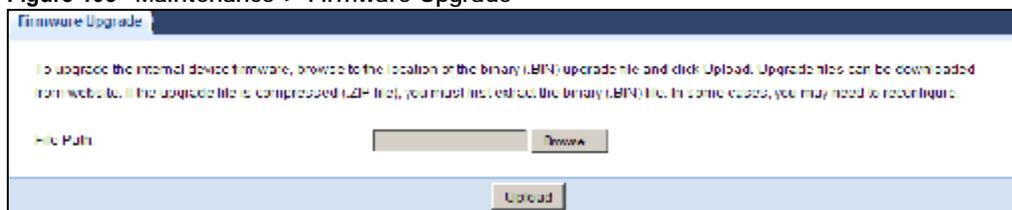
| LABEL | DESCRIPTION |
|----------------------------------|--|
| Get from Time Server | Select this radio button to have the NBG5715 get the time and date from the time server you specified below. |
| User Defined Time Server Address | Select User Defined Time Server Address and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information. |
| Time Zone Setup | |
| Time Zone | Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT). |
| Daylight Savings | Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time. |
| Start Date | Configure the day and time when Daylight Saving Time starts if you selected Daylight Savings . The o'clock field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, April and type 2 in the o'clock field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March . The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| End Date | Configure the day and time when Daylight Saving Time ends if you selected Daylight Savings . The o'clock field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Last, Sunday, October and type 2 in the o'clock field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October . The time you type in the o'clock field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| Apply | Click Apply to save your changes back to the NBG5715. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

22.6 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., "NBG5715.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 NBG5715.

Figure 105 Maintenance > Firmware Upgrade



The following table describes the labels in this screen.

Table 71 Maintenance > Firmware Upgrade

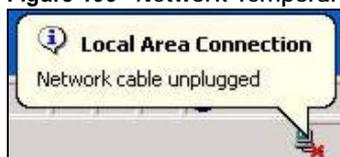
| LABEL | DESCRIPTION |
|-----------|--|
| File Path | Type in the location of the file you want to upload in this field or click Browse... to find it. |
| Browse... | Click Browse... to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload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

Note: Do not turn off the NBG5715 while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the NBG5715 again.

The NBG5715 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 106 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.

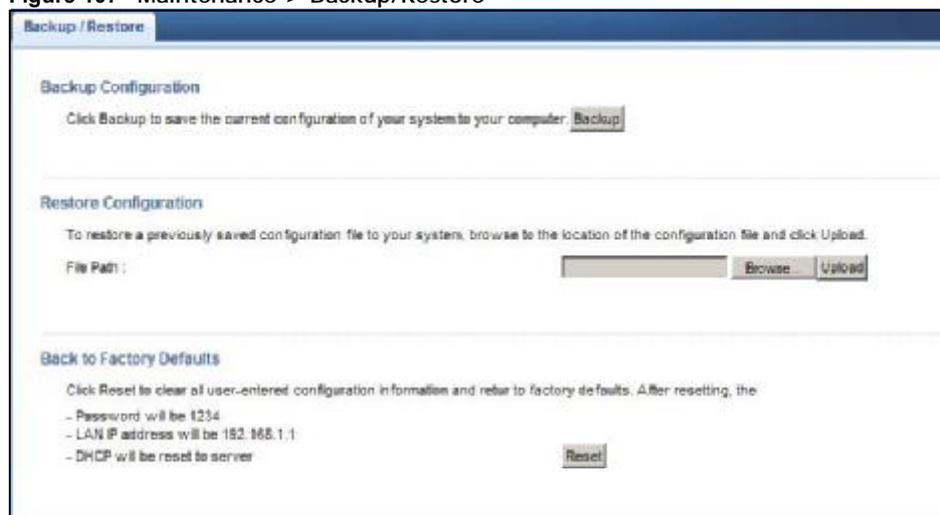
22.7 Backup/Restore Screen

Backup configuration allows you to back up (save) the NBG5715's current configuration to a file on your computer. Once your NBG5715 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 NBG5715.

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

Figure 107 Maintenance > Backup/Restore



The following table describes the labels in this screen.

Table 72 Maintenance > Backup/Restore

| LABEL | DESCRIPTION |
|-----------|--|
| Backup | Click Backup to save the NBG5715'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 NBG5715 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 NBG5715 again. The NBG5715 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 NBG5715 to its factory defaults. You can also press the RESET button on the rear panel to reset the factory defaults of your NBG5715. 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 NBG5715 IP address (192.168.1.2). See [Appendix D on page 205](#) for details on how to set up your computer's IP address.

22.8 The Language Screen

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

Select the language you prefer and click **Apply**. The Web Configurator language changes after a while without restarting the NBG5715.

Figure 108



Troubleshooting

23.1 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](#)
- [NBG5715 Access and Login](#)
- [Internet Access](#)
- [Resetting the NBG5715 to Its Factory Defaults](#)
- [Wireless Router Troubleshooting](#)
- [USB Device Problems](#)
- [ZyXEL NetUSB Share Center Utility Problems](#)

23.2 Power, Hardware Connections, and LEDs

The NBG5715 does not turn on. None of the LEDs turn on.

- 1 Make sure you are using the power adaptor or cord included with the NBG5715.
- 2 Make sure the power adaptor or cord is connected to the NBG5715 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 NBG5715.
- 4 Make sure the LED button on the side panel of the NBG5715 is at the ON position. If the LED button is turned off, the Power LED should be still on for you to determine if the NBG5715 is receiving power.
- 5 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 23](#).

- 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 NBG5715.
- 5 If the problem continues, contact the vendor.

23.3 NBG5715 Access and Login

I don't know the IP address of my NBG5715.

- 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 NBG5715 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 NBG5715 (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 NBG5715'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 NBG5715 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 NBG5715 to change all settings back to their default. This means your current settings are lost. See [Section 23.5 on page 175](#) in the **Troubleshooting** for information on resetting your NBG5715.

I forgot the password.

- 1 The default password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 23.5 on page 175](#).

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 12.4 on page 97](#)), 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 NBG5715](#).
- 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 183](#).
- 4 Make sure your computer is in the same subnet as the NBG5715. (If you know that there are routers between your computer and the NBG5715, skip this step.)
 - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See [Section 13.2 on page 99](#).
 - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG5715. See [Appendix C on page 196](#).
- 5 Reset the device to its factory defaults, and try to access the NBG5715 with the default IP address. See [Chapter 22 on page 167](#).
- 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the NBG5715 using another service, such as Telnet. If you can access the NBG5715, check the remote management settings and firewall rules to find out why the NBG5715 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 NBG5715.](#)

- 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 NBG5715. Log out of the NBG5715 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 NBG5715.
- 5 If this does not work, you have to reset the device to its factory defaults. See [Section 23.5 on page 175](#).

23.4 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 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
- 4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 5 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NBG5715), 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 23](#).
- 2 Reboot the NBG5715.
- 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 23](#). If the NBG5715 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 NBG5715 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 NBG5715.
- 4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestion

- Check the settings for QoS. If it is disabled, you might consider activating it.

23.5 Resetting the NBG5715 to Its Factory Defaults

If you reset the NBG5715, you lose all of the changes you have made. The NBG5715 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 NBG5715:

- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for longer than 1 second to restart/reboot the NBG5715.
- 3 Press the **RESET** button for longer than five seconds to set the NBG5715 back to its factory-default configurations.

If the NBG5715 restarts automatically, wait for the NBG5715 to finish restarting, and log in to the Web Configurator. The password is "1234".

If the NBG5715 does not restart automatically, disconnect and reconnect the NBG5715's power. Then, follow the directions above again.

23.6 Wireless Router Troubleshooting

I cannot access the NBG5715 or ping any computer from the WLAN.

- 1 Make sure the wireless LAN is enabled on the NBG5715. Check if the **WLAN** button is at the **ON** position. Or you can enable the wireless LAN in the **Network > Wireless LAN 2.4G/5G > General** screen.
- 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 NBG5715.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG5715.
- 5 Check that both the NBG5715 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 NBG5715.
- 7 Make sure you allow the NBG5715 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 can access the Internet, but I cannot open my network folders.

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

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

23.7 USB Device Problems

I cannot access or see a USB device that is connected to the NBG5715.

- 1 Be sure to install the ZyXEL NetUSB Share Center Utility (for NetUSB functionality) first from the included disc, or download the latest version from the zyxel.com website.
- 2 Disconnect the problematic USB device, then reconnect it to the NBG5715.
- 3 Ensure that the USB device in question has power.
- 4 Check your cable connections.
- 5 Restart the NBG5715 by disconnecting the power and then reconnecting it.
- 6 If the USB device requires a special driver, install the driver from the installation disc that came with the device. After driver installation, reconnect the USB device to the NBG5715 and try to connect to it again with your computer.

If the problem persists, contact your vendor.

What kind of USB devices do the NBG5715 support?

- 1 It is strongly recommended to use version 2.0 or lower USB storage devices (such as memory sticks, USB hard drives) and/or USB devices (such as USB printers). Other USB products are not guaranteed to function properly with the NBG5715.

23.8 ZyXEL NetUSB Share Center Utility Problems

I cannot install the ZyXEL NetUSB Share Center Utility.

- 1 Make sure that the set up program is one required for your operating system.
- 2 Install the latest patches and updates for your operating system.
- 3 Check the zyxel.com's Download Library site and look for a newer version of the utility software under the device's model name.

Product Specifications

The following tables summarize the NBG5715's hardware and firmware features.

Table 73 Hardware Features

| | |
|-----------------------|---|
| Dimensions | 213.7 mm (W) x 164 mm (D) x 73.6 mm (H) |
| Weight | 251g |
| SDRAM | 128 MB |
| Flash Memory | 128 MB |
| Power Specification | Input: 100~240AC, 50/60Hz, 0.8A Output: 12V 2A |
| Ethernet ports | Auto-negotiating: 100 Mbps, 1000 Mbps in either half-duplex or full-duplex mode. Auto-crossover: Use either crossover or straight-through Ethernet cables. |
| Built-in Switch | A combination of switch and router makes your NBG5715 a cost-effective and viable network solution. You can add up to two computers to the NBG5715 without the cost of a hub when connecting to the Internet through the WAN port. You can add up to three computers to the NBG5715 when you connect to the Internet in AP mode. Add more than four computers to your LAN by using a hub. |
| LEDs | Power, LAN1-4, WAN, Internet, WLAN_2.4G, WLAN 5G, WPS, USB1-2 |
| LED On/Off Switch | One LED On/Off switch to control the LEDs. |
| Reset button | The reset button is built into the rear panel. Use this button to restore the NBG5715 to its factory default settings. Press for 1 second to restart the device. Press for 5 seconds to restore to factory default settings. |
| WPS button | Press the WPS on two WPS enabled devices within 120 seconds for a security-enabled wireless connection. |
| Power switch | Turn on or turn off the power of the NBG5715 using this switch. |
| WLAN switch | Turn on or turn off the 2.4G and 5G wireless function by using this switch. |
| Antenna | The NBG5715 is equipped with three 2dBi (2.4GHz and 5GHz) detachable antenna to provide clear radio transmission and reception on the wireless network. |
| USB Port | The NBG5715 has two built-in USB 2.0 type A for USB device connectivity. |
| Operation Environment | Temperature: 0° C ~ 45° C / 32°F ~ 113°F Humidity: 10% ~ 90% |
| Storage Environment | Temperature: -40° C ~ 70° C / -40°F ~ 158°F Humidity: 10% ~ 95% |

Table 74 Firmware Features

| FEATURE | DESCRIPTION |
|------------------------------------|---|
| Default LAN IP Address | 192.168.1.1 |
| Default LAN Subnet Mask | 255.255.255.0 (24 bits) |
| Default Password | 1234 |
| DHCP Pool | 192.168.1.33 to 192.168.1.64 |
| Wireless Interface | Wireless LAN 2.4GHz, 5GHz |
| Default Wireless SSID | ZyXEL |
| Device Management | Use the Web Configurator to easily configure the rich range of features on the NBG5715. |
| Wireless Functionality | Allows IEEE 802.11a, IEEE 802.11b, IEEE 802.11g and/or IEEE 802.11n wireless clients to connect to the NBG5715 wirelessly. Enable wireless security (WPA(2)-PSK) and/or MAC filtering to protect your wireless network. Note: The NBG5715 may be prone to RF (Radio Frequency) interference from other 2.4 GHz and 5 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 NBG5715. Note: Only upload firmware for your specific model! |
| Configuration Backup & Restoration | Make a copy of the NBG5715's configuration and put it back on the NBG5715 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 NBG5715 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. |
| IPSec VPN | This allows you to establish a secure Virtual Private Network (VPN) tunnel to connect with business partners and branch offices using data encryption and the Internet without the expense of leased site-to-site lines. The NBG5715 VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products. |
| 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 NBG5715. |
| 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 NBG5715. 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. |

Table 74 Firmware Features (continued)

| FEATURE | DESCRIPTION |
|--|--|
| DHCP (Dynamic Host Configuration Protocol) | Use this feature to have the NBG5715 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 NBG5715 supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236). |
| IP Alias | IP Alias allows you to subdivide a physical network into logical networks over the same Ethernet interface with the NBG5715 itself as the gateway for each subnet. |
| PPPoE | PPPoE mimics a dial-up Internet access connection. |
| PPTP Encapsulation | Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The NBG5715 supports one PPTP connection at a time. |
| Universal Plug and Play (UPnP) | The NBG5715 can communicate with other UPnP enabled devices in a network. |

23.9 Wall-mounting Instructions

Complete the following steps to hang your NBG5715 on a wall.

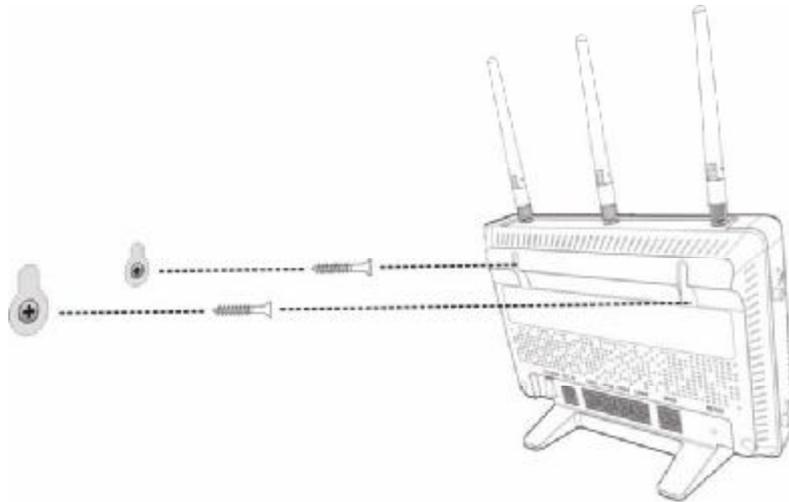
- 1 Select a position free of obstructions on a sturdy wall.
- 2 Drill two holes for the screws.

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 NBG5715 with the connection cables.

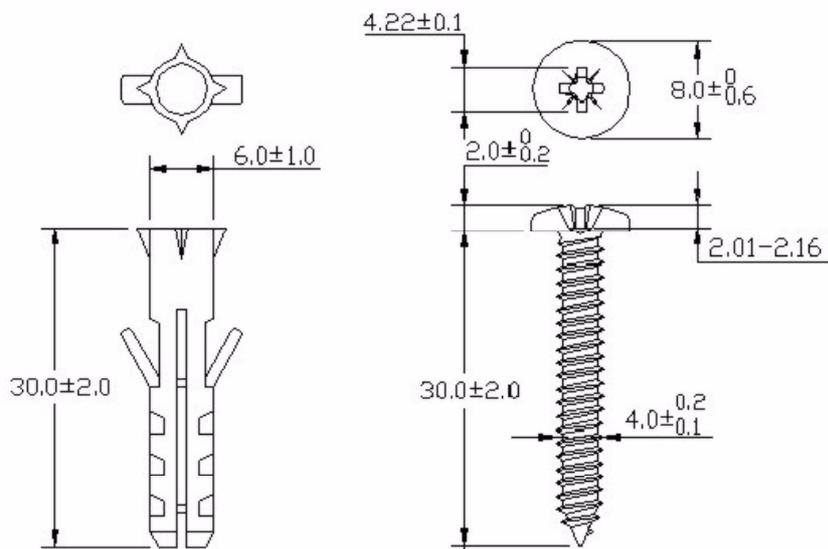
- 5 Align the holes on the back of the NBG5715 with the screws on the wall. Hang the NBG5715 on the screws.

Figure 109 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 110 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

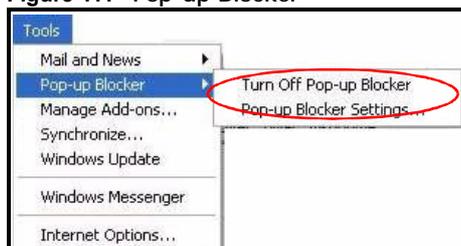
You may have to disable pop-up blocking to log into your device.

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 111 Pop-up Blocker

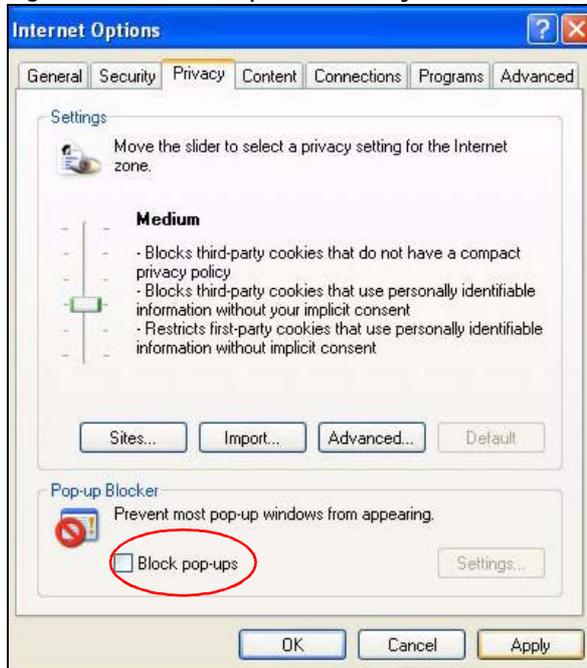


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 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 112 Internet Options: Privacy



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

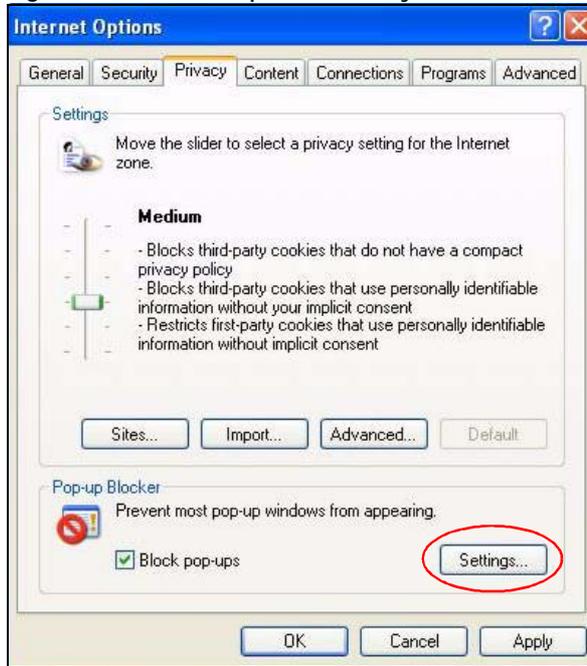
Enable Pop-up Blockers with Exceptions

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.

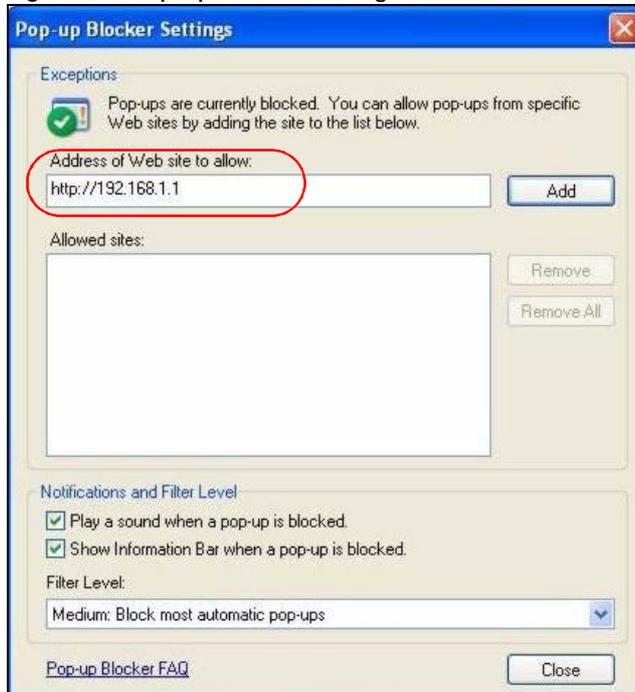
Figure 113 Internet Options: Privacy



- 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 114 Pop-up Blocker Settings



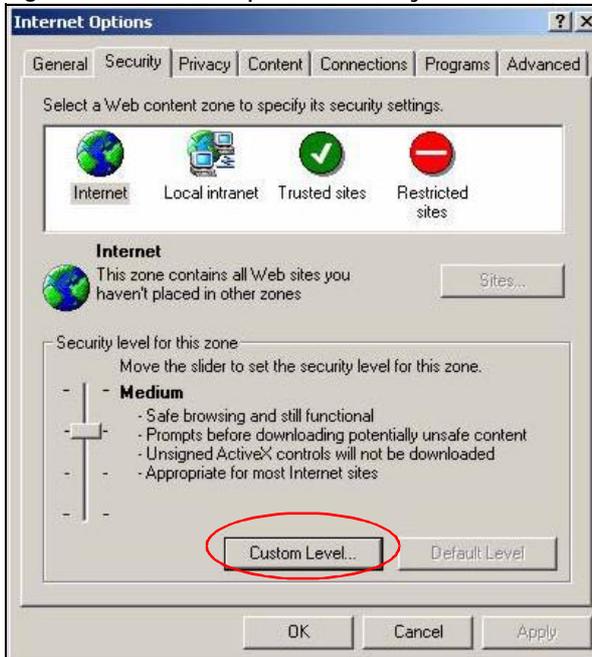
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

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.

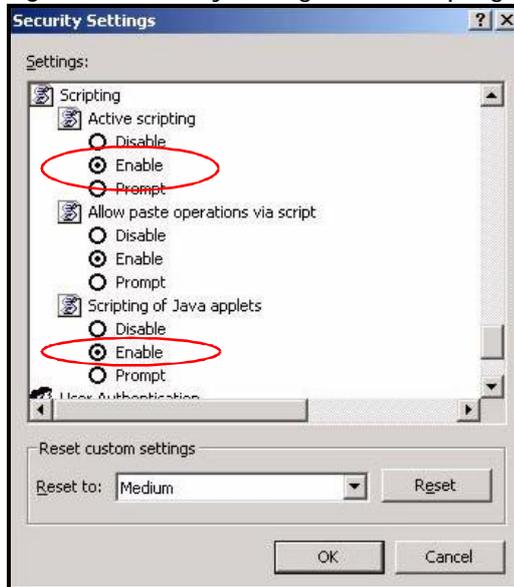
Figure 115 Internet Options: Security



- 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 116 Security Settings - Java Scripting

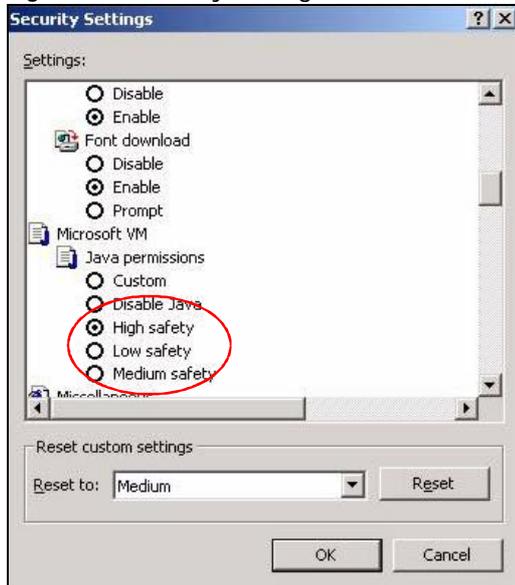


Java Permissions

- 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 117 Security Settings - Java

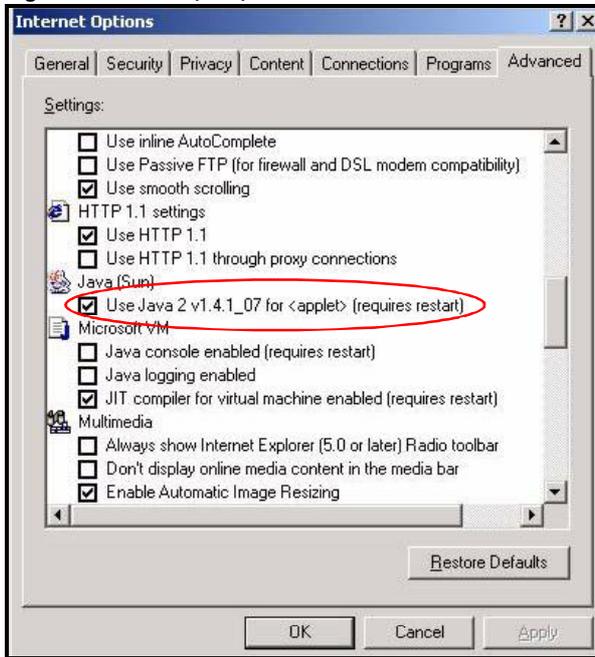


JAVA (Sun)

- 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 118 Java (Sun)

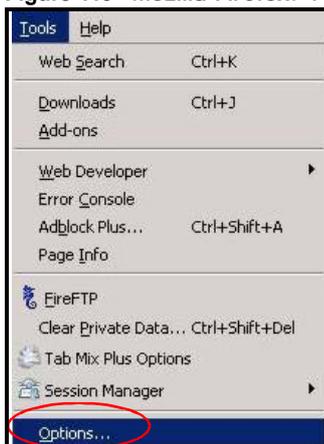


Mozilla Firefox

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.

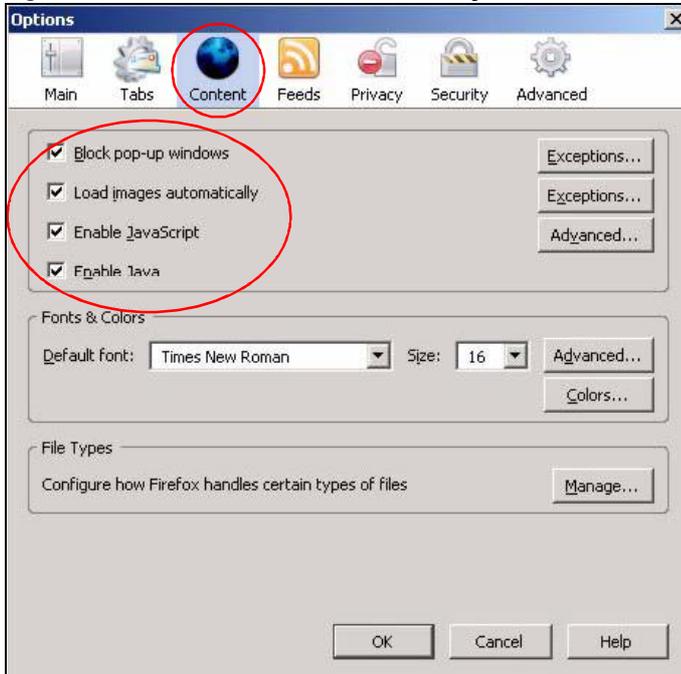
You can enable Java, Javascript and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

Figure 119 Mozilla Firefox: TOOLS > Options



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

Figure 120 Mozilla Firefox Content Security



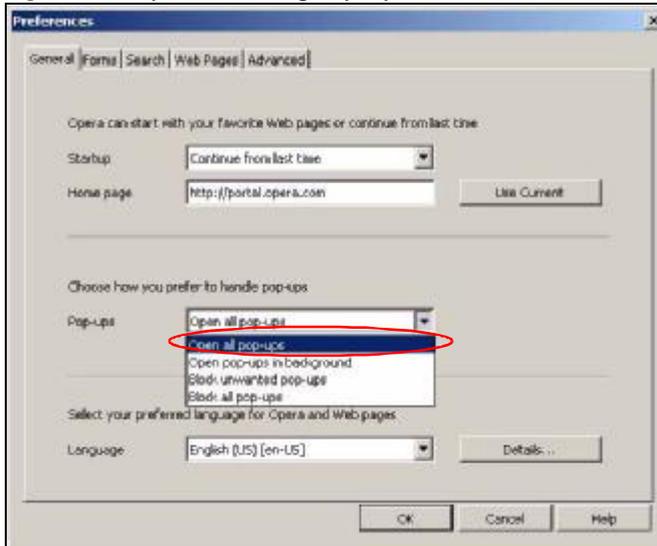
Opera

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**.

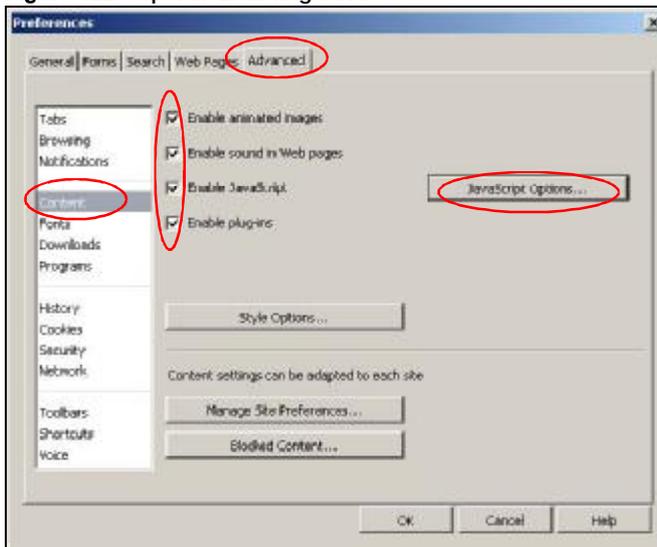
Figure 121 Opera: Allowing Pop-Ups



Enabling Java

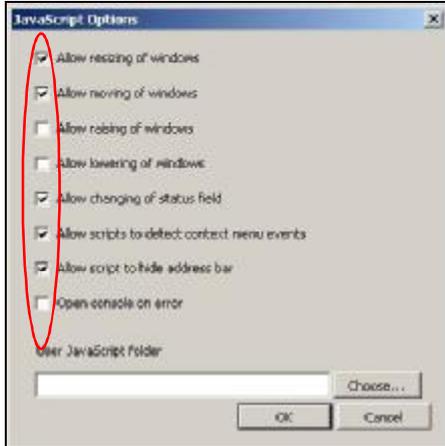
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 122 Opera: Enabling Java



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

Figure 123 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.

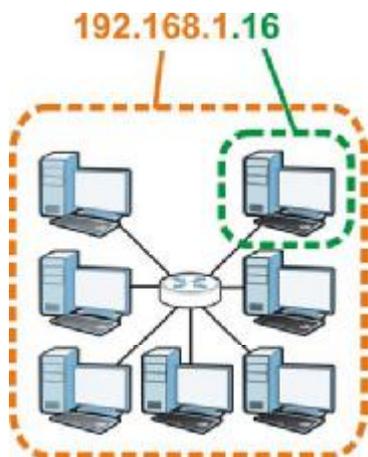
Structure

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 124 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 75 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 76 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 77 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 78 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 78 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 |

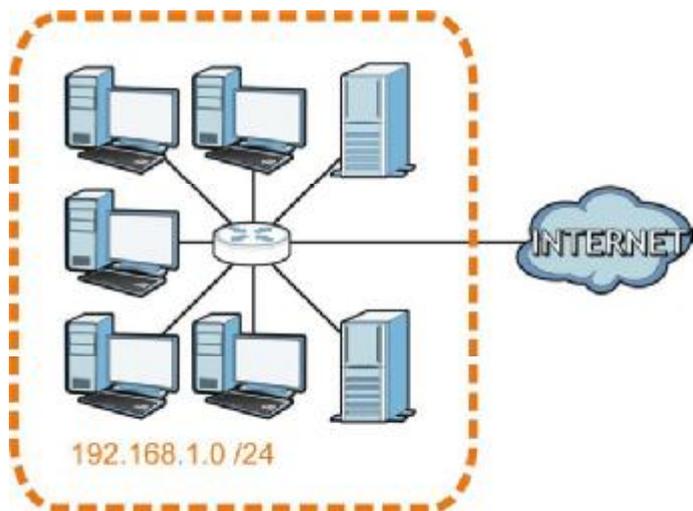
Subnetting

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 125 Subnetting Example: Before Subnetting

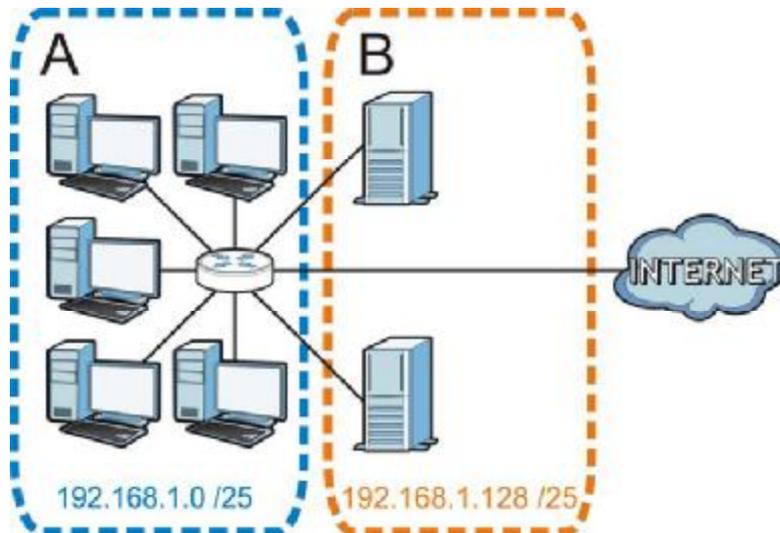


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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 126 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 79 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 79 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 80 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 81 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 82 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 83 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 84 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 85 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 85 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 NBG5715.

Once you have decided on the network number, pick an IP address for your NBG5715 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 NBG5715 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 NBG5715 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.

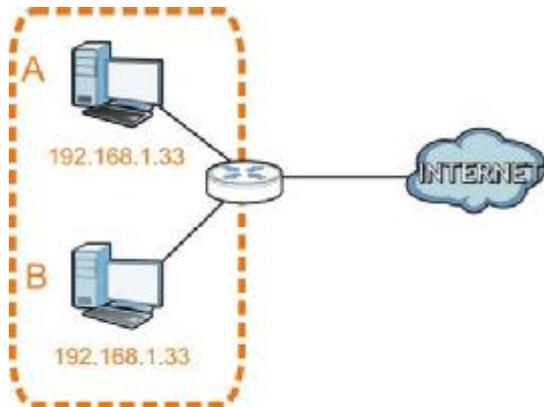
IP Address Conflicts

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.

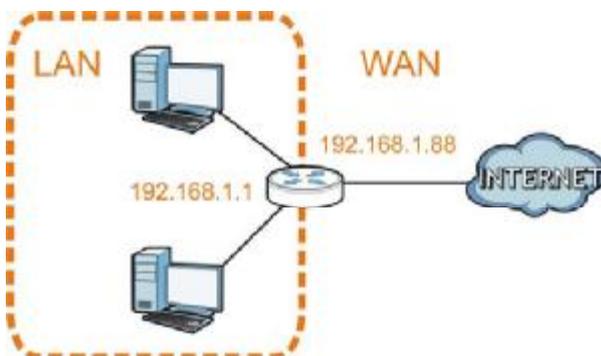
Figure 127 Conflicting Computer IP Addresses Example



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.

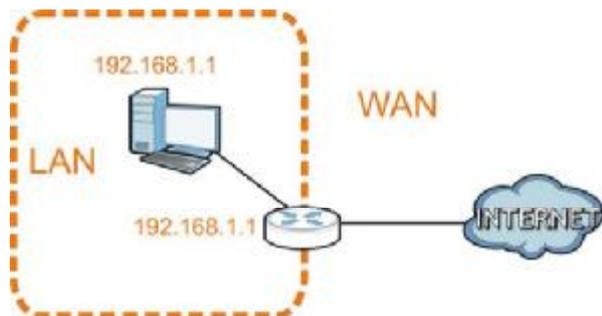
Figure 128 Conflicting Router IP Addresses Example



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 129 Conflicting Computer and Router IP Addresses Example



Setting Up Your Computer's IP Address

Note: Your specific NBG5715 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.

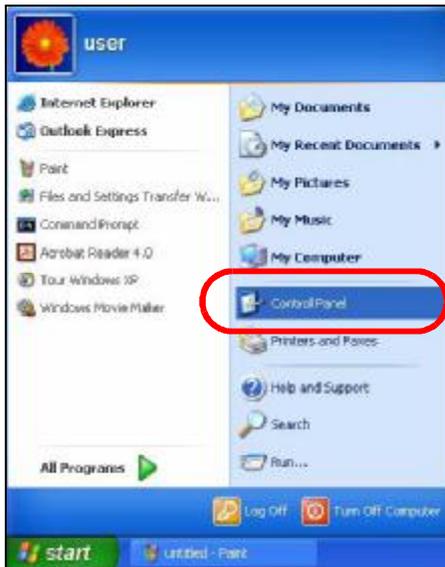
In this appendix, you can set up an IP address for:

- [Windows XP/NT/2000](#) on [page 206](#)
- [Windows Vista](#) on [page 209](#)
- [Windows 7](#) on [page 213](#)
- [Mac OS X: 10.3 and 10.4](#) on [page 217](#)
- [Mac OS X: 10.5 and 10.6](#) on [page 220](#)
- [Linux: Ubuntu 8 \(GNOME\)](#) on [page 223](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 227](#)

Windows XP/NT/2000

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

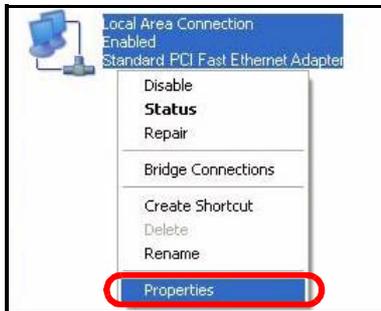
- 1 Click **Start > Control Panel**.



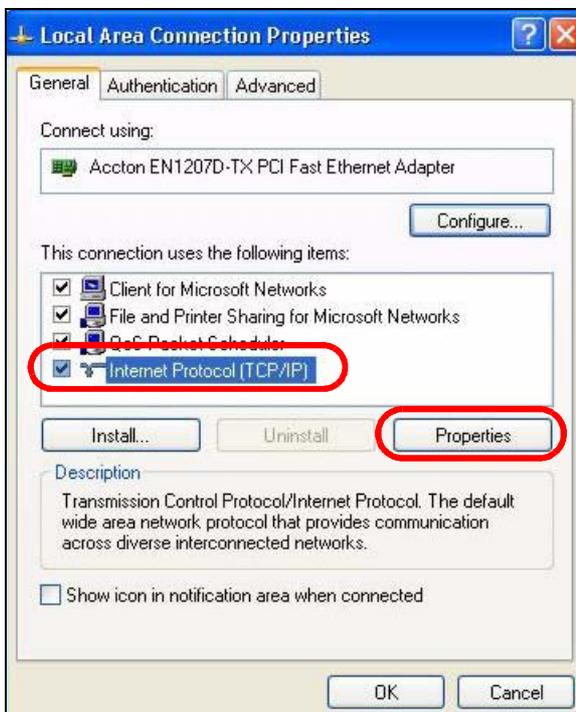
- 2 In the Control Panel, click the **Network Connections** icon.



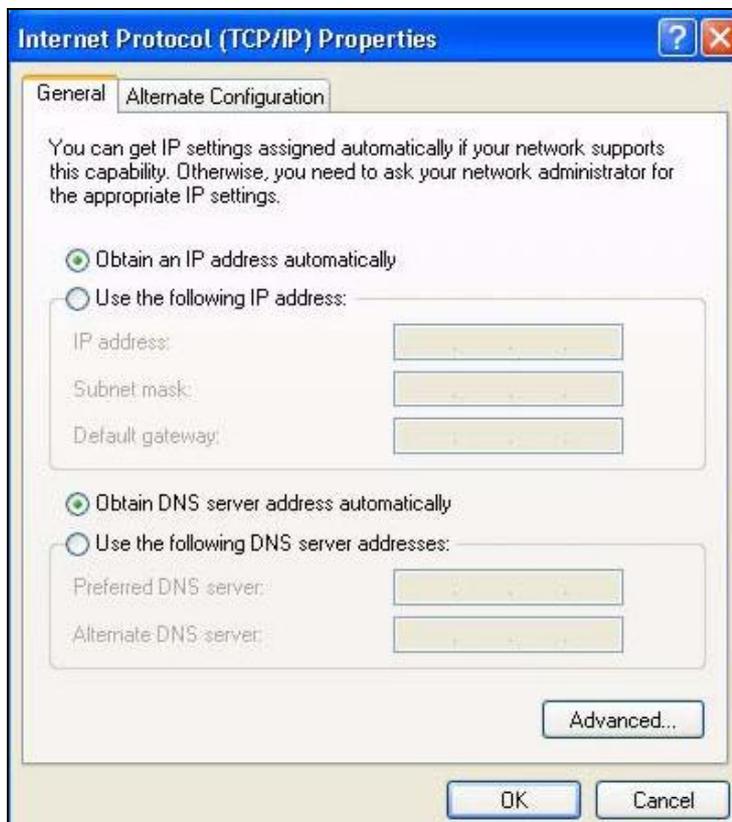
- 3 Right-click **Local Area Connection** and then select **Properties**.



- 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.

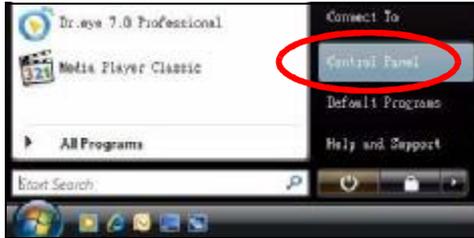
Verifying Settings

- 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.

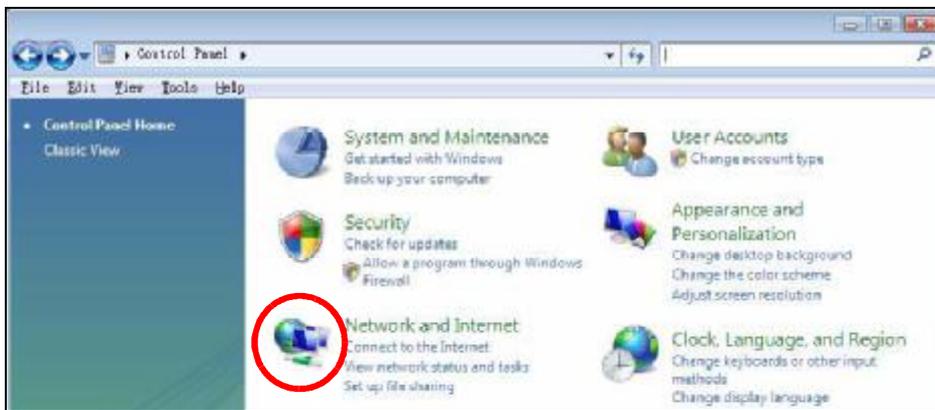
Windows Vista

This section shows screens from Windows Vista Professional.

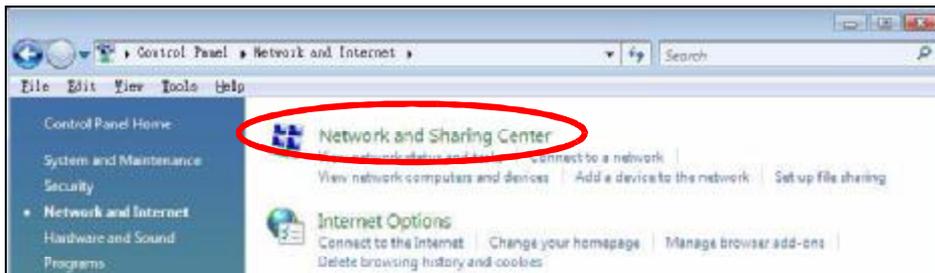
- 1 Click Start > Control Panel.



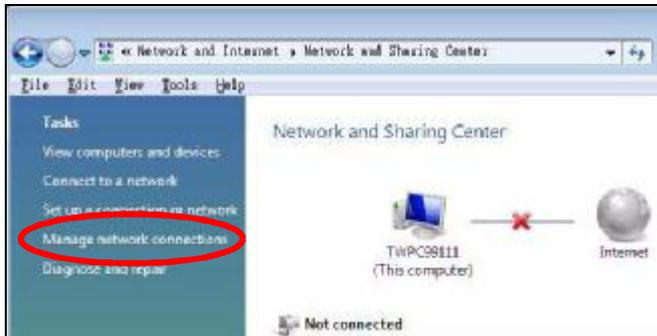
- 2 In the Control Panel, click the Network and Internet icon.



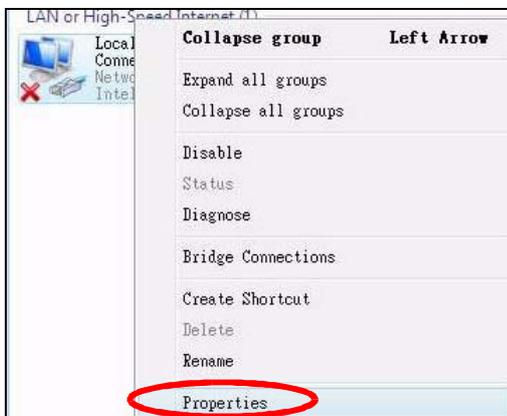
- 3 Click the Network and Sharing Center icon.



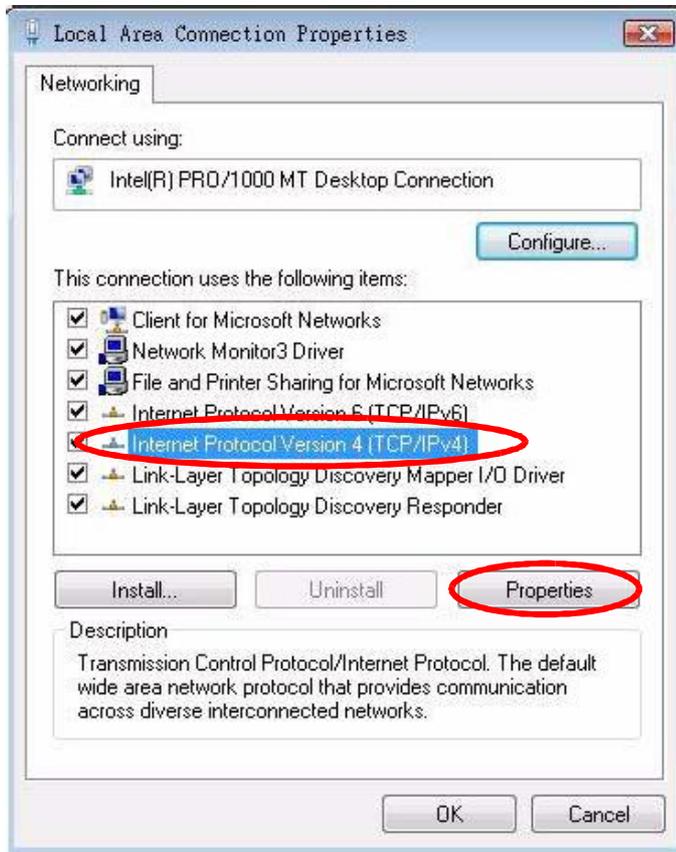
- 4 Click **Manage network connections**.



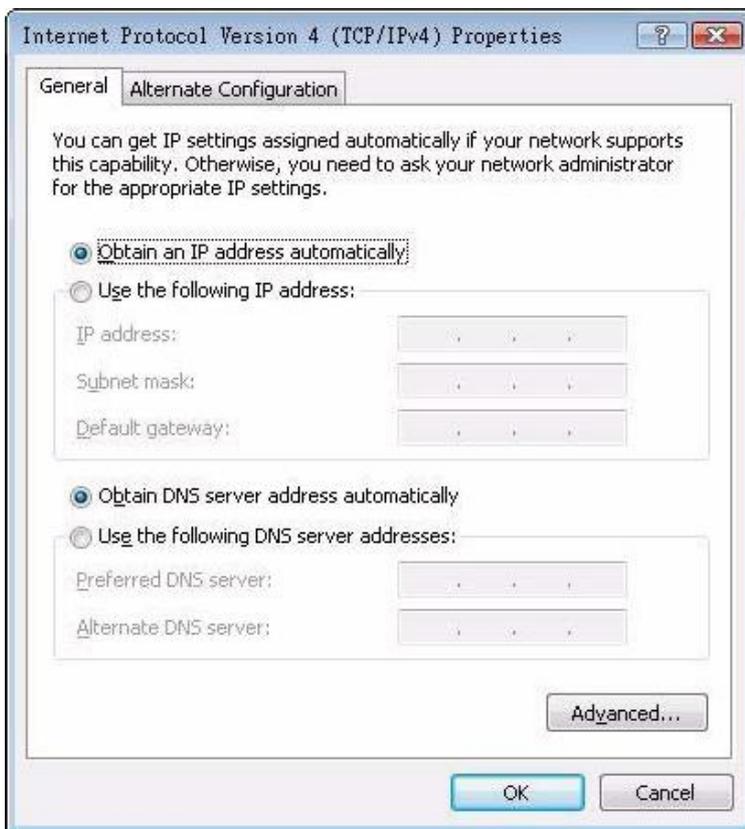
- 5 Right-click **Local Area Connection** and then select **Properties**.



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.

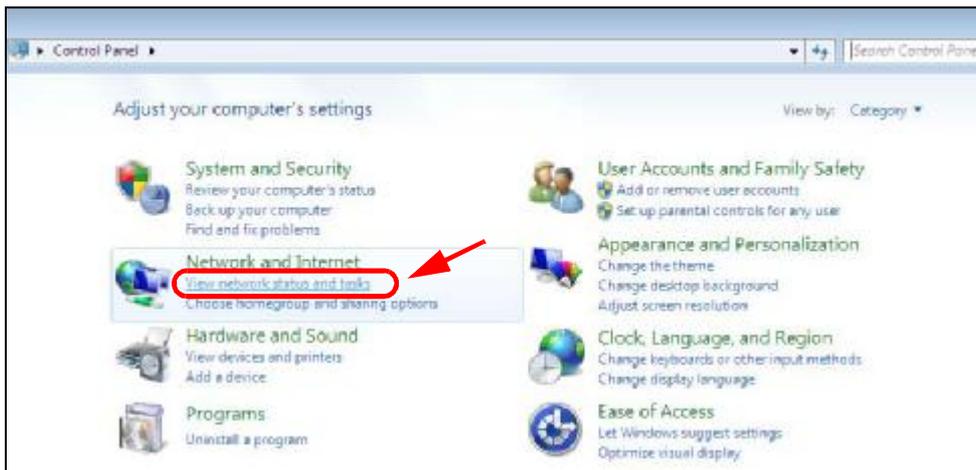
Windows 7

This section shows screens from Windows 7 Enterprise.

- 1 Click Start > Control Panel.



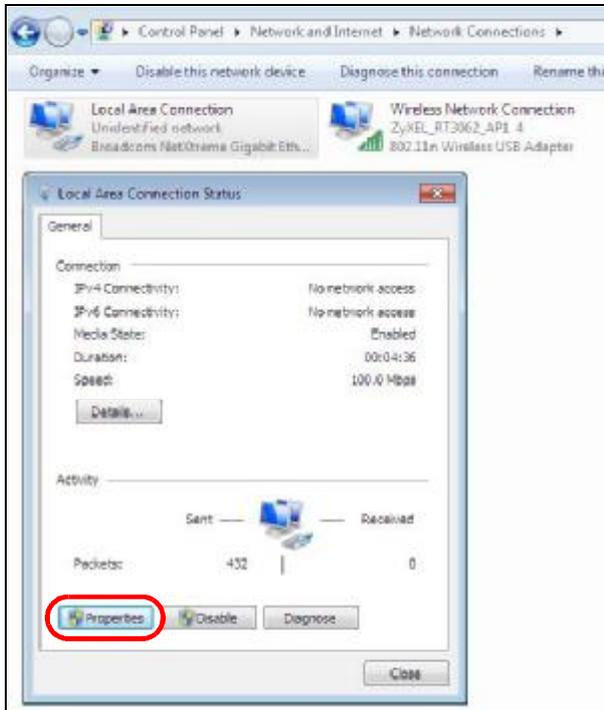
- 2 In the Control Panel, click View network status and tasks under the Network and Internet category.



- 3 Click Change adapter settings.

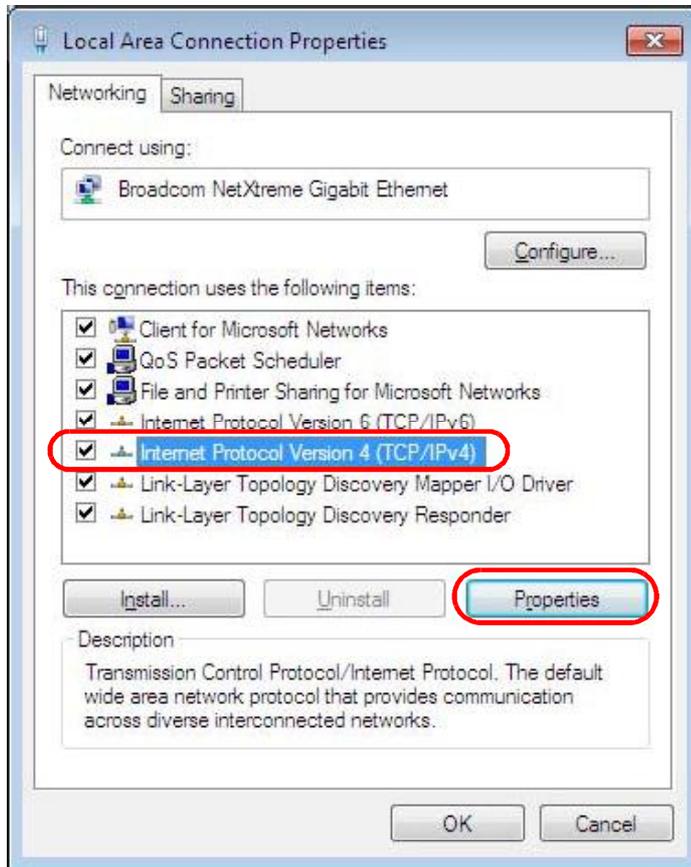


4 Double click Local Area Connection and then select Properties.

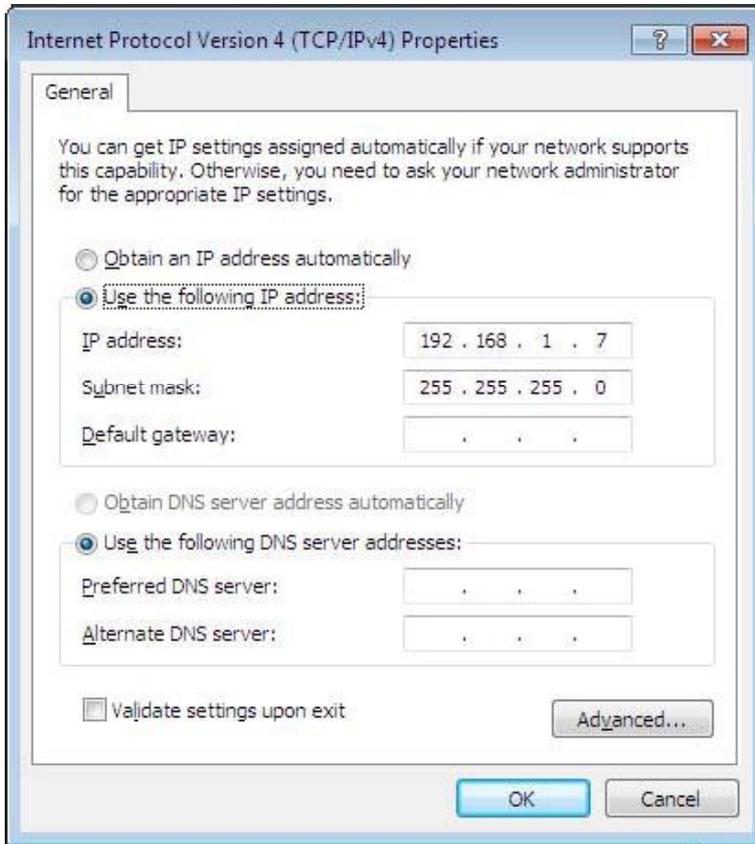


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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



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



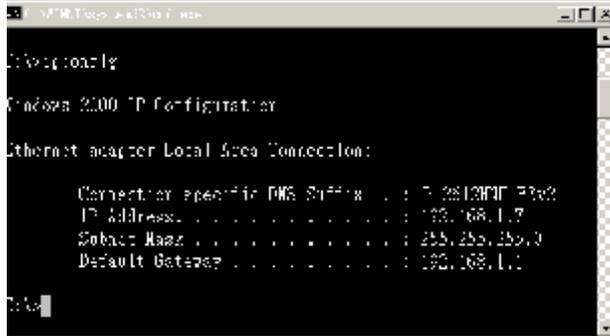
- 7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

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.

- 8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9 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.



```
Microsoft Windows [Version 5.0.2600.5512]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 7.253.131.0
    IP Address. . . . . : 192.168.1.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
```

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.

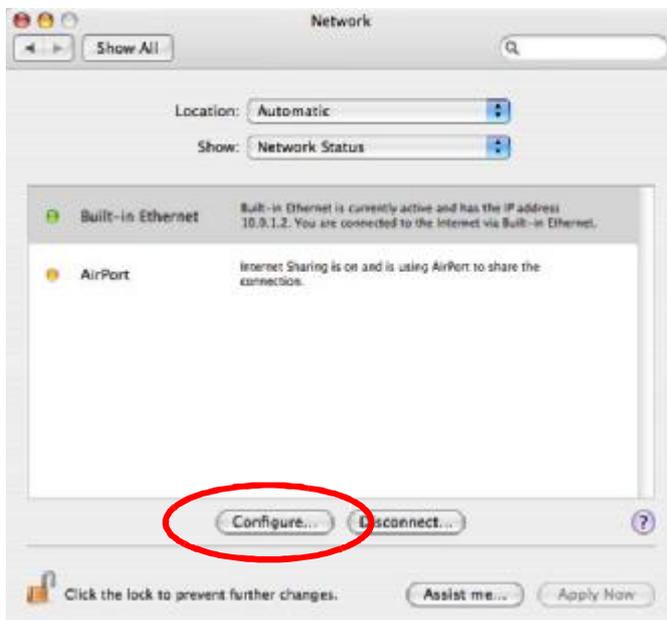
- 1 Click **Apple > System Preferences**.



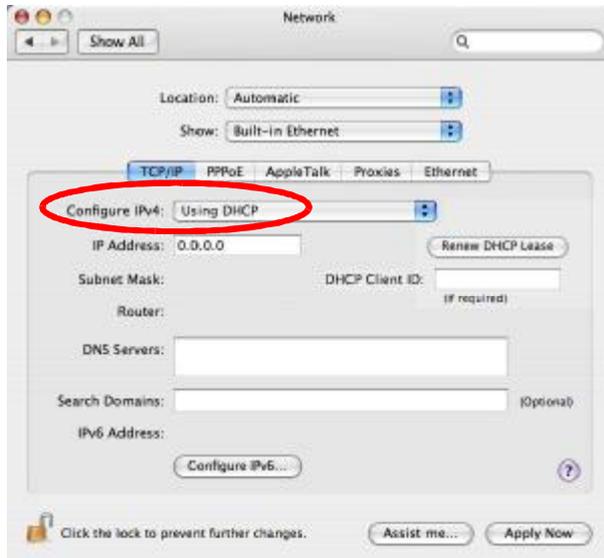
- 2 In the System Preferences window, click the Network icon.



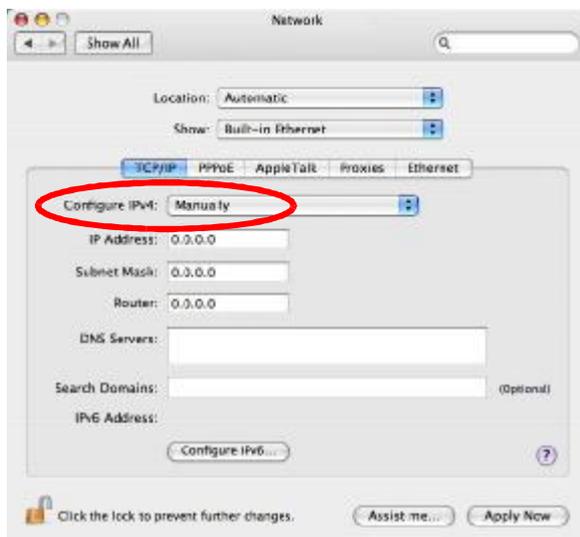
- 3 When the Network preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure**.



- 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.

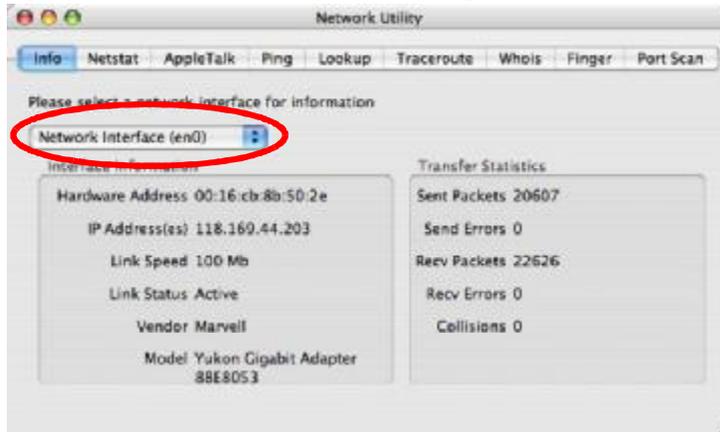


- Click **Apply Now** and close the window.

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 130 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.

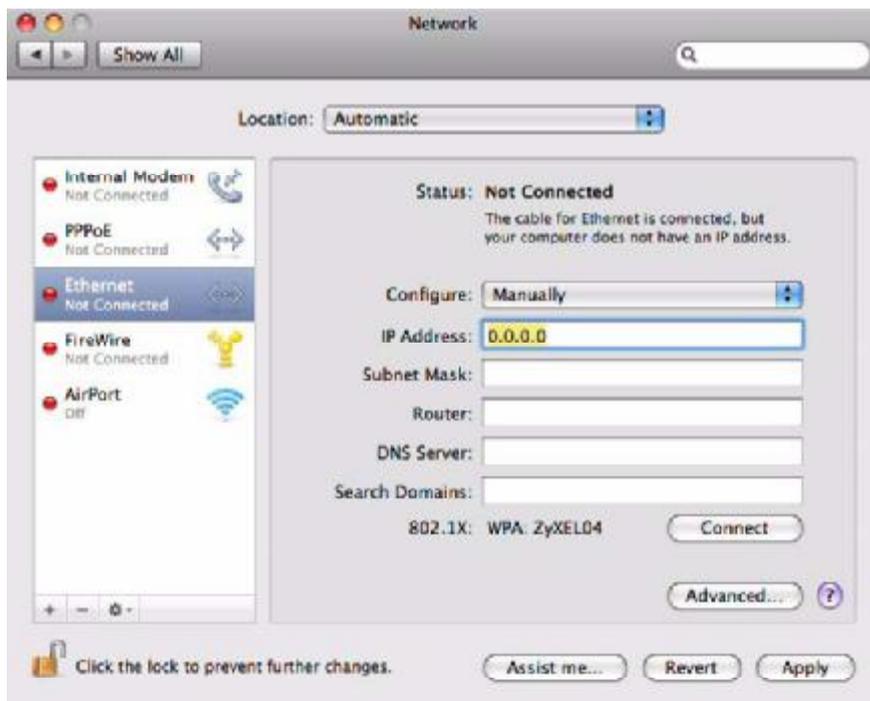


- 3 When the Network preferences pane opens, select Ethernet from the list of available connection types.



- 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 NBG5715.

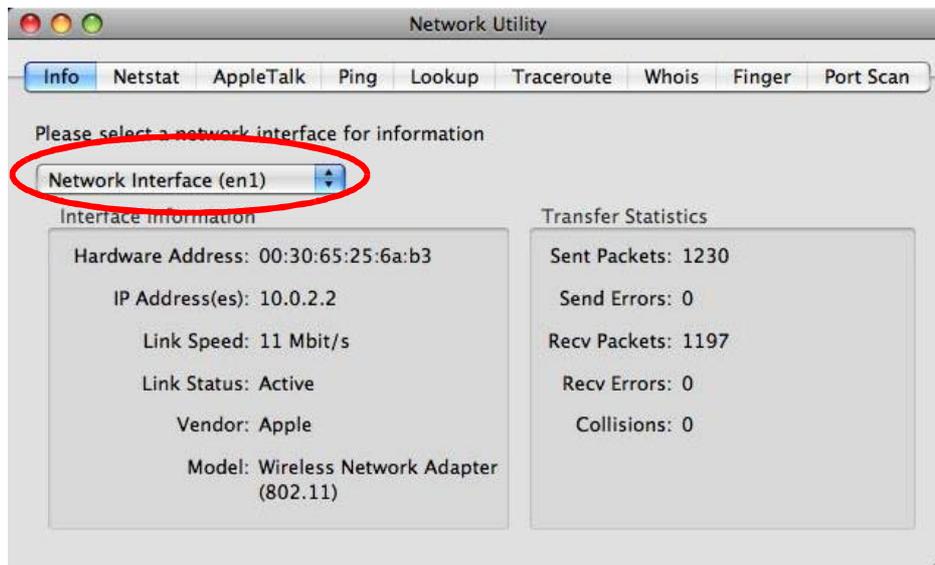


- 6 Click **Apply** and close the window.

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 131 Mac OS X 10.5: Network Utility



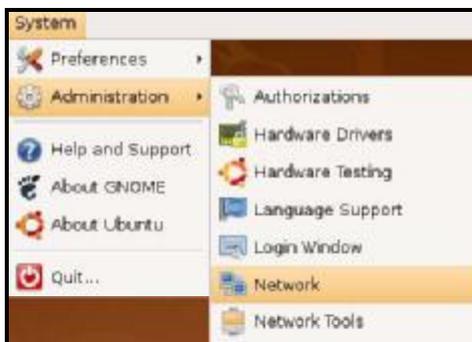
Linux: Ubuntu 8 (GNOME)

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.

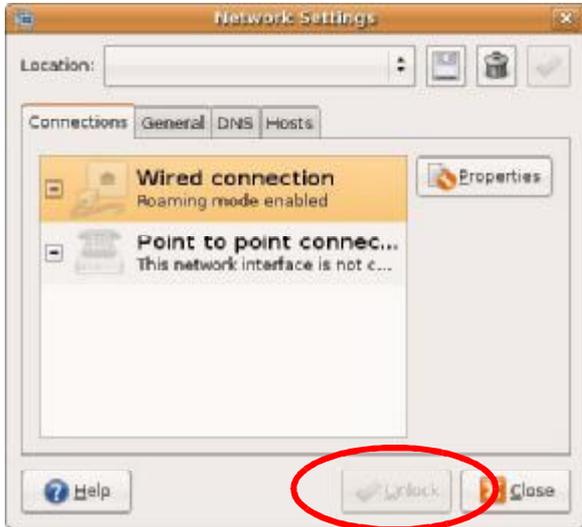
Note: Make sure you are logged in as the root administrator.

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

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



- 2 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.



- 3 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.

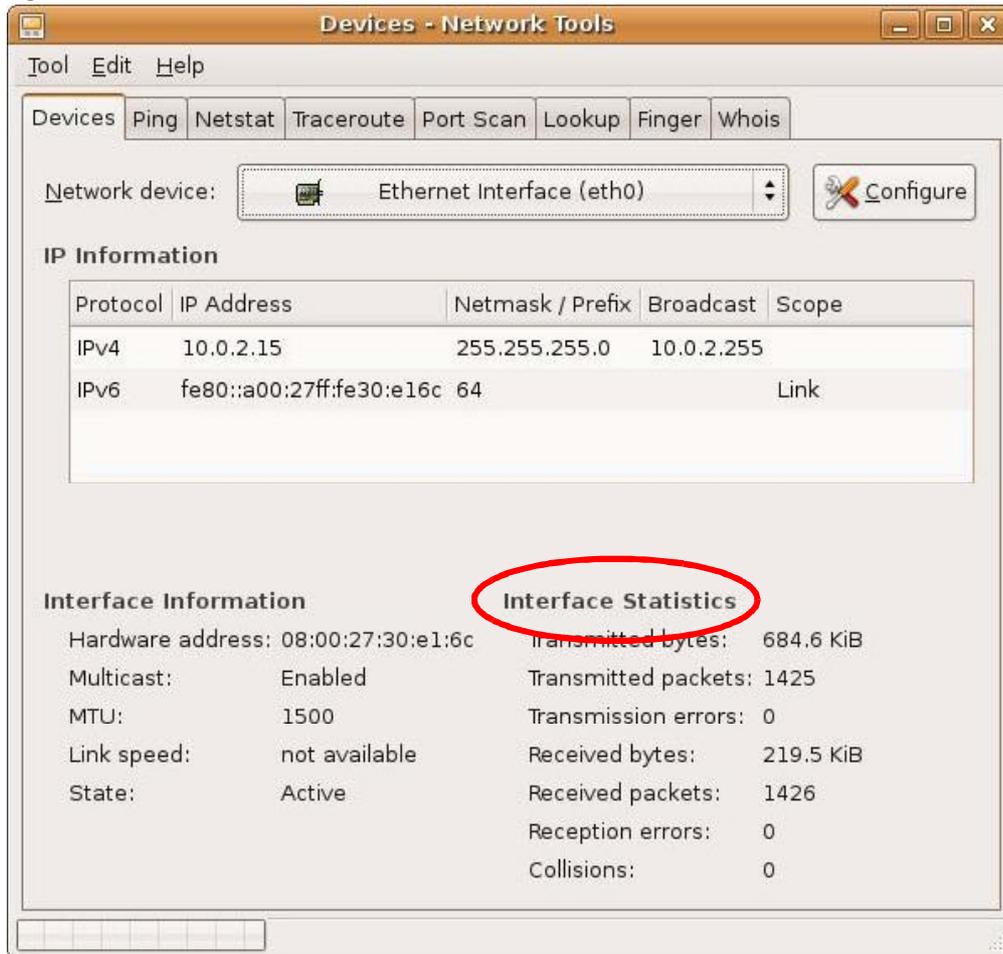


- 8 Click the **Close** button to apply the changes.

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 132 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:

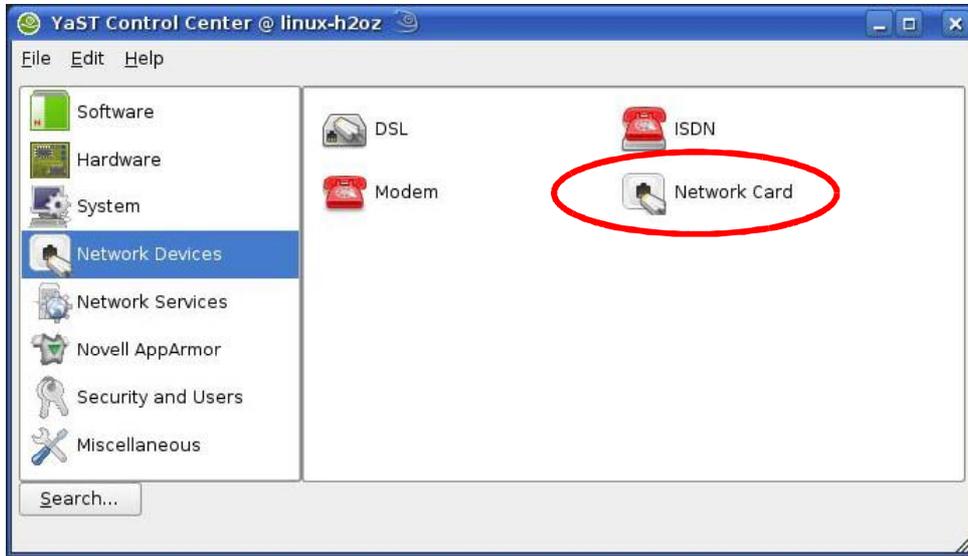
- 1 Click K Menu > Computer > Administrator Settings (YaST).



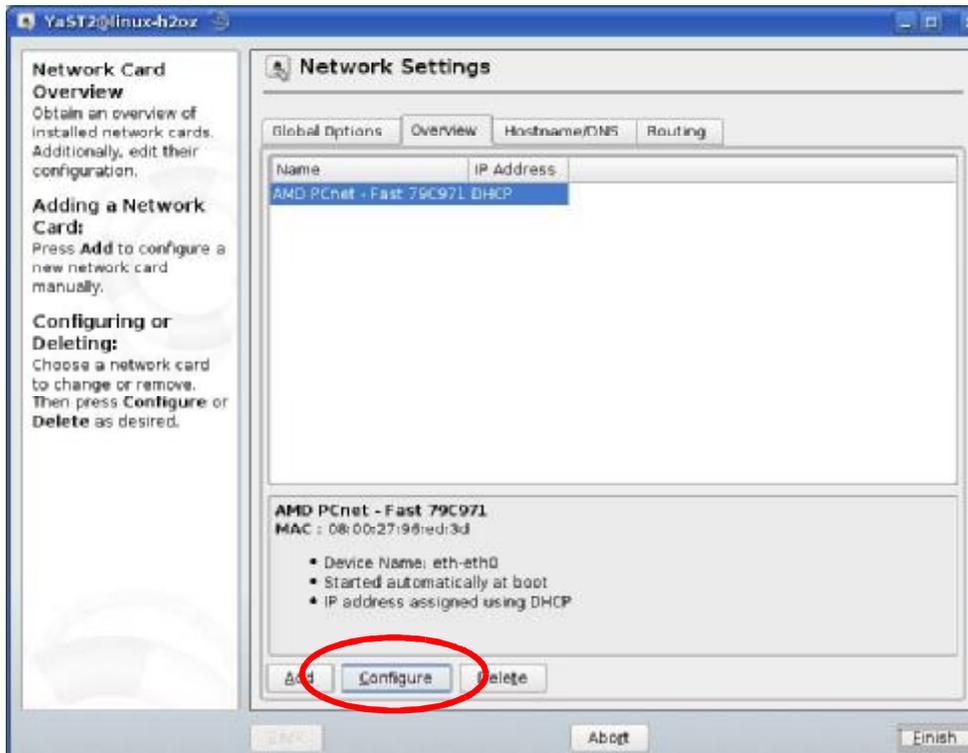
- 2 When the Run as Root - KDE su dialog opens, enter the admin password and click OK.



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

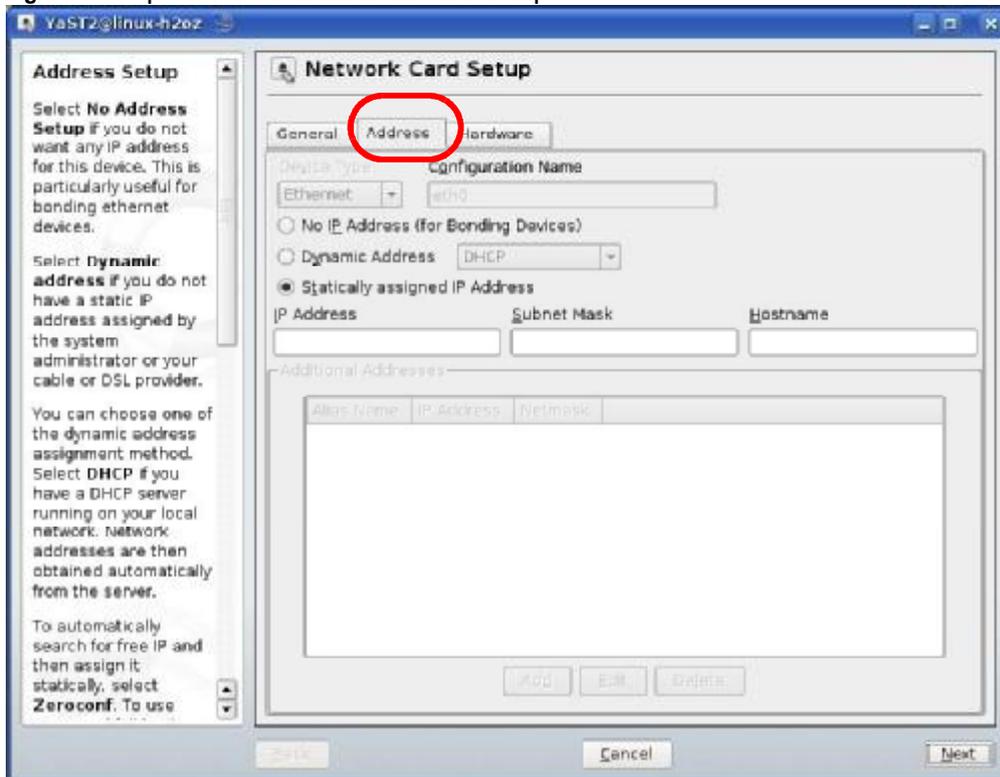


- 4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection Name from the list, and then click the **Configure** button.



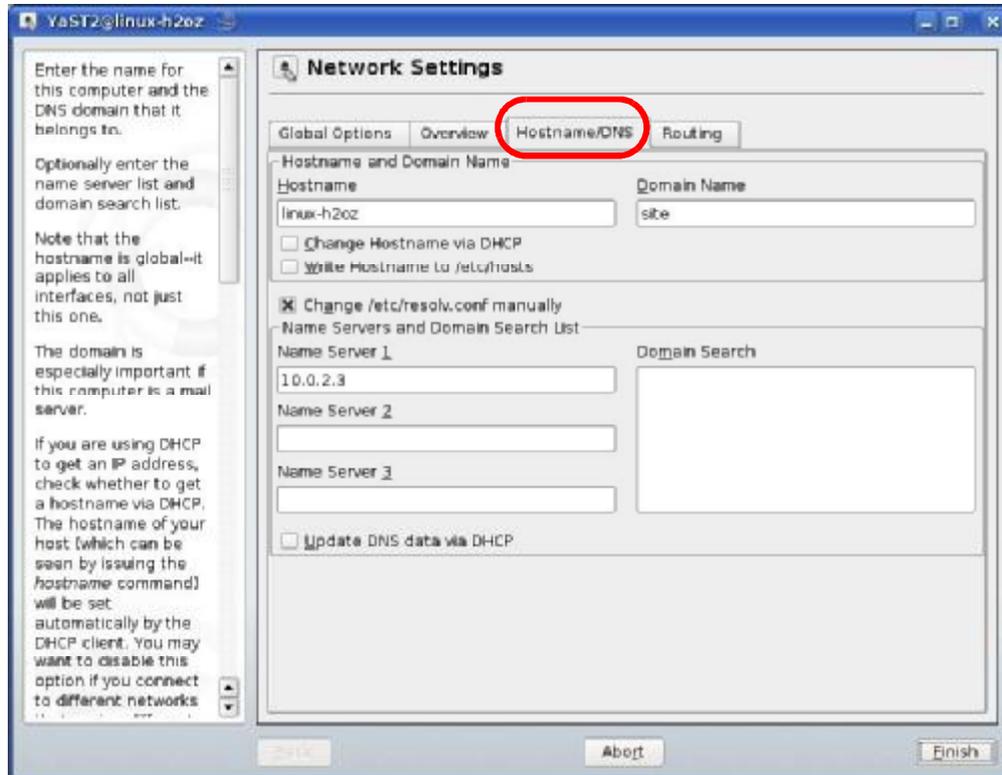
- 5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 133 openSUSE 10.3: Network Card Setup



- 6 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.
- 7 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.

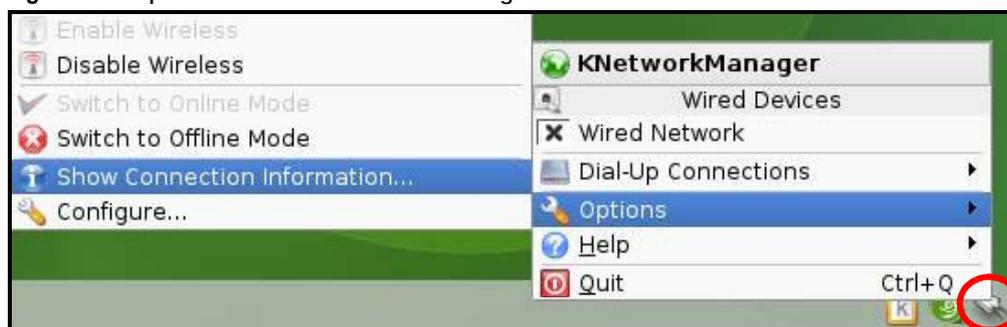


- 9 Click **Finish** to save your settings and close the window.

Verifying Settings

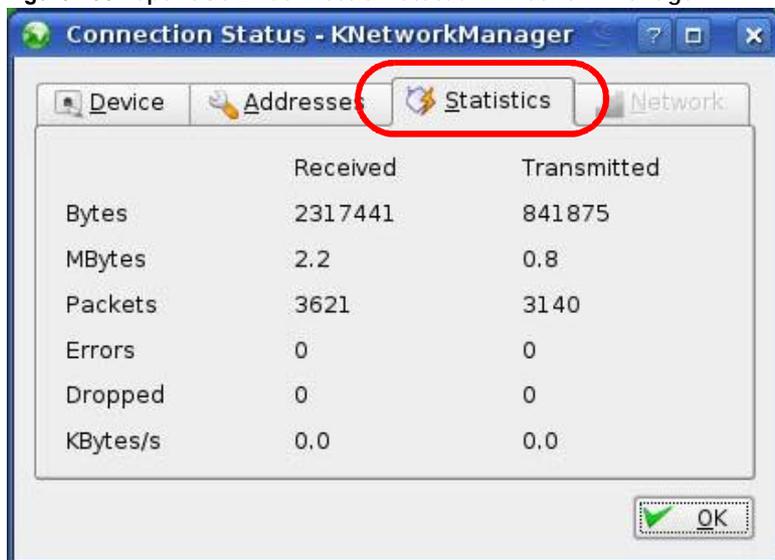
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 134 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 135 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 136 Peer-to-Peer Communication in an Ad-hoc Network



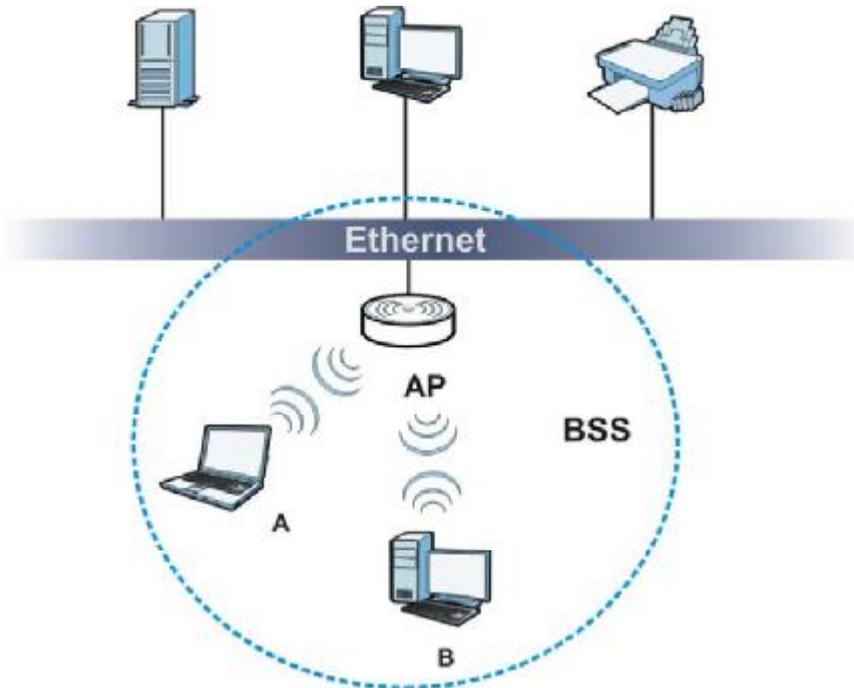
BSS

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 137 Basic Service Set



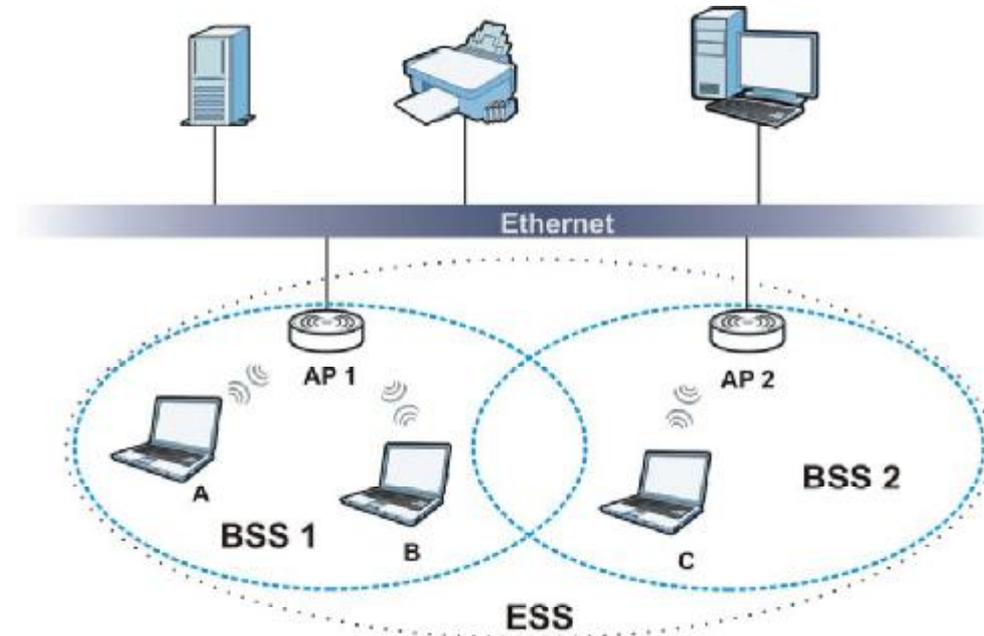
ESS

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 138 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.

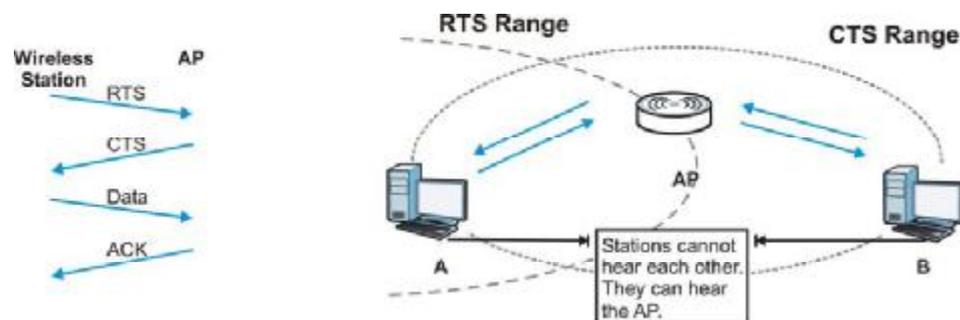
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel 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 139 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 NBG5715 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 86 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 NBG5715 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the NBG5715 identity.

The following figure shows the relative effectiveness of these wireless security methods available on your NBG5715.

Table 87 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) |
| | WPA2 |
| Most Secure | |

Note: You must enable the same wireless security settings on the NBG5715 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 88 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 prevent 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 with 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 140 WPA(2) with RADIUS Application Example



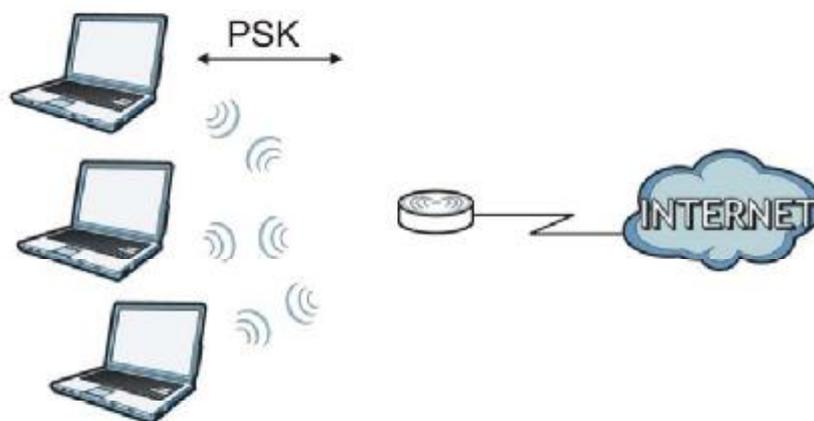
WPA(2)-PSK Application Example

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 141 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 89 Wireless Security Relational Matrix

| AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL | ENCRYPTION METHOD | ENTER MANUAL KEY | IEEE 802.1X |
|--|-------------------|------------------|--------------------------------|
| Open | None | No | Disable |
| | | | Enable without Dynamic WEP Key |
| Open | WEP | No | Enable with Dynamic WEP Key |
| | | Yes | Enable without Dynamic WEP Key |
| | | Yes | Disable |
| Shared | WEP | No | Enable with Dynamic WEP Key |
| | | Yes | Enable without Dynamic WEP Key |
| | | Yes | Disable |
| WPA | TKIP/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 90 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. |
| FTP | TCP TCP | 20 21 | File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail. |
| H.323 | TCP | 1720 | NetMeeting uses this protocol. |

Table 90 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. |
| SFTP | TCP | 115 | Simple File Transfer Protocol. |

Table 90 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. |
| TFTP | UDP | 69 | Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol). |
| VDOLIVE | TCP | 7000 | Another videoconferencing solution. |

Open Software Announcements

End-User License Agreement for "NBG5715"

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE 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 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 OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED. HOWEVER, CERTAIN ZYXEL'S PRODUCTS MAY CONTAIN-IN PART-SOME THIRD PARTY'S FREE AND OPEN SOFTWARE PROGRAMS WHICH ALLOW YOU TO FREELY COPY, RUN, DISTRIBUTE, MODIFY AND IMPROVE THE SOFTWARE UNDER THE APPLICABLE TERMS OF SUCH THRID PARTY'S LICENSES ("OPEN-SOURCED COMPONENTS"). THE OPEN-SOURCED COMPONENTS ARE LISTED IN THE NOTICE OR APPENDIX BELOW. ZYXEL MAY HAVE DISTRIBUTED TO YOU HARDWARE AND/OR SOFTWARE, OR MADE AVAILABLE FOR ELECTRONIC DOWNLOADS THESE FREE SOFTWARE PROGRAMS OF THRID PARTIES AND YOU ARE LICENSED TO FREELY COPY, MODIFY AND REDISTRIBUTE THAT SOFTWARE UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY. NONE OF THE STATEMENTS OR DOCUMENTATION FROM ZYXEL INCLUDING ANY RESTRICTIONS OR CONDITIONS STATED IN THIS END USER LICENSE AGREEMENT SHALL RESTRICT ANY RIGHTS AND LICENSES YOU MAY HAVE WITH RESPECT TO THE OPEN-SOURCED COMPONENTS UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY.

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 international copyright law, trade secret law, international treaty provisions, and the applicable national laws of each respective country. 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. 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, you may not market, co-brand, and 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 License Notice as below for the third party software, and your use of such material is exclusively 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 other than compliance with the applicable license terms of such third party, and makes no warranty (express, implied or statutory) whatsoever with respect thereto. 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, AND NON-INFRINGEMENT. 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 SOFTWARE OR PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's TOTAL 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 if the parties agree to a binding arbitration. 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 free software programs covered under the open source code licenses which allows you to freely copy, modify and redistribute the software. For at least three (3) years from the date of distribution of the applicable product or software, we will give to anyone who contacts us at the ZyXEL Technical Support (support@zyxel.com.tw), for a charge of no more than our cost of physically performing source code distribution, a complete machine-readable copy of the complete corresponding source code for the version of the Programs that we distributed to you if we are in possession of such.

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes Busybox, Dnsmasq, e2fsprogs, ethtool, gdbm, haserl, hotplug2, Igmpproxy, lproute2, keynote, libnetfilter_contrack, libnfnetlink, libtool, Mtd-utils, net-tools, ntpclient, radvd, rp-pppoe, screen, uboot-envtools, uci, udev, Updatedd, Wireless_tools, base-files, bridge-utils, iptables, linux kernel, openssl, u-boot, uClibc, and gcc under below GPL license

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License

applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the

operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and

"any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes Dropbear, Lua, and ncurses under the MIT License.

The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is

furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This Product includes isakmpd, miniupnpd, ipsec-tools, Ppp, and libpcap, under the license by BSD

BSD

Copyright (c) [dates as appropriate to package]

The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes luci, and uhttpd under the license by Apache software

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems,

and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct

or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
- (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
- (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
- (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or

documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the

origin of the Work and reproducing the content of the NOTICE file.

7. **Disclaimer of Warranty.** Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. **Limitation of Liability.** In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. **Accepting Warranty or Additional Liability.** While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this

License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

This Product includes gmp, and libcli under the LGPL License.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License").

Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License. d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other

licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of

these things: a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE

LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS.

This Product includes zlib under the zlib License

```
/* zlib.h -- interface of the 'zlib' general purpose compression library
   version 1.2.2, October 3rd, 2004
```

Copyright (C) 1995-2004 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

* /

This Product includes lldt under the following license

**MICROSOFT WINDOWS RALLY PROGRAM
LICENSE AGREEMENT**

This Microsoft Windows Rally Program License Agreement (the "Agreement") is by and between MICROSOFT CORPORATION, a corporation organized under the laws of Washington ("Microsoft"), and the individual or entity identified and signing below ("You" or "Licensee"). *If You want a license from Microsoft to access, view or implement one or more Licensed Technologies (as defined below), You must (1) complete the designated information in the box below, and (2) sign and return this Agreement AS IS to Microsoft at the address shown in Section 8.3.* This is an offer to be accepted only on the terms set forth in this Agreement. If any other changes are made to this Agreement, the offer is revoked. This Agreement, completed and fully executed by You, will become effective on the date it is received by Microsoft pursuant to Section 8.3 (the "Effective Date").

| |
|---|
| Licensee full legal name: Type of legal entity (corporation, partnership, sole proprietorship, individual or other): State/Province organized: Street address: City, State & Country: Email contact for notices: |
|---|

Recitals

Microsoft has developed certain "Windows Rally" technologies, including communications protocols, that are intended to facilitate certain tasks performed by or in conjunction with network connected devices. Licensee desires a license from Microsoft to access, view or implement the Licensed Technology(ies) for which the applicable box(es) are checked on Exhibit A, and to use the corresponding Technical Documentation (as defined below) for the purpose of such implementation(s).

1. Definitions

1.1 "Affiliate" means, with respect to any legal entity, any other such entity directly or indirectly Controlling, Controlled by, or under common Control with such entity. "Control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of a legally recognizable entity, whether through the ownership of voting shares or other voting interests, by contract, or otherwise.

1.2 "Authorized Purpose" means, with respect to each Licensed Technology, the function(s) corresponding to such Licensed Technology as set forth in Exhibit A.

1.3 "Licensed Implementation(s)" means only those specific portion(s) of Licensee's products that (a) implement Licensed Technology(ies) solely to carry out the corresponding Authorized Purpose(s), and (b) are compliant with all Required Portions of the relevant Technical Documentation.

1.4 "Licensed Product" means a product, branded with a trademark owned or controlled by Licensee, that includes Licensed Implementation(s) either alone or with other components.

1.5 "Licensed Technology(ies)" means the version(s) of the software communications protocol(s) and related technology(ies) which Licensee indicates it has selected from the list on Exhibit A. "Licensed Technology(ies)" also includes any version(s) of such protocol(s) or technology(ies) and any new protocol(s) or technology(ies) that may be added to this Agreement by mutual written agreement between Licensee and Microsoft in the future.

1.6 "Necessary Claims" means claims of an unexpired patent or patent application that (a) are owned or controlled by Microsoft or a Microsoft Affiliate; and (b) are necessarily infringed by implementing the Required Portions of the Technical Documentation, wherein a claim is necessarily infringed only when it is not possible to avoid infringing it because there is no non-infringing alternative for implementing the Required Portion of the relevant Technical Documentation. "Necessary Claims" do not include any claims: (i) other than those set forth above even if contained in the same patent as Necessary Claims; (ii) that, if licensed, would require a payment of royalties or other fee(s) by a party to unaffiliated third parties; (iii) to any underlying or enabling technologies that may be used or needed to make or use a system or product or

portion thereof that implements the relevant Licensed Technology(ies); or (iv) to any implementation of other technical documentation, specifications or technologies that are merely referred to in the body of the Technical Documentation.

1.7 “Required Portions” means all portions of Technical Documentation with the exception of any portions that are expressly identified by Microsoft as being “optional.”

1.8 “Technical Documentation” means Microsoft’s proprietary technical documentation for the Licensed Technology(ies).

2. Windows Rally Program Administration; Program Additions and Updates

2.1 Delivery. Microsoft has made the Technical Documentation available to Windows Rally program licensees at www.microsoft.com/rally. The Technical Documentation shall be deemed accepted by Licensee upon its download.

2.2 Program Additions and Updates. Microsoft may in its discretion elect to include additional software communications protocols or other technologies in the Windows Rally program in the future by publishing technical documentation for them at www.microsoft.com/rally and making available amended terms of this Agreement at such website in order to make such protocols or other technologies available under this Agreement. Except in the event Microsoft makes such additional protocols or other technologies available and Licensee accepts applicable terms governing their inclusion under this Agreement, no other protocols, technologies, technical documentation, or Microsoft enhancements or updates to the Licensed Technology(ies) and/or Technical Documentation are licensed under this Agreement.

2.3 No Technical Support. This Agreement does not include technical support by Microsoft to Licensee, its channel entities, or end users. Licensee is solely responsible for all such support and shall advise channel entities and end users accordingly.

3. Licenses

3.1 Copyright License. Microsoft hereby grants Licensee a non-exclusive, royalty-free, non-sublicensable, nontransferable, personal, worldwide license to make a reasonable number of complete copies of the Technical Documentation for use solely in developing and testing such Licensed Implementation(s). Licensee shall retain in all copies of, and shall comply with, any copyright-related notices that are included in such Technical Documentation.

3.2 Patent License. Microsoft hereby grants Licensee a nonexclusive, royalty-free, non-sublicensable, nontransferable, personal, worldwide license under the Necessary Claims to use the Technical Documentation for the Licensed Technology(ies) to:

(a) make, use, import, offer to sell, sell and distribute directly or indirectly to end users, object code versions of Licensed Implementations only as incorporated into Licensed Products and solely for the purpose of conforming with the corresponding Technical Documentation in order for Licensed Implementations to carry out the Authorized Purpose corresponding to such Licensed Technology(ies), and

(b) to distribute or otherwise disclose source code copies of the Licensed Implementation(s) licensed in Section 3.2(a) only if Licensee (i) prominently displays the following notice in all copies of such source code, and (ii) distributes or discloses the source code only under a license agreement that includes the following notice as a term of such license agreement and does not include any other terms that are inconsistent with, or would prohibit, the following notice:

“This source code incorporates intellectual property owned by Microsoft Corporation and cannot be made, used, sold, offered for sale, imported or redistributed without a license from Microsoft Corporation. Our provision of this source code does not include any licenses or any other rights to you under any Microsoft intellectual property. If you would like a license from Microsoft, you need to contact Microsoft directly (send mail to rally@microsoft.com).”

3.3 License Clarifications. The licenses granted to Licensee in this Agreement do not include any right to (i) modify the Technical Documentation, change any of the packet types or content types described in the Technical Documentation, or extend any such packet types or content types except as described in the Technical Documentation, or (ii) implement any Licensed Technology(ies) or exercise rights under any

Necessary Claims in any software other than a Licensed Implementation or to support any communications between computing devices and/or computing functions other than as expressly provided in the definition of the Authorized Purpose corresponding to the applicable Licensed Technology(ies). For the avoidance of doubt, regardless of whether a Licensed Implementation performs or is capable of performing functions other than the Authorized Purpose, the licenses set forth in Section 3.2 apply only to the performance of the Authorized Purpose corresponding to such Licensed Implementation.

3.4 Licensee Covenant Not to Sue. In consideration of the terms of this Agreement, Licensee covenants on behalf of itself and its Affiliates that it will not sue Microsoft or any Microsoft Affiliate for infringement of any claims of patents reading on any Technical Documentation (“**Licensee Patents**”) on account of any manufacture, use, sale, offer for sale, importation or other disposition or promotion, worldwide, of any Microsoft product, technology, service or portion thereof. If Licensee assigns or transfers any Licensee Patents, applications therefor, or rights to enforce the same, Licensee shall require as a condition of any such assignment that the assignee agrees to be bound by the provisions of this Section 3.4 with respect to Licensee Patents. Any purported assignment or transfer of rights in derogation of the foregoing requirements shall be null and void.

3.5 No Warranties. Licensee shall make no representation, or any express or implied warranty to third parties (including, without limitation, to any end users) on behalf of Microsoft.

3.6 Excluded Licenses. Nothing in this Agreement authorizes Licensee to subject the Licensed Technology(ies), Technical Documentation or any Microsoft intellectual property right in any Licensed Implementation to the terms of any license that requires, as a condition of use, modification or distribution of technology subject to such license, that such technology or other technology combined or distributed with such technology (a) be disclosed or distributed in source code form; (b) be licensed for the purpose of making derivative works; or (c) be re-distributable at no charge.

3.7 Reservation of Rights. All rights not expressly granted in this Agreement are reserved. No additional rights whatsoever (including, without limitation, any implied licenses) are granted by implication, estoppel or otherwise. Without limiting the generality of the foregoing, this Agreement does not grant Licensee any license or other right to use or display any name, trade name, logo, trademark or other identifier of Microsoft (provided, however, that this Agreement also does not restrict any right that Licensee may have under applicable laws to make accurate, descriptive and nominative references to Microsoft or its products in any press release, public announcement or other disclosure, including pursuant to Section 7).

4. Term and Termination

4.1 Term. The term of this Agreement shall commence as of the Effective Date and continue unless and until terminated in accordance with the provisions of this Agreement.

4.2 Termination. (a) Licensee may terminate this Agreement at any time upon written notice to Microsoft. Microsoft may terminate this Agreement (i) immediately upon written notice at any time, if Licensee is in material breach of Section 3.2(b); or (ii) if Licensee otherwise materially breaches this Agreement and fails to cure the breach within thirty (30) days after Licensee receives notice of the breach from Microsoft. (b) Upon termination, Licensee’s licenses under this Agreement shall end and Licensee shall cease all use of the Technical Documentation (including but not limited to all production and all distribution of Licensed Implementations and Licensed Products).

4.3 Survival. Sections 1, 2.2, 3.4, 3.6, 3.7, 4.2, 5.2, 6, 8 and this Section 4.3 shall survive any termination of this Agreement. Licenses granted prior to the termination of this Agreement by Licensee to end users for Licensed Implementations in accordance with the terms of this Agreement shall survive any termination of this Agreement.

5. Representations and Disclaimers of Warranty

5.1 Licensee represents and warrants that the person signing this Agreement on Licensee's behalf has all necessary power and authority to do so, and that upon such signature this Agreement is a binding obligation on Licensee.

5.2 DISCLAIMERS. THE TECHNICAL DOCUMENTATION, LICENSED TECHNOLOGY(IES) AND ALL INTELLECTUAL PROPERTY MADE AVAILABLE AND/OR LICENSED BY MICROSOFT UNDER OR IN CONNECTION WITH THIS AGREEMENT ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT DISCLAIMS ALL WARRANTIES, DUTIES AND CONDITIONS, EITHER EXPRESS, IMPLIED OR STATUTORY WITH RESPECT TO SUCH TECHNICAL DOCUMENTATION, LICENSED TECHNOLOGY(IES) AND INTELLECTUAL PROPERTY, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT.

6. Limitation of Liability

MICROSOFT SHALL NOT BE LIABLE FOR ANY DAMAGES ARISING FROM OR OTHERWISE RELATED TO THIS AGREEMENT, INCLUDING INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR SPECIAL DAMAGES, EVEN IF MICROSOFT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

7. Marketing

7.1 Press Release.

(a) Promptly following the Effective Date, Licensee will issue a press release in which Licensee announces that it has entered into a Microsoft Windows Rally Program License Agreement and describes Windows Rally technology as being intended to provide effortless, secure and reliable connectivity between devices and PCs, support for new connectivity scenarios, and richer experiences for customers.

(b) The parties may cooperate with each other on press releases and similar communications regarding the non-confidential subject matter of this Agreement. The content and specific timing of each such press release (including the press release to be issued pursuant to Section 7.1(a)) or similar public communications must be agreed upon in writing by both parties.

7.2 Microsoft Marketing Materials. Notwithstanding Section 7.1(b), Licensee consents to Microsoft's listing Licensee as a party to its Microsoft Windows Rally Program License Agreement on the Microsoft Windows Rally website, as well as in marketing materials generated by or for Microsoft.

8. Miscellaneous

8.1 No Partnership, Joint Venture or Franchise. Neither this Agreement, nor any terms and conditions contained herein, shall be construed as creating a partnership, joint venture or agency relationship or as granting a franchise as defined in the Washington Franchise Investment Protection Act, RCW 19.100, as amended, or 16 CFR Section 436.2(a), or any similar laws in other jurisdictions.

8.2 Export Regulations. Licensee acknowledges that the Technical Documentation and Licensed Implementations may be subject to U.S. export jurisdiction and other applicable national or international laws. Licensee agrees to comply with all applicable international and national laws that apply to the Technical Documentation and Licensed Implementations, including the U.S. Export Administration Regulations, as well as end-user, end-use and destination restrictions issued by U.S. and other governments, and privacy laws. See <http://www.microsoft.com/exporting/>.

8.3 Executed Agreements and Effectiveness; Notices. To be effective, executed Agreement(s) must be sent by messenger, traceable express mail or prepaid certified mail, return receipt requested, addressed to Microsoft as follows:

Microsoft Corporation
 One Microsoft Way
 Redmond, WA 98052-6399
 Attention: Windows Rally Program Manager (Scott Manchester or successor)
 Copy to: Law & Corporate Affairs

Except for the foregoing, all notices in connection with this Agreement shall be deemed given as of the day they are received either by messenger, delivery service, or in the United States of America mails, postage prepaid, certified or registered, return receipt requested, and addressed either to Licensee as stated in the box on the first page of this Agreement or to Microsoft as stated above, or to such other address as a party may designate pursuant to this notice provision.

8.4 Governing Law; Jurisdiction; Attorneys' Fees. This Agreement shall be construed and controlled by the laws of the State of Washington, and Licensee consents to exclusive jurisdiction and venue in the federal courts sitting in King County, Washington, unless no federal subject matter jurisdiction exists, in which case Licensee consents to exclusive jurisdiction and venue in the Superior Court of King County, Washington. Licensee waives all defenses of lack of personal jurisdiction and forum non conveniens. Process may be served on either party in the manner authorized by applicable law or court rule.

8.5 Assignment. Licensee shall not transfer or assign this Agreement, or any rights or obligations hereunder, whether by operation of contract, law or otherwise, except with the express written consent of Microsoft, and any attempted assignment by Licensee in violation of this Section is void. For purposes of this Agreement, an "assignment" by Licensee is deemed to include, without limitation, each of the following: (a) a change in beneficial ownership of Licensee of greater than twenty percent (20%) (whether in a single transaction or series of transactions) if Licensee is a partnership, trust, limited liability company or other like entity; (b) a merger of Licensee with another party, whether or not Licensee is the surviving entity; (c) the acquisition of more than twenty percent (20%) of any class of Licensee's voting stock (or any class of non-voting security convertible into voting stock) by another party (whether in a single transaction or series of transactions); and (d) the sale or other transfer of more than fifty percent (50%) of Licensee's assets (whether in a single transaction or series of transactions). In the event of such assignment or attempted assignment by Licensee, Microsoft may, but is not obligated to, immediately terminate this Agreement and any licenses or rights grants hereunder.

8.6 Construction. If for any reason a court of competent jurisdiction finds any provision of this agreement, or portion thereof, to be unenforceable (other than Section 3.2(b)), such provision and the rest of the Agreement will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the Agreement will continue in full force and effect. In the event that a court of competent jurisdiction finds that Section 3.2(b) is unenforceable, this entire Agreement and any licenses granted hereunder shall be rendered null and void. Failure by a party to enforce any provision of this Agreement will not be deemed a waiver of future enforcement of that or any other provision.

8.7 No Requirement to Implement. Nothing in this Agreement shall be construed as requiring Licensee to use or implement Licensed Technology(ies), or limit either party from competing in any way without infringing the intellectual property rights of the other party, including by engaging in activities, independently or with others, that may be deemed competitive with Licensed Technology(ies), Licensed Implementation(s) or Licensed Product(s).

8.8 Entire Agreement. This Agreement constitutes the entire agreement between the parties with respect to its subject matter, and merges all prior and contemporaneous communications. It shall not be modified except by a written agreement dated subsequent to the date of this Agreement and signed on behalf of Licensee and Microsoft by their respective duly authorized representatives.

By signing below Licensee agrees to the foregoing and represents that Licensee has not modified this Agreement in any way.

| | |
|-----------------|----------------|
| By (signature): | Licensee Name: |
| Name (printed): | Dated: |
| Title: | |

EXHIBIT A
LICENSED TECHNOLOGY(IES)

The Licensed Technology(ies) that Licensee has chosen to license under this Agreement are indicated by check(s) in the box(es) on the left. Each Licensed Implementation is licensed to perform only the corresponding Authorized Purpose and is subject to the further terms of this Agreement.

| | Technology | Authorized Purpose |
|--------------------------|-------------------------------|---|
| <input type="checkbox"/> | Link Layer Topology Discovery | Licensed Implementations of this Licensed Technology may use such Licensed Technology only for the following purpose: to request or respond to requests (in either case in communications with other devices that include a Licensed Implementation) for information describing (i) the device on which the Licensed Implementation is running, (ii) information about other devices connected to or which have wireless access to the same network as the device on which the Licensed Implementation is running, and (iii) characteristics about the physical media to which the device in (i) is connected. |
| <input type="checkbox"/> | PnP-X | Licensed Implementations of this Licensed Technology may use such Licensed Technology only for the following purpose: to implement the methodology described in the Technical Documentation for how specific communications protocols described in (but not licensed under) such Technical Documentation can be extended and employed to provide a plug and play experience. |
| <input type="checkbox"/> | WCN | Licensed Implementations of this Licensed Technology may use such Licensed Technology only for the following purpose: to permit the transfer of Windows Connect Now Settings to a Licensed Product from a computing device and then from such Licensed Product to other devices. |
| <input type="checkbox"/> | DPWS | <p>Licensed Implementations of this Licensed Technology may use such Licensed Technology only for the following purpose: to perform the functions of a Compliant Device or a Compliant Control Point, as defined below.</p> <ul style="list-style-type: none"> • A Compliant Device means a Licensed Product that includes a Licensed Implementation which implements the mandatory aspects of at least one DCP (as defined below) for the sole purpose of responding to requests from a Compliant Control Point. • A Compliant Control Point means a Licensed Product that includes a Licensed Implementation the sole function of which is to send requests to a Compliant Device. • A DCP means a device control protocol, including a device-specific schema described using the web-services description language, which device control protocol enables interaction between a device associated with one device class and devices associated with the same or different device classes in a networked environment. |

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.

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 is designed for the WLAN 2.4 GHz and/or 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 2,4 GHz et/ou 5 GHz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l'ARCEP, la puissance d'émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d'une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MHz.

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 (<ftp://opensource.zyxel.com>) (collectively the "Open-Sourced Components") You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part

thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the online electronic documentation for the Software (<ftp://opensource.zyxel.com>), and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5 Confidentiality

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

6 No Warranty

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

7 Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL'S AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8 Export Restrictions

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

9 Audit Rights

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

10 Termination

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

11 General

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

Note: 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 <ftp://opensource.zyxel.com> to get it.

Index

A

Address Assignment [72](#)

Advanced Encryption Standard

See AES.

AES [241](#)

AH [140](#)

algorithms [140](#)

alternative subnet mask notation [197](#)

antenna

directional [245](#)

gain [245](#)

omni-directional [245](#)

AP (access point) [235](#)

B

Bandwidth management

overview [147](#)

priority [149](#)

Basic Service Set, See BSS [233](#)

bridged APs, security [82](#)

BSS [233](#)

C

CA [240](#)

Certificate Authority

See CA.

certifications

notices [281](#)

viewing [282](#)

channel [80](#), [235](#)

interference [235](#)

Configuration

restore [168](#)

copyright [281](#)

CPU usage [57](#)

CTS (Clear to Send) [236](#)

D

Daylight saving [166](#)

DDNS [113](#)

see also Dynamic DNS

service providers [114](#)

DH [146](#)

DHCP [38](#), [99](#)

DHCP server

see also Dynamic Host Configuration Protocol

DHCP server [96](#), [99](#)

DHCP table [38](#)

DHCP client information

DHCP status

Diffie-Hellman key groups [146](#)

Dimensions [179](#)

disclaimer [281](#)

DNS [101](#)

DNS Server [72](#)

DNS server [101](#)

Domain Name System [101](#)

Domain Name System. See DNS.

duplex setting [58](#)

Dynamic DNS [113](#)

Dynamic Host Configuration Protocol [99](#)

dynamic WEP key exchange [240](#)

DynDNS [114](#)

DynDNS see also DDNS [114](#)

DynDNS Wildcard [113](#)

E

EAP Authentication [239](#)

encapsulation [141](#)

encryption [81](#), [241](#)

- and local (user) database [82](#)
- key [82](#)
- WPA compatible [82](#)

[ESP](#) [140](#)

[ESS](#) [234](#)

[ESSID](#) [175](#)

Extended Service Set, See [ESS](#) [234](#)

F

[Firewall](#) [120](#)

- Firewall overview guidelines [120](#)
- ICMP packets [121](#)
- network security
- Stateful inspection [120](#)
- ZyXEL device firewall [120](#)

firewall

- stateful inspection [119](#)

Firmware upload [166](#)

- file extension
- using HTTP

firmware version [57](#)

fragmentation threshold [236](#)

G

General wireless LAN screen [82](#)

H

hidden node [235](#)

I

[IANA](#) [202](#)

[IBSS](#) [233](#)

ID type and content [144](#)

IEEE 802.11g [237](#)

[IGMP](#) [73](#)

see also [Internet Group Multicast Protocol](#) version

[IGMP](#) version [73](#)

[IKE](#) phases [142](#)

[IKE SA](#)

- aggressive mode [125](#)

- IP address, remote IPSec router [126](#)

- IP address, ZyXEL Device [125](#)

- main mode [125](#)

- negotiation mode [125](#)

[IKE SA](#). See also [VPN](#).

[Independent Basic Service Set](#)

- See [IBSS](#) [233](#)

[initialization vector \(IV\)](#) [242](#)

[inside header](#) [141](#)

[Internet Assigned Numbers Authority](#)

- See [IANA](#) [202](#)

[Internet Group Multicast Protocol](#) [73](#)

[Internet Key Exchange](#) [142](#)

[Internet Protocol Security](#). See [IPSec](#).

[IP Address](#) [97](#), [98](#), [106](#)

[IP Pool](#) [100](#)

[IPSec](#) [124](#)

- algorithms [140](#)

- architecture [140](#)

- [NAT](#) [143](#)

[IPSec SA](#)

- authentication key (manual keys) [135](#)

- encryption key (manual keys) [135](#)

- local policy [126](#)

- manual keys [135](#)

- remote policy [126](#)

- when [IKE SA](#) is disconnected [126](#)

[IPSec SA](#). See also [VPN](#).

[IPSec](#). See also [VPN](#).

L

[LAN](#) [95](#)

- IP pool setup [96](#)

[LAN](#) overview [95](#)

[LAN](#) setup [95](#)

[LAN TCP/IP](#) [96](#)

[Link](#) type [58](#)

local (user) database [81](#)
and encryption [82](#)
Local Area Network [95](#)

M

MAC [88](#)
MAC address [72](#), [80](#)
cloning [72](#)
MAC address filter [80](#)
MAC address filtering [88](#)
MAC filter [88](#)
managing the device
good habits [22](#)
using the web configurator. See [web configurator](#).
using the WPS. See [WPS](#).
Media access control [88](#)
Memory usage [58](#)
Message Integrity Check (MIC) [241](#)
Multicast [73](#)
IGMP [73](#)

N

NAT [103](#), [106](#), [202](#)
global [104](#)
how it works [105](#)
inside [104](#)
IPSec [143](#)
local [104](#)
outside [104](#)
overview [103](#)
port forwarding [110](#)
see also [Network Address Translation](#)
server [104](#)
server sets [110](#)
traversal [144](#)
NAT Traversal [155](#)
Navigation Panel [58](#)
navigation panel [58](#)
negotiation mode [142](#)
Network Address Translation [103](#), [106](#)

O

outside header [141](#)

P

Pairwise Master Key (PMK) [242](#), [243](#)
Point-to-Point Protocol over Ethernet [75](#)
Pool Size [100](#)
Port forwarding [106](#), [110](#)
default server [106](#), [110](#)
example [110](#)
local server [106](#)
port numbers
services
port speed [58](#)
Power Specification [179](#)
PPPoE [75](#)
dial-up connection
preamble mode [237](#)
pre-shared key [145](#)
product registration [282](#)
PSK [242](#)

Q

Quality of Service (QoS) [90](#)

R

RADIUS [238](#)
message types [239](#)
messages [239](#)
shared secret key [239](#)
RADIUS server [81](#)
registration
product [282](#)
related documentation [3](#)
Remote management
and NAT [152](#)
limitations [152](#)
system timeout [153](#)

Reset button [35](#)
Reset the device [35](#)
Restore configuration [168](#)
RF (Radio Frequency) [180](#)
Roaming [90](#)
Router Mode
 status screen [56](#)
RTS (Request To Send) [236](#)
 threshold [235](#), [236](#)
RTS/CTS Threshold [80](#), [90](#)

S

safety warnings [7](#)
Scheduling [93](#)
security associations. See VPN.
Security Parameter Index [134](#)
Service and port numbers [123](#), [151](#)
Service Set [51](#), [83](#)
Service Set IDentification [51](#), [83](#)
Service Set IDentity. See SSID.
SPI [134](#)
SSID [51](#), [57](#), [80](#), [83](#)
stateful inspection firewall [119](#)
Static DHCP [100](#)
Static Route [115](#)
Status [56](#)
subnet [195](#)
Subnet Mask [97](#), [98](#)
subnet mask [196](#)
subnetting [198](#)
Summary
 DHCP table [38](#)
 Packet statistics [40](#)
 Wireless station status [41](#)
syntax conventions [5](#)
System General Setup [163](#)

T

TCP/IP configuration [99](#)
Temperature [179](#)

Temporal Key Integrity Protocol (TKIP) [241](#)
Time setting [165](#)
transport mode [141](#)
trigger port [111](#)
Trigger port forwarding [111](#)
 example [111](#)
 process [111](#)
tunnel mode [141](#)

U

Universal Plug and Play [155](#)
 Application [155](#)
 Security issues [155](#)
UPnP [155](#)
user authentication [81](#)
 local (user) database [81](#)
 RADIUS server [81](#)
User Name [114](#)

V

Virtual Private Network. See VPN.
VPN [124](#)
 established in two phases [125](#)
 IKE SA. See IKE SA.
 IPSec [124](#)
 IPSec SA. See IPSec SA.
 local network [124](#)
 remote IPSec router [124](#)
 remote network [124](#)
 security associations (SA) [125](#)
VPN. See also IKE SA, IPSec SA.

W

WAN (Wide Area Network) [71](#)
WAN MAC address [72](#)
warranty [282](#)
 note [282](#)
Web Configurator
 how to access [33](#)

- Overview [33](#)
- web configurator [22](#)
- WEP Encryption [86, 87](#)
- WEP encryption [85](#)
- WEP key [85](#)
- Wi-Fi Protected Access [241](#)
- Wildcard [113](#)
- Wireless association list [41](#)
- wireless channel [175](#)
- wireless client WPA supplicants [242](#)
- wireless LAN [175](#)
- wireless LAN scheduling [93](#)
- Wireless network
 - basic guidelines [79](#)
 - channel [80](#)
 - encryption [81](#)
 - example [79](#)
 - MAC address filter [80](#)
 - overview [79](#)
 - security [80](#)
 - SSID [80](#)
- Wireless security [80](#)
 - overview [80](#)
 - type [80](#)
- wireless security [175, 237](#)
- Wireless tutorial [61](#)
- WLAN
 - interference [235](#)
 - security parameters [244](#)
- WPA [241](#)
 - key caching [242](#)
 - pre-authentication [242](#)
 - user authentication [242](#)
 - vs WPA-PSK [242](#)
 - wireless client supplicant [242](#)
 - with RADIUS application example [243](#)
- WPA compatible [82](#)
- WPA2 [241](#)
 - user authentication [242](#)
 - vs WPA2-PSK [242](#)
 - wireless client supplicant [242](#)
 - with RADIUS application example [243](#)
- WPA2-Pre-Shared Key [241](#)
- WPA2-PSK [241, 242](#)
 - application example [243](#)
- WPA-PSK [241, 242](#)
 - application example [243](#)
- WPS [22](#)

Federal Communication Commission Interference Statement

This equipment 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 equipment 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 equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with FCC 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.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

以下警語適用台灣地區

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。

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，指依電信法規定作業之無線電通信。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。

在5.25-5.35 GHz頻帶內操作之無線資訊傳輸設備，限於室內使用。