



NBG4615 v2

Wireless N300 Gigabit NetUSB Router

Version 1.00
Edition 1, 09/2012

User's Guide

Default Login Details

LAN IP Address	http://192.168.1.1
Password	1234

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

The Quick Start Guide shows how to connect the NBG4615 v2 and access the Web Configurator wizards. It contains information on setting up your network and configuring for Internet access.

Contents Overview

User's Guide	13
Introduction	15
ZyXEL NetUSB Share Center Utility	21
Connection Wizard	27
Introducing the Web Configurator	39
NBG4615 v2 Modes	43
Easy Mode	45
Router Mode	57
Access Point Mode	63
Universal Repeater Mode	71
WISP Mode	81
WISP + Universal Repeater Mode	91
Tutorials	97
Technical Reference	117
Monitor	119
WAN	125
Wireless LAN	135
LAN	157
DHCP Server	161
NAT	167
DDNS	177
Static Route	179
Firewall	183
Content Filtering	189
Bandwidth Management	193
Remote Management	201
Universal Plug-and-Play (UPnP)	205
Maintenance	211
Troubleshooting	223

Table of Contents

Contents Overview	3
Table of Contents	5
 Part I: User's Guide	 13
Chapter 1	
Introduction.....	15
1.1 Overview	15
1.2 Applications	15
1.3 Ways to Manage the NBG4615 v2	15
1.4 Good Habits for Managing the NBG4615 v2	16
1.5 Resetting the NBG4615 v2	16
1.5.1 How to Use the RESET Button	16
1.6 The WPS Button	16
1.7 LEDs	17
1.8 Wall Mounting	18
 Chapter 2	
ZyXEL NetUSB Share Center Utility.....	21
2.1 Overview	21
2.1.1 Quick Setup	21
2.1.2 Installing ZyXEL NetUSB Share Center Utility	21
2.2 The ZyXEL NetUSB Share Center Utility	22
2.2.1 The Menus	23
2.2.2 The ZyXEL NetUSB Share Center Configuration Window	24
2.2.3 The Auto-Connect Printer List Window	25
2.2.4 Exit the ZyXEL NetUSB Share Center Utility	26
 Chapter 3	
Connection Wizard	27
3.1 Overview	27
3.2 Accessing the Wizard	27
3.3 Connect to Internet	28
3.3.1 Connection Type: IPoE	29
3.3.2 Connection Type: PPPoE	30
3.3.3 Connection Type: PPTP	32
3.4 Router Password	33

3.5 Wireless Security	34
3.5.1 Wireless Security: No Security	34
3.5.2 Wireless Security: WPA2-PSK	35
Chapter 4	
Introducing the Web Configurator	39
4.1 Overview	39
4.2 Accessing the Web Configurator	39
4.2.1 Login Screen	39
4.2.2 Password Screen	40
Chapter 5	
NBG4615 v2 Modes	43
5.1 Overview	43
5.1.1 Web Configurator Modes	43
5.1.2 Device Modes	43
Chapter 6	
Easy Mode	45
6.1 Overview	45
6.2 What You Can Do	46
6.3 What You Need to Know	46
6.4 Navigation Panel	47
6.5 Network Map	47
6.6 Control Panel	48
6.6.1 Game Engine	49
6.6.2 Power Saving	50
6.6.3 Content Filter	50
6.6.4 Bandwidth MGMT	51
6.6.5 Firewall	52
6.6.6 Wireless Security	52
6.6.7 WPS	53
6.7 Status Screen in Easy Mode	54
Chapter 7	
Router Mode	57
7.1 Overview	57
7.2 Router Mode Status Screen	57
7.2.1 Navigation Panel	60
Chapter 8	
Access Point Mode	63
8.1 Overview	63

8.2 What You Can Do	63
8.3 What You Need to Know	63
8.3.1 Setting your NBG4615 v2 to AP Mode	64
8.3.2 Accessing the Web Configurator in Access Point Mode	64
8.3.3 Configuring your WLAN and Maintenance Settings	65
8.4 AP Mode Status Screen	65
8.4.1 Navigation Panel	67
8.5 LAN Screen	67
Chapter 9	
Universal Repeater Mode.....	71
9.1 Overview	71
9.2 What You Can Do	71
9.3 What You Need to Know	72
9.4 Setting your NBG4615 v2 to Universal Repeater Mode	72
9.5 Universal Repeater Mode Status Screen	73
9.5.1 Navigation Panel	75
9.6 Universal Repeater Screen	75
9.6.1 No Security	76
9.6.2 Static WEP	76
9.6.3 WPA(2)-PSK	78
9.7 Site Survey Screen	78
Chapter 10	
WISP Mode	81
10.1 Overview	81
10.2 What You Can Do	81
10.3 What You Need to Know	82
10.3.1 Setting your NBG4615 v2 to WISP Mode	82
10.3.2 Accessing the Web Configurator in WISP Mode	82
10.4 WISP Mode Status Screen	83
10.4.1 Navigation Panel	85
10.5 Wireless LAN General Screen	85
10.5.1 No Security	86
10.5.2 Static WEP	87
10.5.3 WPA(2)-PSK	88
10.6 Site Survey Screen	89
Chapter 11	
WISP + Universal Repeater Mode.....	91
11.1 Overview	91
11.2 What You Can Do	91
11.3 What You Need to Know	92

11.3.1 Setting your NBG4615 v2 to WISP + UR Mode	92
11.3.2 Accessing the Web Configurator in WISP + UR Mode	93
11.4 WISP + UR Mode Status Screen	93
11.4.1 Navigation Panel	96
Chapter 12	
Tutorials.....	97
12.1 Overview	97
12.2 Set Up a Wireless Network with WPS	97
12.2.1 Push Button Configuration (PBC)	97
12.2.2 PIN Configuration	98
12.3 Configure Wireless Security without WPS	99
12.3.1 Configure Your Notebook	101
12.4 Using Multiple SSIDs on the NBG4615 v2	103
12.4.1 Configuring Security Settings of Multiple SSIDs	104
12.5 Connecting the NBG4615 v2 to an AP or Wireless Router	108
12.6 Connecting to USB Storage with the ZyXEL NetUSB Share Center Utility	111
12.6.1 Multiple Connections to the USB Device	112
12.7 Automatically Connecting to a USB Printer	114
 Part II: Technical Reference.....	 117
Chapter 13	
Monitor.....	119
13.1 Overview	119
13.2 What You Can Do	119
13.3 The Log Screen	119
13.3.1 View Log	119
13.4 DHCP Table	120
13.5 Packet Statistics	121
13.6 WLAN Station Status	122
 Chapter 14	
WAN	125
14.1 Overview	125
14.2 What You Can Do	125
14.3 What You Need To Know	125
14.3.1 Configuring Your Internet Connection	126
14.3.2 Multicast	127
14.4 Internet Connection	127
14.4.1 IPoE Encapsulation	127

14.4.2 PPPoE Encapsulation	129
14.4.3 PPTP Encapsulation	131
14.5 Advanced WAN Screen	134

Chapter 15

Wireless LAN..... 135

15.1 Overview	135
15.1.1 What You Can Do	136
15.1.2 What You Should Know	136
15.2 General Wireless LAN Screen	140
15.3 Wireless Security	142
15.3.1 No Security	142
15.3.2 WEP Encryption	142
15.3.3 WPA-PSK/WPA2-PSK	144
15.3.4 WPA/WPA2	145
15.4 More AP Screen	147
15.4.1 More AP Edit	148
15.5 MAC Filter Screen	150
15.6 Wireless LAN Advanced Screen	152
15.7 Quality of Service (QoS) Screen	152
15.8 WPS Screen	153
15.9 WPS Station Screen	155
15.10 Scheduling Screen	155

Chapter 16

LAN 157

16.1 Overview	157
16.2 What You Can Do	157
16.3 What You Need To Know	157
16.3.1 IP Pool Setup	158
16.3.2 LAN TCP/IP	158
16.3.3 IP Alias	158
16.4 LAN IP Screen	158
16.5 IP Alias Screen	159

Chapter 17

DHCP Server 161

17.1 Overview	161
17.1.1 What You Can Do	161
17.1.2 What You Need To Know	161
17.2 DHCP Server General Screen	161
17.3 DHCP Server Advanced Screen	162
17.4 DHCP Client List Screen	164

Chapter 18	
NAT.....	167
18.1 Overview	167
18.1.1 What You Can Do	167
18.1.2 What You Need To Know	168
18.2 General	169
18.3 Port Forwarding Screen	170
18.3.1 Port Forwarding Edit Screen	172
18.4 Port Trigger Screen	173
18.5 Technical Reference	174
18.5.1 NATPort Forwarding: Services and Port Numbers	174
18.5.2 NAT Port Forwarding Example	174
18.5.3 Trigger Port Forwarding	175
18.5.4 Trigger Port Forwarding Example	175
18.5.5 Two Points To Remember About Trigger Ports	176
 Chapter 19	
DDNS.....	177
19.1 Overview	177
19.1.1 What You Need To Know	177
19.2 General	177
 Chapter 20	
Static Route.....	179
20.1 Overview	179
20.2 IP Static Route Screen	179
20.2.1 Add/Edit Static Route	180
 Chapter 21	
Firewall	183
21.1 Overview	183
21.1.1 What You Can Do	183
21.1.2 What You Need To Know	183
21.2 General Screen	185
21.3 Services Screen	185
 Chapter 22	
Content Filtering.....	189
22.1 Overview	189
22.1.1 What You Need To Know	189
22.2 Content Filter	189
22.3 Technical Reference	191
22.3.1 Customizing Keyword Blocking URL Checking	191

Chapter 23	
Bandwidth Management.....	193
23.1 Overview	193
23.2 What You Can Do	193
23.3 What You Need To Know	194
23.4 General Screen	194
23.5 Advanced Screen	194
23.5.1 Rule Configuration: Application Rule Configuration	196
23.5.2 Rule Configuration: User Defined Service Rule Configuration	197
23.5.3 Predefined Bandwidth Management Services	199
Chapter 24	
Remote Management.....	201
24.1 Overview	201
24.2 What You Can Do in this Chapter	201
24.3 What You Need to Know	201
24.3.1 Remote Management and NAT	202
24.3.2 System Timeout	202
24.4 WWW Screen	202
24.5 Telnet Screen	203
24.6 Wake On LAN Screen	203
Chapter 25	
Universal Plug-and-Play (UPnP).....	205
25.1 Overview	205
25.2 What You Need to Know	205
25.2.1 NAT Traversal	205
25.2.2 Cautions with UPnP	205
25.3 UPnP Screen	206
25.4 Technical Reference	206
25.4.1 Using UPnP in Windows XP Example	206
25.4.2 Web Configurator Easy Access	208
Chapter 26	
Maintenance	211
26.1 Overview	211
26.2 What You Can Do	211
26.3 General Screen	211
26.4 Password Screen	212
26.5 Time Setting Screen	213
26.6 Firmware Upgrade Screen	214
26.7 Configuration Backup/Restore Screen	216
26.8 Restart Screen	217

26.9 Language Screen	217
26.10 System Operation Mode Overview	218
26.11 Sys OP Mode Screen	220
Chapter 27	
Troubleshooting.....	223
27.1 Overview	223
27.2 Power, Hardware Connections, and LEDs	223
27.3 NBG4615 v2 Access and Login	224
27.4 Internet Access	226
27.5 Resetting the NBG4615 v2 to Its Factory Defaults	227
27.6 Wireless Router/AP Troubleshooting	227
27.7 USB Device Problems	229
27.8 ZyXEL Share Center Utility Problems	230
Appendix A Pop-up Windows, JavaScript and Java Permissions	231
Appendix B IP Addresses and Subnetting.....	241
Appendix C Setting Up Your Computer's IP Address	251
Appendix D Wireless LANs.....	279
Appendix E Common Services	293
Appendix F Legal Information.....	297
Index	303

PART I

User's Guide

Introduction

1.1 Overview

This chapter introduces the main features and applications of the NBG4615 v2.

The NBG4615 v2 extends the range of your existing wired network without additional wiring, providing easy network access to mobile users. You can set up a wireless network with other IEEE 802.11b/g/n compatible devices.

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

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.

1.2 Applications

You can have the following networks using the NBG4615 v2:

- **Wired.** You can connect network devices via the Ethernet ports of the NBG4615 v2 so that they can communicate with each other and access the Internet.
- **Wireless.** Wireless clients can connect to the NBG4615 v2 to access network resources. You can use WPS (WiFi Protected Setup) to create an instant network connection with another WPS-compatible device.
- **WAN.** Connect to a broadband modem/router for Internet access.
- **NetUSB.** The NBG4615 v2 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 network.

1.3 Ways to Manage the NBG4615 v2

Use any of the following methods to manage the NBG4615 v2.

- **WPS (Wi-Fi Protected Setup).** You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your ZyXEL Device.
- **Web Configurator.** This is recommended for everyday management of the NBG4615 v2 using a (supported) web browser.

1.4 Good Habits for Managing the NBG4615 v2

Do the following things regularly to make the NBG4615 v2 more secure and to manage the NBG4615 v2 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 NBG4615 v2 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG4615 v2. You could simply restore your last configuration.

1.5 Resetting the NBG4615 v2

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 NBG4615 v2 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".

1.5.1 How to Use the RESET Button


- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for one to four seconds to restart/reboot the NBG4615 v2.
- 3 Press the **RESET** button for longer than five seconds to set the NBG4615 v2 back to its factory-default configurations.

1.6 The WPS Button

Your NBG4615 v2 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.

You can use the WPS button () on the front panel of the NBG4615 v2 to activate WPS in order to quickly set up a wireless network with strong security.

- 1 Make sure the power LED is on (not blinking).
- 2 Press the WPS button for more than three seconds and release it. Press the WPS button on another WPS-enabled device within range of the NBG4615 v2.

Note: You must activate WPS in the NBG4615 v2 that acts as the AP and in another wireless device within two minutes of each other.

For more information on using WPS, see [Section 12.2 on page 97](#).

1.7 LEDs

Figure 1 Front Panel



The following table describes the LEDs.

Table 1 Front panel LEDs

LED	COLOR	STATUS	DESCRIPTION
Power	Green	On	The NBG4615 v2 is receiving power and functioning properly.
	Off		The NBG4615 v2 is not receiving power.
WAN	Green	On	The NBG4615 v2's WAN connection is ready.
		Blinking	The NBG4615 v2 is sending/receiving data through the WAN.
	Off		The WAN connection is not ready, or has failed.

Table 1 Front panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
LAN 1-4	Green	On	The NBG4615 v2's LAN connection is ready.
		Blinking	The NBG4615 v2 is sending/receiving data through the LAN.
	Off		The LAN connection is not ready, or has failed.
WLAN	Green	On	The NBG4615 v2 is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The NBG4615 v2 is sending/receiving data through the wireless LAN.
	Off		The wireless LAN is not ready or has failed.
WPS	Green	On	WPS is enabled.
		Blinking	The NBG4615 v2 is negotiating a WPS connection with a wireless client.
	Off		WPS is disabled.
USB	Green	On	The NBG4615 v2 has a USB device installed.
	Off		There is no USB device connected to the NBG4615 v2.

1.8 Wall Mounting

You may need screw anchors if mounting on a concrete or brick wall.

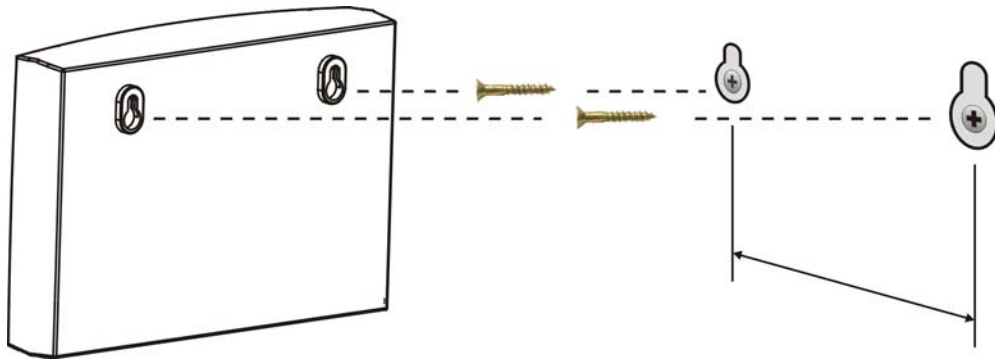
Table 2 Wall Mounting Information

Distance between holes	12 cm
M4 Screws	Two
Screw anchors (optional)	Two

- 1 Select a position free of obstructions on a wall strong enough to hold the weight of the device.
- 2 Mark two holes on the wall at the appropriate distance apart for the screws.

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

- 3 If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.
If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap of about 0.5 cm.
- 4 Make sure the screws are fastened well enough to hold the weight of the NBG4615 v2 with the connection cables.
- 5 Align the holes on the back of the NBG4615 v2 with the screws on the wall. Hang the NBG4615 v2 on the screws.

Figure 2 Wall Mounting Example

ZyXEL NetUSB Share Center Utility

2.1 Overview

The ZyXEL NetUSB Share Center Utility allows you to work with the USB devices that are connected directly to the NBG4615 v2 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 NBG4615 v2 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.

2.1.1 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 NBG4615 v2.
- 2 Connect a USB device to the USB port on the NBG4615 v2.
- 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.

2.1.2 Installing ZyXEL NetUSB Share Center Utility

Before you can access USB devices connected to the NBG4615 v2, 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.

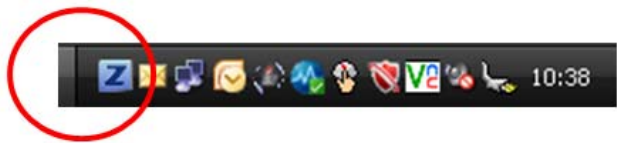
Note: In order to properly use the utility with your NBG4615 v2, ensure that the NBG4615 v2 firmware is version v1.00(AAFI.0) or higher. See [Chapter 26 on page 214](#) for information on updating your device's firmware.

To install the ZyXEL NetUSB Share Center Utility:

- 1 Insert the disc that came with your NBG4615 v2 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), and Mac OS X 10.6.

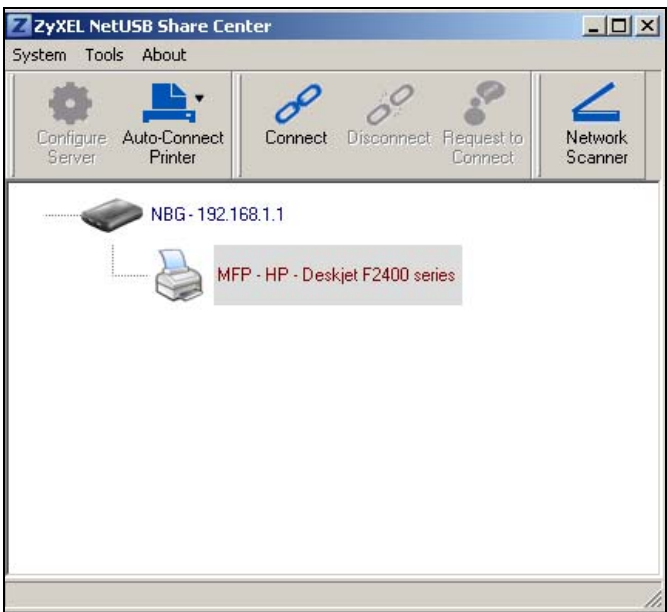
- 3 To open the ZyXEL NetUSB Share Center Utility, double-click its system tray icon.



2.2 The ZyXEL NetUSB Share Center Utility

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

Figure 3 ZyXEL NetUSB Share Center Utility Main Window



The following table describes the icons in this window.

Table 3 ZyXEL NetUSB Share Center Utility Main Window Icons







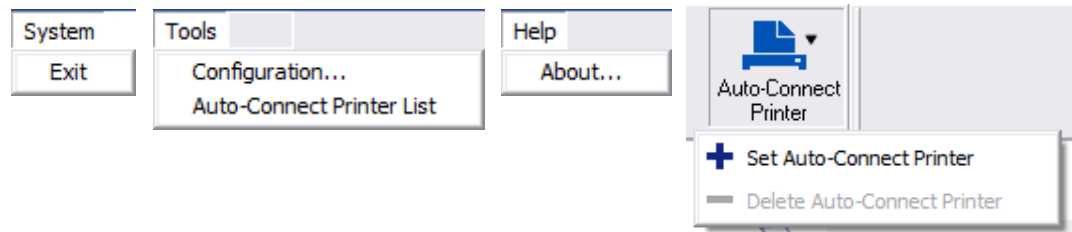
ICON	DESCRIPTION
	<p>Configure Server</p> <p>Click to open the NBG4615 v2's built-in Web Configurator, which you can use to set up the NBG4615 v2 (see Chapter 4 on page 39 for details).</p>
	<p>Auto-Connect Printer</p> <p>You can set the selected printer to 'auto-connect' after you have connected it to your computer during initial connection. If the printer is auto-connected to your computer, they will always be connected over the network. You do not need to configure it manually each time.</p> <p>Note: If the computer is connecting to the shared USB printer for the first time, you need to click Connect and setup the printer before you can use the Auto-Connect Printer function. See Chapter 12 on page 114 for more details.</p> <p>Note: You first must install the appropriate drivers for the printer that you intend to use.</p>

Table 3 ZyXEL NetUSB Share Center Utility Main Window Icons (continued)

ICON	DESCRIPTION
	Connect 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 NBG4615 v2.
	Disconnect Select a device to which your computer is connected and then click this button to disconnect from it.
	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.

2.2.1 The Menus

This section describes the utility's menus.

Figure 4 ZyXEL NetUSB Share Center Utility Menus

The following table describes the menus in this screen.

Table 4 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 NBG4615 v2.
Help	About	This opens the about window, which provides information of the utility software and driver versions.

Table 4 ZyXEL NetUSB Share Center Utility Main Screen Menus (continued)

MENU	ITEM	DESCRIPTION
Auto-Connect Printer	Set Auto-Connect Printer	<p>You can set the selected printer to 'auto-connect' after you have connected it to your computer during initial connection. If the printer is auto-connected to your computer, they will always be connected over the network. You do not need to configure it manually each time.</p> <p>Click this to show your installed printer list and select the one you want to set as auto-connected.</p> <p>Note: If the computer is connecting to the shared USB printer for the first time, you need to click Connect and setup the printer before you can use the Auto-Connect Printer function. See Chapter 12 on page 114 for more details.</p> <p>Note: You first must install the appropriate drivers for the printer that you intend to use.</p>
	Delete Auto-Connect Printer	This removes the auto-connect option from the selected printer.

2.2.2 The ZyXEL NetUSB 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 NBG4615 v2.

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

Figure 5 ZyXEL NetUSB Share Center Utility Configuration Window



The following table describes the labels in this window.

Table 5 ZyXEL NetUSB Share Center Utility Configuration Window

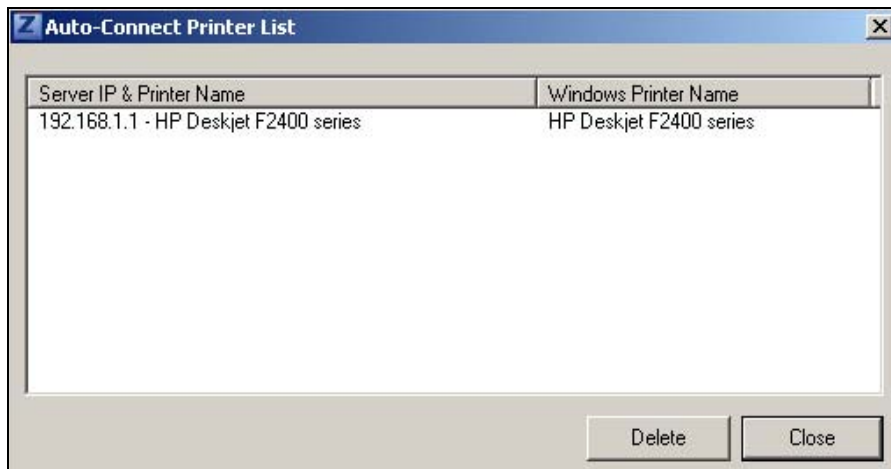
LABEL	DESCRIPTION
Basic	Select this to run the utility automatically when you log into or start up Windows.
Language	Select a language for the ZyXEL NetUSB Share Center Utility. You must restart the utility for the change to take effect.
OK	Click this to save your changes and close the window.
Cancel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

2.2.3 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.

Note: If the computer is connecting to the shared USB printer for the first time, you need to click **Connect** and setup the printer before you can use the **Auto-Connect Printer** function. See [Chapter 12 on page 114](#) for more details.

Figure 6 ZyXEL NetUSB Share Center Utility Auto-Connect Printer List Window



The following table describes the labels in this screen.

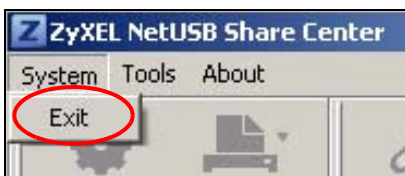
Table 6 ZyXEL NetUSB Share Center Utility Auto-Connect Printer List Window

LABEL	DESCRIPTION
Server IP & Printer Name	Displays a list of print server IPs and printer names connected to this NBG4615 v2.
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.

2.2.4 Exit the ZyXEL NetUSB Share Center Utility

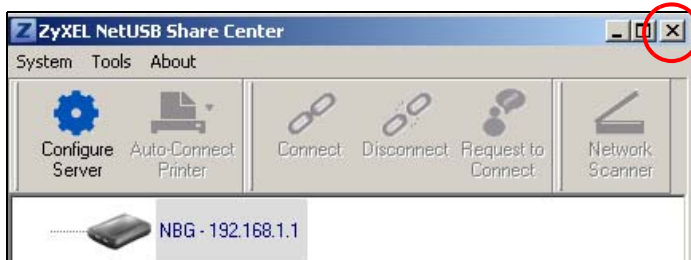
If you want to exit the ZyXEL NetUSB Share Center Utility when your computer is not connected to any USB device, follow the steps below:

- 1 Click **System > Exit** on the Utility screen. The Utility will automatically close.



Or you can close the Utility screen first, then exit:

- 1 Click the **X** on the upper-right corner of the Utility:



- 2 This will close the Utility screen to an icon at the system tray of your computer. Right-click on the Utility's icon and click **Exit**.



Connection Wizard

3.1 Overview

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

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

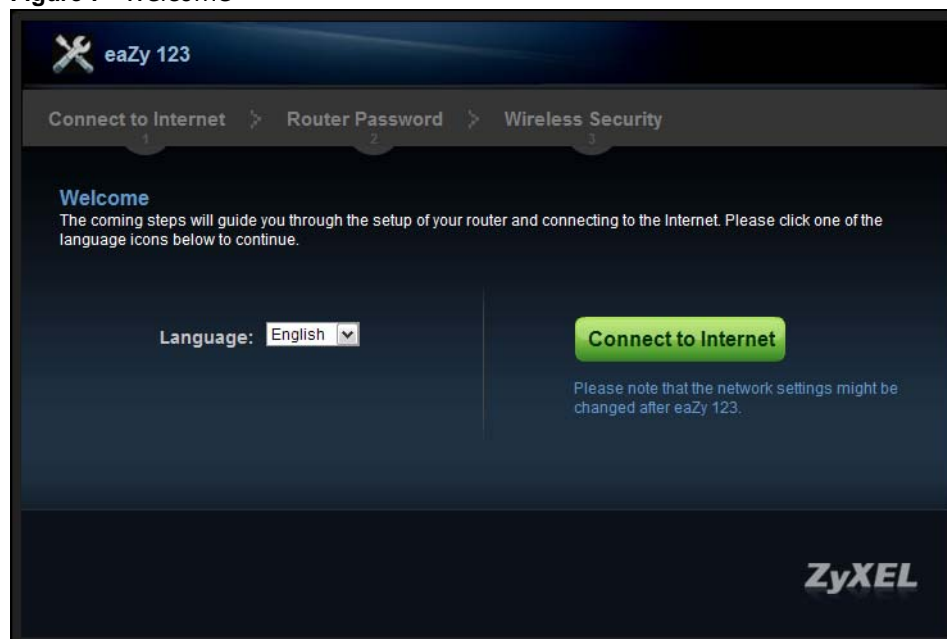
3.2 Accessing the Wizard

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

Note: The Wizard appears when the NBG4615 v2 is accessed for the first time or when you reset the NBG4615 v2 to its default factory settings.

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

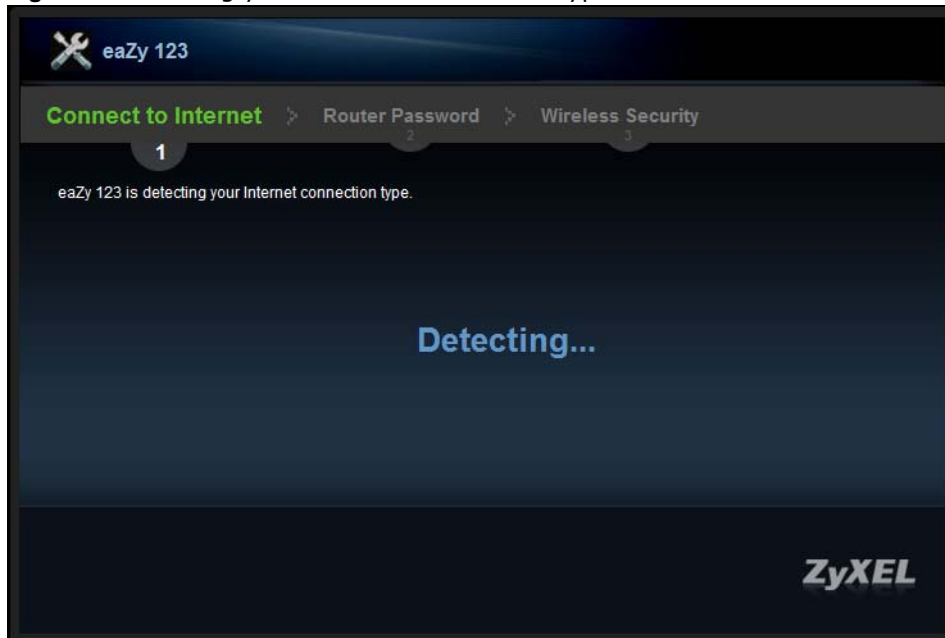
Figure 7 Welcome



3.3 Connect to Internet

The NBG4615 v2 offers three Internet connection types. They are **IPoE**, **PPPoE** or **PPTP**. The wizard attempts to detect which WAN connection type you are using.

Figure 8 Detecting your Internet Connection Type



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

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

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

Figure 9 Internet Connection Type

eaZy 123

Connect to Internet > Router Password > Wireless Security

1

Internet Connection Type : IPoE

Please refer to the information provided by your Internet Service Provider (ISP) and complete the following blanks.

☒ Obtain an IP Address Automatically ☐ Static IP Address

IP Address :

Subnet Mask :

Gateway IP address :

Exit Back Next

ZyXEL

Your NBG4615 v2 detects the following Internet Connection type.

Table 7 Internet Connection Type

CONNECTION TYPE	DESCRIPTION
IPoE	Select the IPoE (IP over Ethernet) option when the WAN port is used as a regular Ethernet.
PPPoE	Select the PPPoE (Point-to-Point Protocol over Ethernet) option for a dial-up connection.
PPTP	Select the PPTP (Point-to-Point Tunneling Protocol) option for a dial-up connection, and your ISP gave you an IP address and/or subnet mask.

3.3.1 Connection Type: IPoE

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

Figure 10 Internet Connection Type: IPoE

The following table describes the labels in this screen.

Table 8 Internet Connection Type: IPoE

LABEL	DESCRIPTION
Internet Connection Type	Select the IPoE option.
Obtain an IP Address Automatically	Select this radio button if your ISP did not assign you a fixed IP address.
Static IP Address	Select this radio button if your ISP assigned an IP address for your Internet connection.
IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the IP subnet mask in this field.
Gateway IP Address	Enter the gateway IP address in this field.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

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

3.3.2 Connection Type: PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

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

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

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

By implementing PPPoE directly on the NBG4615 v2 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG4615 v2 does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Figure 11 Internet Connection Type: PPPoE

The following table describes the labels in this screen.

Table 9 Internet Connection Type: PPPoE

LABEL	DESCRIPTION
Internet Connection Type	Select the PPPoE option for a dial-up connection.
Get automatically from ISP	Select this radio button if your ISP did not assign you a fixed IP address.
Use Fixed IP Address	Select this radio button, provided by your ISP to give the NBG4615 v2 a fixed, unique IP address.
PPP Username	Type the user name given to you by your ISP.
PPP Password	Type the password associated with the user name above.
My WAN IP Address	Type the name of your service provider.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

3.3.3 Connection Type: PPTP

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

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

Refer to the appendix for more information on PPTP.

The NBG4615 v2 supports one PPTP server connection at any given time.

Figure 12 Internet Connection Type: PPTP

The screenshot shows the 'Connect to Internet' configuration screen on a ZyXEL router. The 'Internet Connection Type' is set to 'PPTP'. Below this, there are two radio buttons: 'Obtain an IP Address Automatically' (selected) and 'Static IP Address'. The 'Obtain an IP Address Automatically' section includes fields for 'PPTP Username', 'PPTP Password', 'PPTP Server IP Address', 'IP Address', 'Subnet Mask', and 'Gateway IP address'. The 'Static IP Address' section is currently inactive. At the bottom right, there are 'Exit', 'Back', and 'Next' buttons.

The following table describes the fields in this screen

Table 10 Internet Connection Type: PPTP

LABEL	DESCRIPTION
Internet Connection Type	Select PPTP from the drop-down list box. To configure a PPTP client, you must configure the PPTP Username and PPTP Password fields for a PPP connection and the PPTP parameters for a PPTP connection.
Obtain an IP Address Automatically	Select this radio button if your ISP did not assign you a fixed IP address.
Static IP Address	Select this radio button if your ISP assigned an IP address for your Internet connection.
PPTP Username	Type the user name given to you by your ISP.
PPTP Password	Type the password associated with the User Name above.
PPTP Server IP Address	Type the server IP address of the PPTP server.
IP Address	Type the (static) IP address assigned to you by your ISP.
Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Gateway IP Address	Type the gateway IP address of the PPTP server.

Table 10 Internet Connection Type: PPTP (continued)

LABEL	DESCRIPTION
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

The NBG4615 v2 connects to the Internet.

Figure 13 Connecting to the Internet

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

3.4 Router Password

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

Figure 14 Router PasswordThe image shows a web-based configuration interface for a ZyXEL router. At the top, there is a header with a wrench icon and the text 'eaZy 123'. Below this is a navigation bar with three steps: 'Connect to Internet' (marked with a green check and the number 1), 'Router Password' (highlighted in green with the number 2), and 'Wireless Security' (marked with the number 3). The main content area is titled 'Change router password' in blue. Below the title, a message states: 'It is highly recommended to have a new administrator password instead of the factory default one (1234)'. There are two input fields: 'New Password :' and 'Retype to Confirm :', both containing four dots to represent masked characters. At the bottom right of the main area are three buttons: 'Exit', 'Back', and 'Next'. The ZyXEL logo is in the bottom right corner of the interface.

3.5 Wireless Security

Configure Wireless Settings. Configure the wireless network settings on your NBG4615 v2 in the following screen. The fields that show up depend on the kind of security you select.

3.5.1 Wireless Security: No Security

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

Figure 15 Wireless Security: No Security

The following table describes the labels in this screen.

Table 11 Wireless Security: No Security

LABEL	DESCRIPTION
Wireless Network Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the NBG4615 v2, make sure all wireless stations use the same SSID in order to access the network.
Security Mode	Select a security level from the drop-down list box. Choose No Security to have no wireless LAN security configured. If you do not enable any wireless security on your NBG4615 v2, your network is accessible to any wireless networking device that is within range.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

3.5.2 Wireless Security: WPA2-PSK

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

Figure 16 Wireless Security: WPA2-PSK



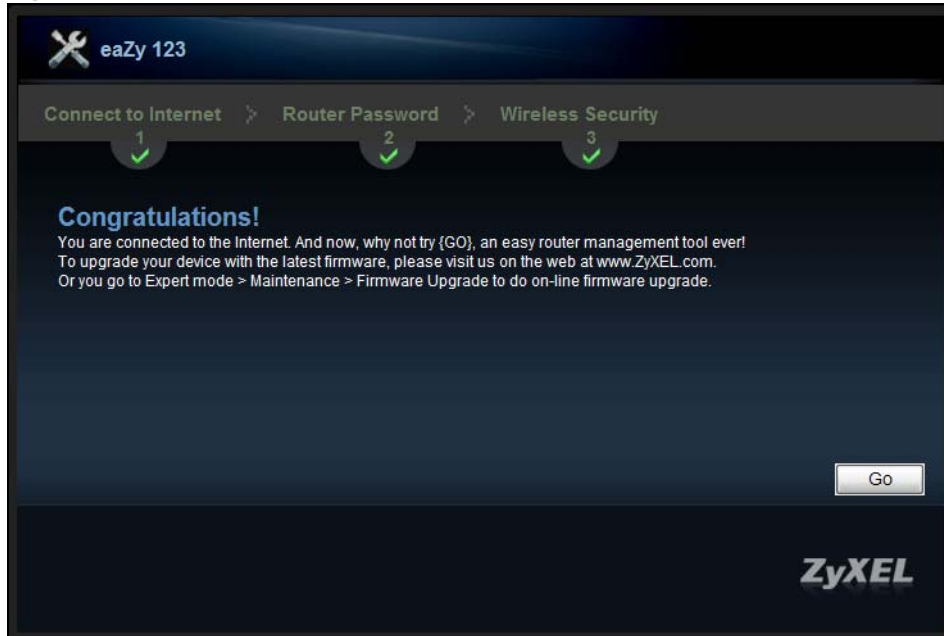
The following table describes the labels in this screen.

Table 12 Wireless Security: WPA2-PSK

LABEL	DESCRIPTION
Wireless Network Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the NBG4615 v2, make sure all wireless stations use the same SSID in order to access the network.
Security Mode	Select a security level from the drop-down list box. Choose WPA2-PSK security to configure a Pre-Shared Key. Choose this option only if your wireless clients support WPA2-PSK.
Wireless password	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the wireless LAN screens.
Verify Password	Retype the password to confirm.
Exit	Click this to close the wizard screen without saving.
Back	Click this to return to the previous screen.
Next	Click this to continue.

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

Note: If you cannot access the Internet when your computer is connected to one of the NBG4615 v2's LAN ports, check your connections. Then turn the NBG4615 v2 off, wait for a few seconds then turn it back on. If that does not work, log in to the web configurator again and check you have typed all information correctly. See the User's Guide for more suggestions.

Figure 17 Congratulations

You can also click **GO** to open the **Easy Mode** Web Configurator of your NBG4615 v2.

You have successfully set up your NBG4615 v2 to operate on your network and access the Internet. You are now ready to connect wirelessly to your NBG4615 v2 and access the Internet.

Introducing the Web Configurator

4.1 Overview

This chapter describes how to access the NBG4615 v2 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 NBG4615 v2 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 27 on page 223](#)) to see how to make sure these functions are allowed in Internet Explorer.

4.2 Accessing the Web Configurator

- 1 Make sure your NBG4615 v2 hardware is properly connected and prepare your computer or computer network to connect to the NBG4615 v2 (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 The NBG4615 v2 is in router mode by default. Type "http://192.168.1.1" as the website address. If the NBG4615 v2 is in access point or universal repeater, the IP address is 192.168.1.2. See [Chapter 5 on page 43](#) for more information about the modes of the NBG4615 v2.

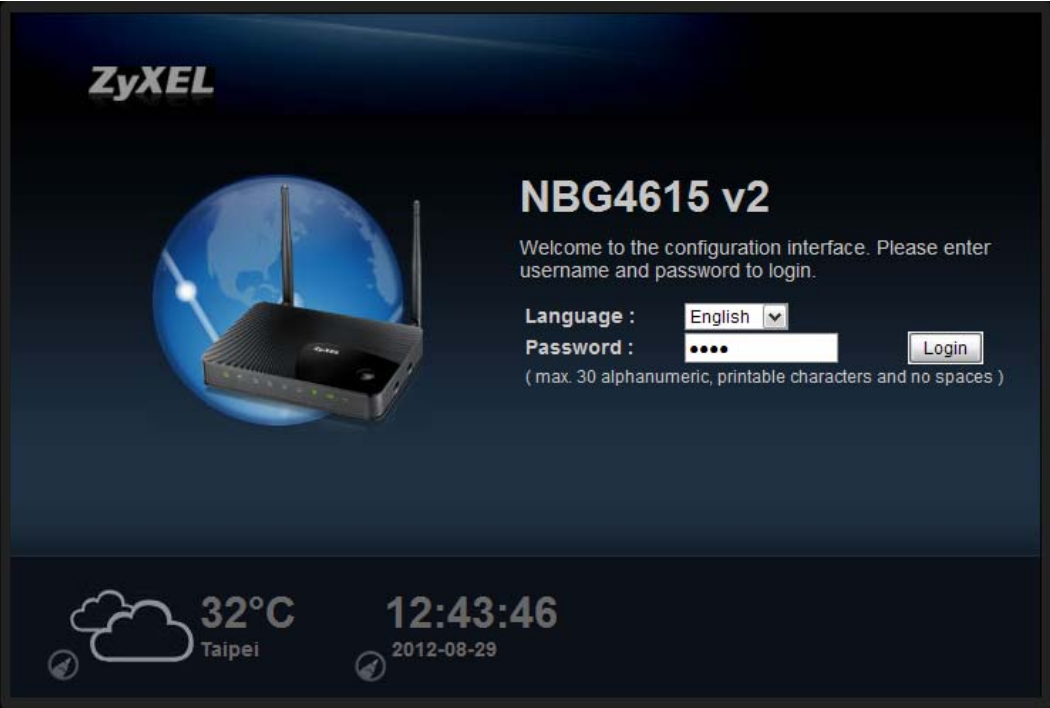
Your computer must be in the same subnet in order to access this website address.

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 3 on page 27](#) for the Connection Wizard screens.


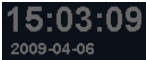
The Web Configurator initially displays the following login screen.

Figure 18 Login screen



The following table describes the labels in this screen.

Table 13 Login screen

LABEL	DESCRIPTION
Password	Type "1234" (default) as the password.
Language	Select the language you want to use to configure the Web Configurator. Click Login .
	This shows the current weather, either in celsius or fahrenheit, of the city you specify in Section 4.2.2.1 on page 41 .
	This shows the time (hh:mm:ss) and date (yyyy:mm:dd) of the timezone you select in Section 4.2.2.2 on page 42 or Section 26.5 on page 213 . The time is in 24-hour format, for example 15:00 is 3:00 PM.

4.2.2 Password Screen

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

Figure 19 Change Password Screen

The following table describes the labels in this screen.

Table 14 Change Password Screen

LABEL	DESCRIPTION
New Password	Type a new password.
Retype to Confirm	Retype the password for confirmation.
Apply	Click Apply to save your changes back to the NBG4615 v2.
Ignore	Click Ignore if you do not want to change the password this time.

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes; go to [Chapter 26 on page 211](#) to change this). Simply log back into the NBG4615 v2 if this happens.

4.2.2.1 Weather Edit

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


Click the  icon to change the Weather display.

Figure 20 Change Weather

The following table describes the labels in this screen.

Table 15 Change Weather

LABEL	DESCRIPTION
Change Unit	Choose which temperature unit you want the NBG4615 v2 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.

4.2.2.2 Time/Date Edit

One timezone can cover more than one country. You can choose a particular country in which the NBG4615 v2 is located and have the NBG4615 v2 display and use the current time and date for its logs.


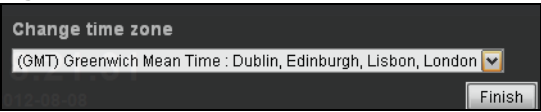
Click the  icon to change the time and date display.

Figure 21 Change Password Screen



The following table describes the labels in this screen.

Table 16 Change Password Screen

LABEL	DESCRIPTION
Change time zone	Select the specific country whose current time and date you want the NBG4615 v2 to display.
Finish	Click this to apply the settings and refresh the weather display.

Note: You can also edit the timezone in [Section 26.5 on page 213](#).

NBG4615 v2 Modes

5.1 Overview

This chapter introduces the different modes available on your NBG4615 v2. 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 NBG4615 v2 features.
- **Device mode.** This is the operating mode of your NBG4615 v2, or simply how the NBG4615 v2 is being used in the network.

5.1.1 Web Configurator Modes

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

- **Easy:** The Web Configurator shows this mode by default. Refer to [Chapter 6 on page 45](#) 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 NBG4615 v2. Click **Expert Mode** after logging into the Web Configurator. The User’s Guide [Chapter 4 on page 39](#) through [Chapter 26 on page 220](#) discusses the screens in this mode.

5.1.2 Device Modes

This refers to the operating mode of the NBG4615 v2, which can act as a:

- **Router:** This is the default device mode of the NBG4615 v2. Use this mode to connect the local network to another network, like the Internet. Go to [Section 7.2 on page 57](#) to view the **Status** screen in this mode.
- **Access Point:** Use this mode if you want to extend your network by allowing network devices to connect to the NBG4615 v2 wirelessly. Go to [Section 8.4 on page 65](#) to view the **Status** screen in this mode.
- **Universal Repeater:** In this mode, the NBG4615 v2 can be an access point and a wireless client at the same time. Use this mode if there is an existing wireless router or access point in your network and you also want to allow clients to connect to the NBG4615 v2. Go to [Section 9.5 on page 73](#) to view the **Status** screen in this mode.
- **WISP:** Use this mode if there is an existing wireless router or access point in the network to which you want to connect your local network. Go to [Section 9.5 on page 73](#) to view the **Status** screen in this mode.
- **WISP + Universal Repeater:** In this mode, the NBG4615 v2 has the same function as in WISP mode. In addition, it can provide WiFi function to the clients on the LAN side. Go to [Section 11.4 on page 93](#) to view the **Status** screen in this mode.

For more information on these modes and to change the mode of your NBG4615 v2, refer to [Chapter 26 on page 220](#).

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

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

When changing to another mode, the IP address of the NBG4615 v2 changes. The running applications and services of the network devices connected to the NBG4615 v2 can be interrupted.

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

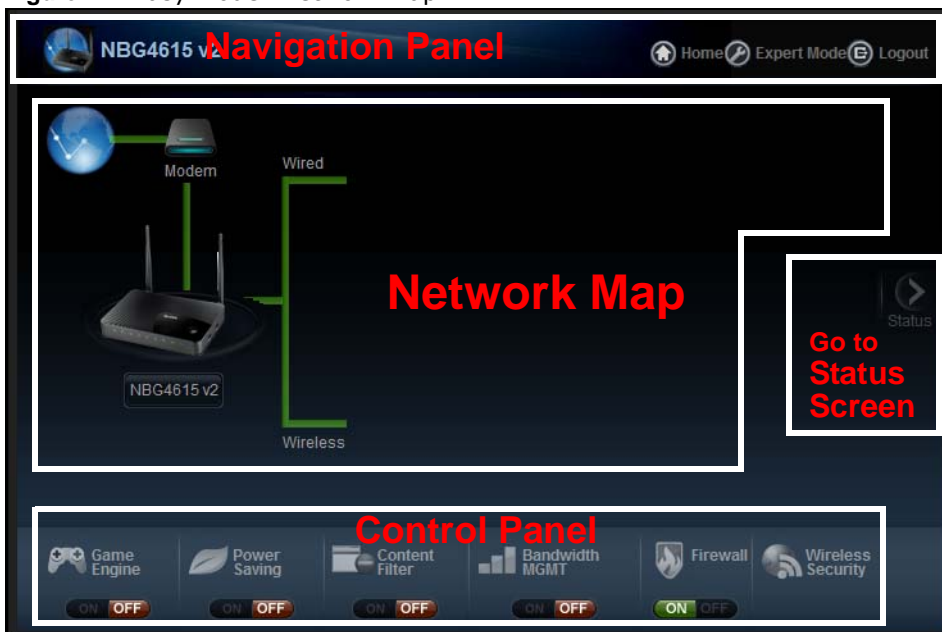
Easy Mode

6.1 Overview

The Web Configurator is set to **Easy Mode** by default. You can configure several key features of the NBG4615 v2 in this mode. This mode is useful to users who are not fully familiar with some features that are usually intended for network administrators.

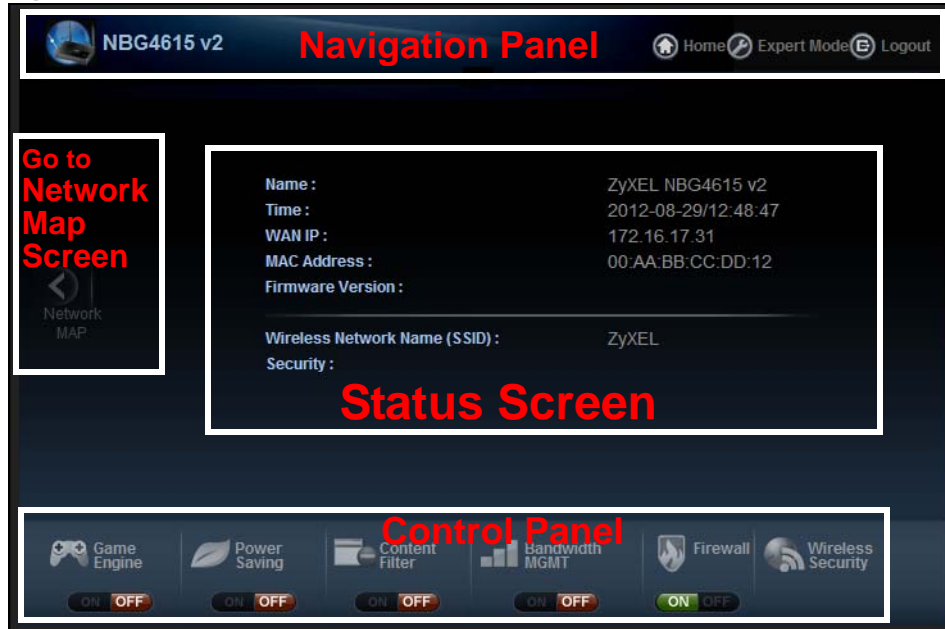
When you log in to the Web Configurator, the following screen opens.

Figure 22 Easy Mode: Network Map



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

Figure 23 Easy Mode: Status Screen



6.2 What You Can Do

You can do the following in this mode:

- Use this **Navigation Panel** to opt out of the **Easy** mode ([Section 6.4 on page 47](#)).
- Use the **Network Map** screen to check if your NBG4615 v2 can ping the gateway and whether it is connected to the Internet ([Section 6.5 on page 47](#)).
- Use the **Control Panel** to configure and enable NBG4615 v2 features, including wireless security, wireless scheduling and bandwidth management and so on ([Section 6.6 on page 48](#)).
- Use the **Status Screen** to view read-only information about the NBG4615 v2, including the WAN IP, MAC Address of the NBG4615 v2 and the firmware version ([Section 6.7 on page 54](#)).

6.3 What You Need to Know

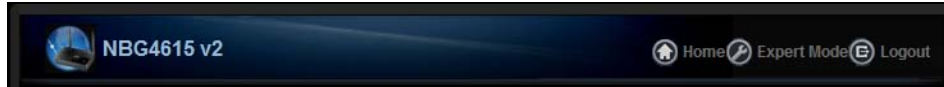
Between the different device modes, the **Control Panel** ([Section 6.6 on page 48](#)) changes depending on which features are applicable to the mode:

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

6.4 Navigation Panel

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

Figure 24 Control Panel



The following table describes the labels in this screen.

Table 17 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 NBG4615 v2.
Logout	Click this to end the Web Configurator session.

6.5 Network Map

Note: The Network MAP is viewable by Windows XP (need to install patch), Windows Vista and Windows 7 users only. For Windows XP (Service Pack 2) users, you can see the network devices connected to the NBG4615 v2 by downloading the LLTD (Link Layer Topology Discovery) patch from the Microsoft Website.

Note: Don't worry if the Network Map does not display in your web browser. This feature may not be supported by your system. You can still configure the Control Panel ([Section 6.6 on page 48](#)) in the Easy Mode and the NBG4615 v2 features that you want to use in the Expert Mode.

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

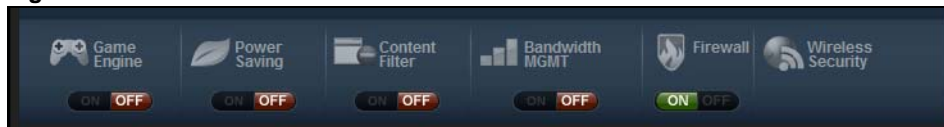
Figure 25 Network Map

The line connecting the NBG4615 v2 to the gateway becomes green when the NBG4615 v2 is able to ping the gateway. It becomes red when the ping initiating from the NBG4615 v2 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 NBG4615 v2, including those connecting wirelessly. Right-click on the NBG4615 v2 icon to refresh the network map and go to the Wizard. Right click on the other icons to view information about the device.

6.6 Control Panel

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

Figure 26 Control Panel

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

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

The following table describes the labels in this screen.

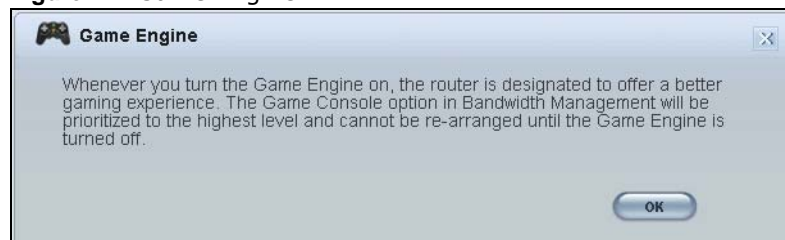
Table 18 Control Panel

ITEM	DESCRIPTION
Game Engine	Switch ON to maximize bandwidth for gaming traffic in your network. Otherwise, switch OFF . Refer to Section 6.6.1 on page 49 to see this screen.
Power Saving	Click this to schedule the wireless feature of the NBG4615 v2. Disabling the wireless function helps lower the energy consumption of the NBG4615 v2. Switch ON to apply wireless scheduling. Otherwise, switch OFF . Refer to Section 6.6.2 on page 50 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 6.6.3 on page 50 to see this screen.
Bandwidth MGMT	Click this to edit bandwidth management for predefined applications. Switch ON to have the NBG4615 v2 management bandwidth for uplink and downlink traffic according to an application or service. Otherwise, switch OFF . Refer to Section 6.6.4 on page 51 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 6.6.5 on page 52 to see this screen.
Wireless Security	Click this to configure the wireless security, such as SSID, security mode and WPS key on your NBG4615 v2. Refer to Section 6.6.6 on page 52 to see this screen.

6.6.1 Game Engine

When this feature is enabled, the NBG4615 v2 maximizes the bandwidth for gaming traffic that it forwards out through an interface.

Figure 27 Game Engine



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

Turn this off if your network is not using gaming.

Click **OK** to close this screen.

6.6.2 Power Saving

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

Disabling the wireless capability lowers the energy consumption of the of the NBG4615 v2.

Figure 28 Power Saving

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

Apply Cancel

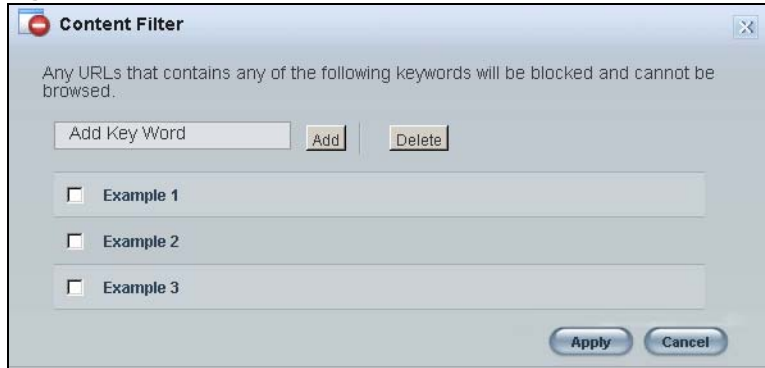
The following table describes the labels in this screen.

Table 19 Power Saving

LABEL	DESCRIPTION
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.
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 NBG4615 v2.
Cancel	Click Cancel to close this screen without saving any changes.

6.6.3 Content Filter

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

Figure 29 Content Filter

The following table describes the labels in this screen.

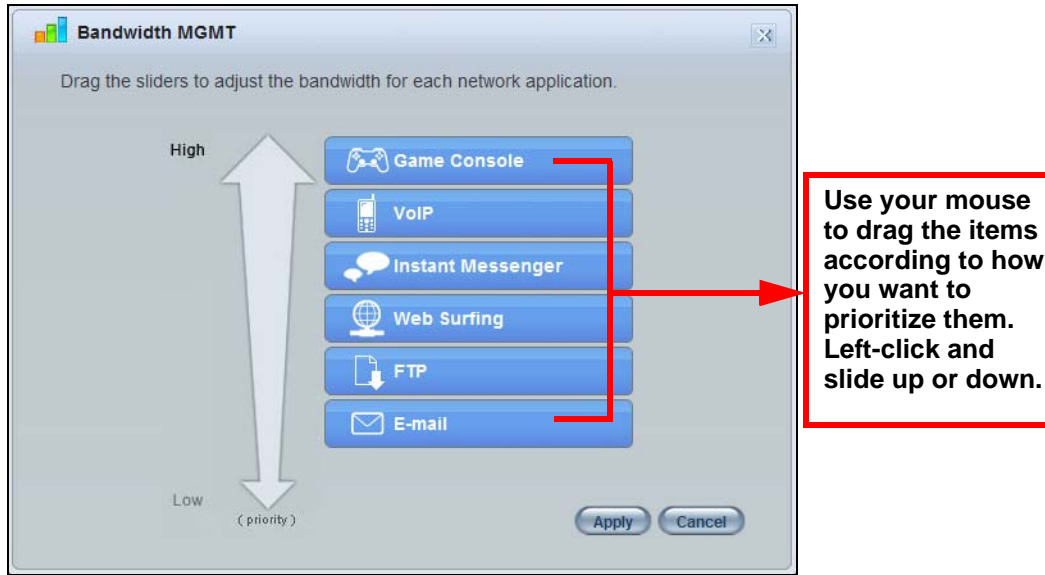
Table 20 Content Filter

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 NBG4615 v2 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.

6.6.4 Bandwidth MGMT

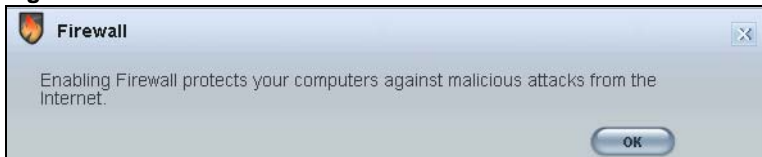
Use this screen to set bandwidth allocation to pre-defined services and applications for bandwidth allocation.

The NBG4615 v2 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 30 Bandwidth MGNT

6.6.5 Firewall

Enable this feature to protect the network from Denial of Service (DoS) attacks. The NBG4615 v2 blocks repetitive pings from the WAN that can otherwise cause systems to slow down or hang.

Figure 31 Firewall

Click **OK** to close this screen.

6.6.6 Wireless Security

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

Note: You can enable the wireless function of your NBG4615 v2 by first turning on the switch in the back panel.

Figure 32 Wireless Security


The image shows a 'Wireless Security' configuration window. At the top, there is a warning message: 'Data transmitted wirelessly without encryption is not safe. Guard your wireless network with a security mode and the password you setup. And then, you can use WPS to connect your computers to your wireless network with just one single click.' Below this, there are four input fields: 'Wireless Network Name (SSID):' with the value 'ZyXEL', 'Security Mode:' with a dropdown menu showing 'WPA2-PSK', 'Wireless Password:', and 'Verify Password:'. To the right of the password fields is a 'WPS' button with a right-pointing arrow. At the bottom, there are 'Apply' and 'Cancel' buttons.

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

Table 21 Wireless Security

LABEL	DESCRIPTION
Wireless Network Name (SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 keyboard characters) for the wireless LAN.
Security mode	Select 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 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 NBG4615 v2.
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.

6.6.7 WPS

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

Figure 33 Wireless Security: WPS



The following table describes the labels in this screen.

Table 22 Wireless Security: WPS

LABEL	DESCRIPTION
Wireless Security	Click this to go back to the Wireless Security screen.
WPS	Create a secure wireless network simply by pressing a button. The NBG4615 v2 scans for a WPS-enabled device within the range and performs wireless security information synchronization. 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.
Register	Create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the NBG4615 v2's interface and pushing this button. 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.
Exit	Click Exit to close this screen.

6.7 Status Screen in Easy Mode

In the Network Map screen, click **Status** to view read-only information about the NBG4615 v2.

Figure 34 Status Screen in Easy Mode



The following table describes the labels in this screen.

Table 23 Status Screen in Easy Mode

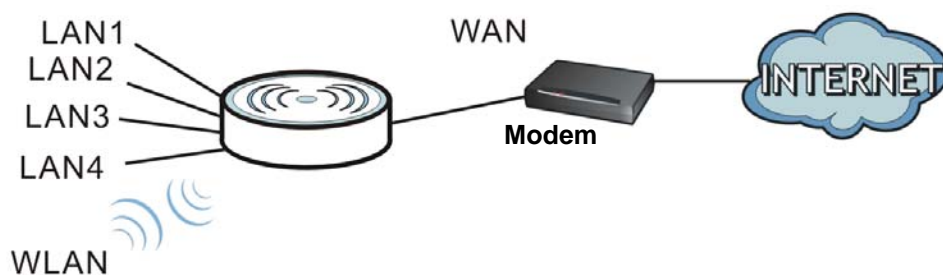
ITEM	DESCRIPTION
Name	This is the name of the NBG4615 v2 in the network. You can change this in the Maintenance > General screen in Section 26.3 on page 211 .
Time	This is the current system date and time. The date is in YYYY:MM:DD (Year-Month-Day) format. The time is in HH:MM:SS (Hour:Minutes:Seconds) format.
WAN IP	This is the IP address of the WAN port.
MAC Address	This is the MAC address of the NBG4615 v2.
Firmware Version	This shows the firmware version of the NBG4615 v2. The firmware version format shows the trunk version, model code and release number.
Wireless Network Name (SSID)	This shows the SSID of the wireless network. You can configure this in the Wireless Security screen (Section 6.6.6 on page 52 ; Section 15.2 on page 140).
Security	This shows the wireless security used by the NBG4615 v2.

Router Mode

7.1 Overview

The NBG4615 v2 is set to router mode by default. Routers are used to connect the local network to another network (for example, the Internet). In the figure below, the NBG4615 v2 connects the local network (**LAN1 ~ LAN4**) to the Internet.

Figure 35 NBG4615 v2 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 NBG4615 v2.

7.2 Router Mode Status Screen


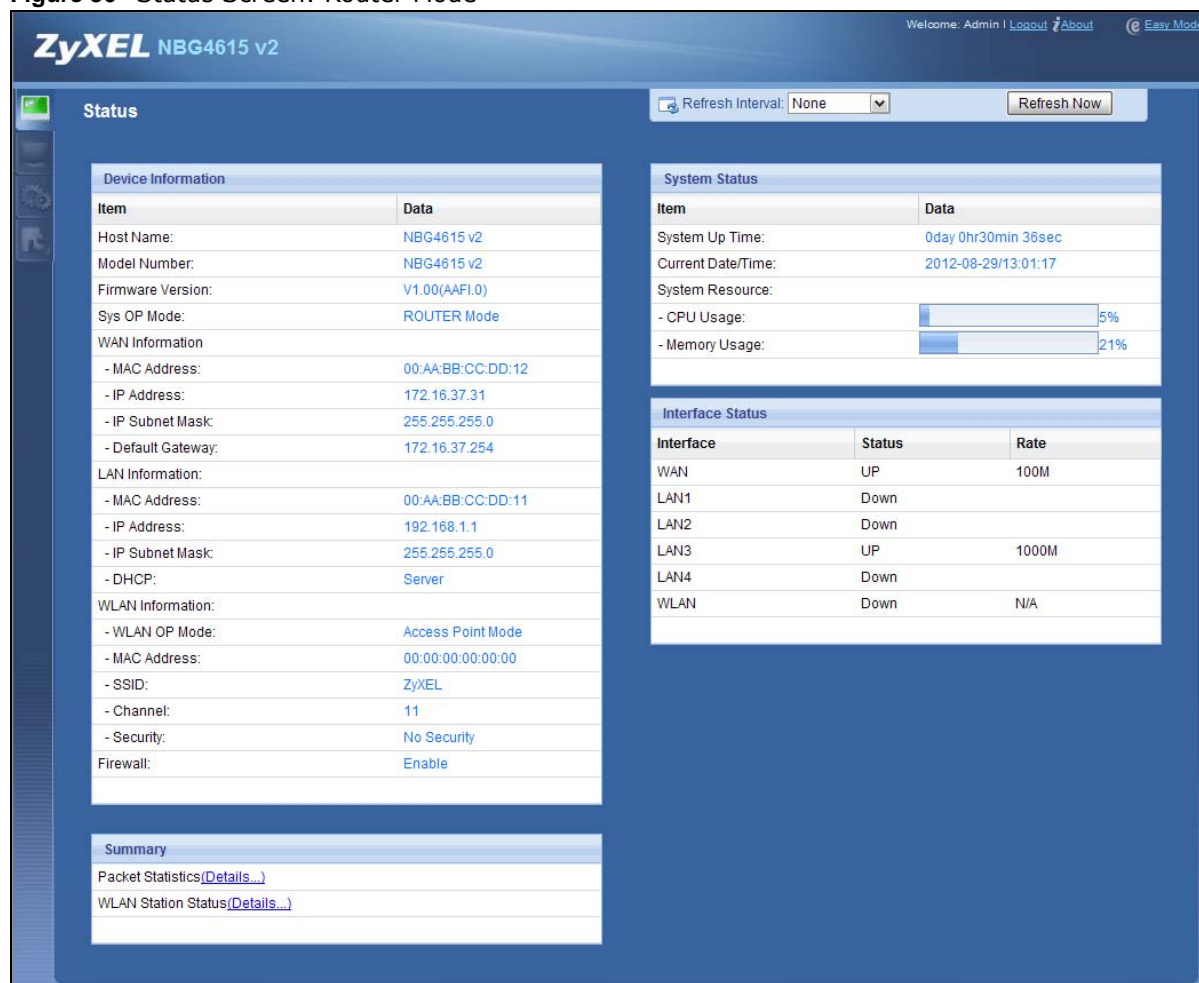
Click  to open the status screen.

Figure 36 Status Screen: Router Mode



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

Table 24 Status Screen Icon Key

ICON	DESCRIPTION
	Click this at any time to exit the Web Configurator.
	Click this icon to view copyright and a link for related product information.
	Click this icon to go to Easy Mode. See Chapter 6 on page 45 .
	Select a number of seconds or None from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
	Click this button to refresh the status screen statistics.
	Click this icon to see the Status page. The information in this screen depends on the device mode you select.
	Click this icon to see the Monitor navigation menu.
	Click this icon to see the Configuration navigation menu.
	Click this icon to see the Maintenance navigation menu.

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

Table 25 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.
Firmware Version	This is the firmware version and the date created.
System OP Mode	This is the device mode (Section 5.1.2 on page 43) to which the NBG4615 v2 is set - Router Mode .
WAN Information	
MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
IP Address	This shows the WAN port's IP address.
IP Subnet Mask	This shows the WAN port's subnet mask.
Default Gateway	This shows the WAN port's gateway IP address.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP	This shows the LAN port's DHCP role - Server or Disable .
WLAN Information	
WLAN OP Mode	This is the device mode (Section 5.1.2 on page 43) to which the NBG4615 v2's wireless LAN is set - Access Point Mode .
MAC Address	This shows the wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the NBG4615 v2 in the wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the NBG4615 v2 is using.
Firewall	This shows whether the firewall is enabled or not.
Summary	
Packet Statistics	Click Details... to go to the Monitor > Packet Statistics screen (Section 13.5 on page 121). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click Details... to go to the Monitor > WLAN Station Status screen (Section 13.6 on page 122). Use this screen to view the wireless stations that are currently associated to the NBG4615 v2.
System Status	
Item	This column shows the type of data the NBG4615 v2 is recording.
Data	This column shows the actual data recorded by the NBG4615 v2.
System Up Time	This is the total time the NBG4615 v2 has been on.
Current Date/Time	This field displays your NBG4615 v2's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG4615 v2's processing ability is currently used. When this percentage is close to 100%, the NBG4615 v2 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.)
- Memory Usage	This shows what percentage of the heap memory the NBG4615 v2 is using.

Table 25 Status Screen: Router Mode (continued)

LABEL	DESCRIPTION
Interface Status	
Interface	This displays the NBG4615 v2 port types. The port types are: WAN , LAN and WLAN .
Status	For the LAN and WAN ports, this field displays Down (line is down) or Up (line is up or connected). For the WLAN, it displays Up when the WLAN is enabled or Down when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or N/A when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation. This field displays N/A when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and N/A when the WLAN is disabled.

7.2.1 Navigation Panel

Use the sub-menus on the navigation panel to configure NBG4615 v2 features.

Figure 37 Navigation Panel: Router Mode

The following table describes the sub-menus.

Table 26 Navigation Panel: Router Mode

LINK	TAB	FUNCTION
Status		This screen shows the NBG4615 v2'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 NBG4615 v2.
DHCP Table		Use this screen to view current DHCP client information.
Packet Statistics		Use this screen to view port status and packet specific statistics.
WLAN Station Status		Use this screen to view the wireless stations that are currently associated to the NBG4615 v2.
CONFIGURATION		

Table 26 Navigation Panel: Router Mode (continued)

LINK	TAB	FUNCTION
Network		
WAN	Internet Connection	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address.
	Advanced	Use this screen to configure other advanced properties.
Wireless LAN	General	Use this screen to enable the wireless LAN and configure wireless LAN and wireless security settings.
	More AP	Use this screen to configure multiple BSSs on the NBG4615 v2.
	MAC Filter	Use the MAC filter screen to configure the NBG4615 v2 to block access to devices or block the devices from accessing the NBG4615 v2.
	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 NBG4615 v2 apply IP alias to create LAN subnets.
DHCP Server	General	Use this screen to enable the NBG4615 v2'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 servers behind the NBG4615 v2 and forward incoming service requests to the server(s) on your local network.
	Port Trigger	Use this screen to change your NBG4615 v2'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.
Content Filter	Content Filter	Use this screen to block certain web features and sites containing certain keywords in the URL.
Management		
Bandwidth Management	General	Use this screen to enable bandwidth management.
	Advanced	Use this screen to set the upstream bandwidth and edit a bandwidth management rule.

Table 26 Navigation Panel: Router Mode (continued)

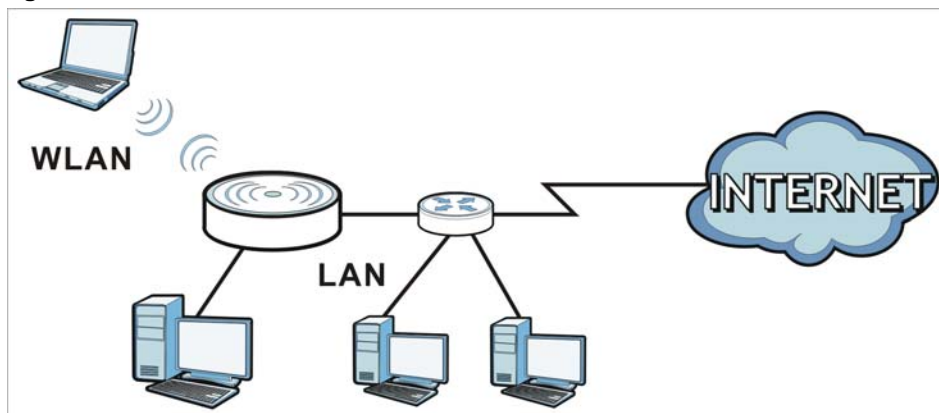
LINK	TAB	FUNCTION
Remote Management	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the NBG4615 v2.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the NBG4615 v2.
	Wake On LAN	Use this screen to enable Wake on LAN to remotely turn on a device on the local network.
UPnP	General	Use this screen to enable UPnP on the NBG4615 v2.
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 NBG4615 v2.
Time	Time Setting	Use this screen to change your NBG4615 v2's time and date.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your NBG4615 v2.
Backup/Restore	Backup/Restore	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG4615 v2.
Restart	System Restart	This screen allows you to reboot the NBG4615 v2 without turning the power off.
Language	Language	This screen allows you to select the language you prefer.
Sys OP Mode	Sys OP Mode	This screen allows you to select whether your device acts as a router, an access point, a universal repeater or a wireless client.

Access Point Mode

8.1 Overview

Use your NBG4615 v2 as an access point (AP) if you already have a router or gateway on your network. In this mode your NBG4615 v2 bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

Figure 38 Wireless Internet Access in Access Point Mode



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

Note: See [Chapter 12 on page 97](#) for an example of setting up a wireless network in Access Point mode.

8.2 What You Can Do

- Use the **Status** screen to view read-only information about your NBG4615 v2 ([Section 8.4 on page 65](#)).
- Use the **LAN** screen to set the IP address for your NBG4615 v2 acting as an access point ([Section 8.5 on page 67](#)).

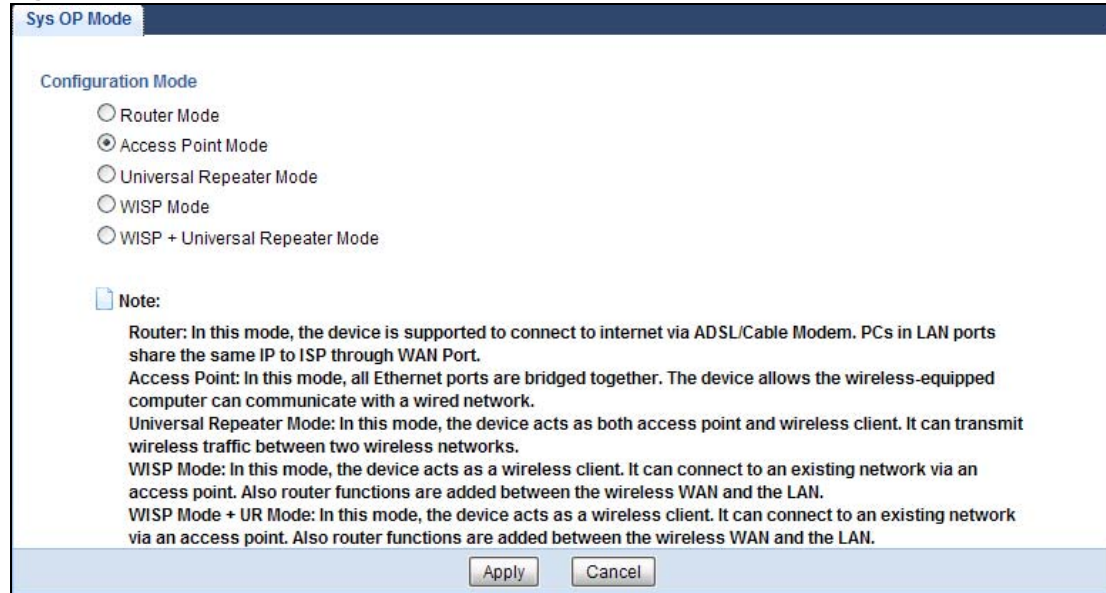
8.3 What You Need to Know

See [Chapter 12 on page 97](#) for a tutorial on setting up a network with the NBG4615 v2 as an access point.

8.3.1 Setting your NBG4615 v2 to AP Mode

- 1 Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.
- 2 To use your NBG4615 v2 as an access point, go to **Maintenance > Sys OP Mode** and select **Access Point Mode**.

Figure 39 Changing to Access Point mode



Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your NBG4615 v2 is already in Access Point mode.

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

Figure 40 Pop up for Access Point mode



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

8.3.2 Accessing the Web Configurator in Access Point Mode

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

- 1 Connect your computer to the LAN port of the NBG4615 v2.
- 2 The default IP address of the NBG4615 v2 is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".

- 3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see [Appendix C on page 251](#) for information on changing your computer's IP address.
- 4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "192.168.1.2" as the web address in your web browser.

Note: After clicking **Login**, the **Easy Mode** appears. Refer to [Section on page 45](#) for the **Easy Mode** screens. Change to **Expert Mode** to see the screens described in the sections following this.

8.3.3 Configuring your WLAN and Maintenance Settings

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

- See [Chapter 15 on page 135](#) for information on the configuring your wireless network.
- See [Chapter 26 on page 211](#) for information on configuring your Maintenance settings.

8.4 AP Mode Status Screen


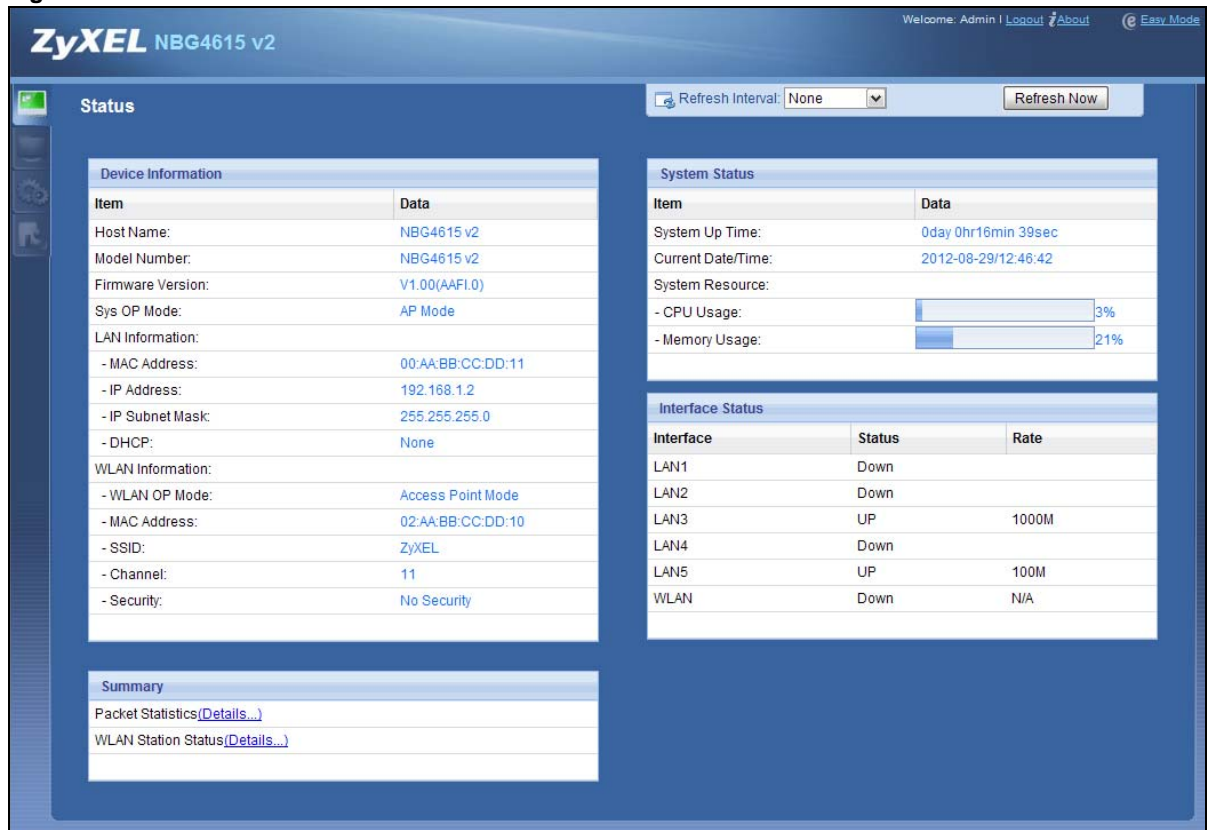
Click  to open the **Status** screen.

Figure 41 Status Screen: Access Point Mode



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

Table 27 Status Screen: Access Point Mode

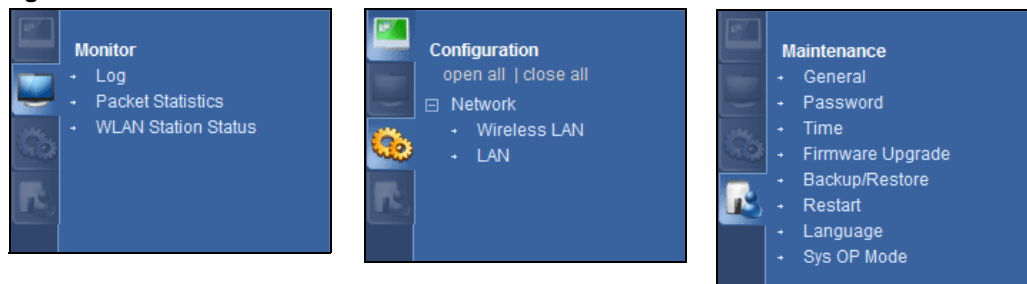
LABEL	DESCRIPTION
Device Information	
Host Name	This is the System Name you enter in the Maintenance > General screen. It is for identification purposes.
Model Number	This is the model name of your device.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode (Section 5.1.2 on page 43) to which the NBG4615 v2 is set - AP Mode .
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP	This shows the LAN port's DHCP role - Client or None .
WLAN Information	
WLAN OP Mode	This is the device mode (Section 5.1.2 on page 43) to which the NBG4615 v2's wireless LAN is set - Access Point Mode .
MAC Address	This shows the wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the NBG4615 v2 in the wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the NBG4615 v2 is using.
Firewall	This shows whether the firewall is enabled or not.
Summary	
Packet Statistics	Click Details... to go to the Monitor > Packet Statistics screen (Section 13.5 on page 121). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click Details... to go to the Monitor > WLAN Station Status screen (Section 13.6 on page 122). Use this screen to view the wireless stations that are currently associated to the NBG4615 v2.
System Status	
Item	This column shows the type of data the NBG4615 v2 is recording.
Data	This column shows the actual data recorded by the NBG4615 v2.
System Up Time	This is the total time the NBG4615 v2 has been on.
Current Date/Time	This field displays your NBG4615 v2's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG4615 v2's processing ability is currently used. When this percentage is close to 100%, the NBG4615 v2 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.)
- Memory Usage	This shows what percentage of the heap memory the NBG4615 v2 is using.
Interface Status	
Interface	This displays the NBG4615 v2 port types. The port types are: LAN and WLAN .

Table 27 Status Screen: Access Point Mode (continued)

LABEL	DESCRIPTION
Status	For the LAN 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 WLAN, it displays the maximum transmission rate when the WLAN is enabled and N/A when the WLAN is disabled.

8.4.1 Navigation Panel

Use the menu in the navigation panel to configure NBG4615 v2 features in **Access Point Mode**.

Figure 42 Menu: Access Point Mode

Refer to [Table 26 on page 60](#) for descriptions of the labels shown in the navigation panel.

8.5 LAN Screen

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

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

Note: If you change the IP address of the NBG4615 v2 in the screen below, you will need to log into the NBG4615 v2 again using the new IP address.

Figure 43 Network > LAN > IP

The table below describes the labels in the screen.

Table 28 Network > LAN > IP

LABEL	DESCRIPTION
Obtain an IP Address Automatically	When you enable this, the NBG4615 v2 gets its IP address from the network's DHCP server (for example, your ISP). Users connected to the NBG4615 v2 can now access the network (i.e., the Internet if the IP address is given by the ISP). The Web Configurator may no longer be accessible unless you know the IP address assigned by the DHCP server to the NBG4615 v2. You need to reset the NBG4615 v2 to be able to access the Web Configurator again (see Section 26.7 on page 216 for details on how to reset the NBG4615 v2). Also when you select this, you cannot enter an IP address for your NBG4615 v2 in the field below.
Static IP Address	Click this if you want to specify the IP address of your NBG4615 v2. Or if your ISP or network administrator gave you a static IP address to access the network or the Internet.
IP Address	Type the IP address in dotted decimal notation. The default setting is 192.168.1.2. If you change the IP address you will have to log in again with the new IP address.
Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG4615 v2 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 NBG4615 v2.
Gateway IP Address	Enter a Gateway IP Address (if your ISP or network administrator gave you one) in this field.
DNS Assignment	
First DNS Server Second DNS Server Third DNS Server	Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the NBG4615 v2'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.

Table 28 Network > LAN > IP (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

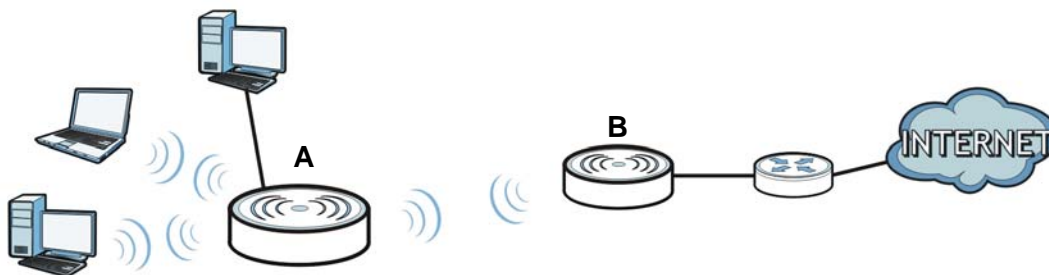
Universal Repeater Mode

9.1 Overview

In universal repeater mode, your NBG4615 v2 can act as an access point and wireless client at the same time. The NBG4615 v2 can connect to an existing network through another access point and also lets wireless clients connect to the network through it. This helps you expand wireless coverage when you have an access point or wireless router already in your network.

In the example below, the NBG4615 v2 (**A**) is configured as a universal repeater. It has three clients that want to connect to the Internet. The NBG4615 v2 wirelessly connects to the available access point (**B**).

Figure 44 Universal Repeater Mode



After the NBG4615 v2 and the access point connect, the NBG4615 v2 acquires its IP address from the access point. The clients of the NBG4615 v2 can now surf the Internet.

9.2 What You Can Do

- Use the **Status** screen to view read-only information about your NBG4615 v2 ([Section 9.5 on page 73](#)).
- Use the **LAN** screen to set the IP address for your NBG4615 v2 acting as an access point ([Section 8.5 on page 67](#)).
- Use the **Wireless LAN > Universal Repeater** screen to configure the security between the NBG4615 v2 and another access point ([Section 9.6 on page 75](#)).
- Use the **Wireless LAN > Site Survey** screen to scan for available access points within transmission range ([Section 9.6 on page 75](#)).
- Use other **Wireless LAN** screens to configure the wireless settings and wireless security between the wireless clients and the NBG4615 v2.

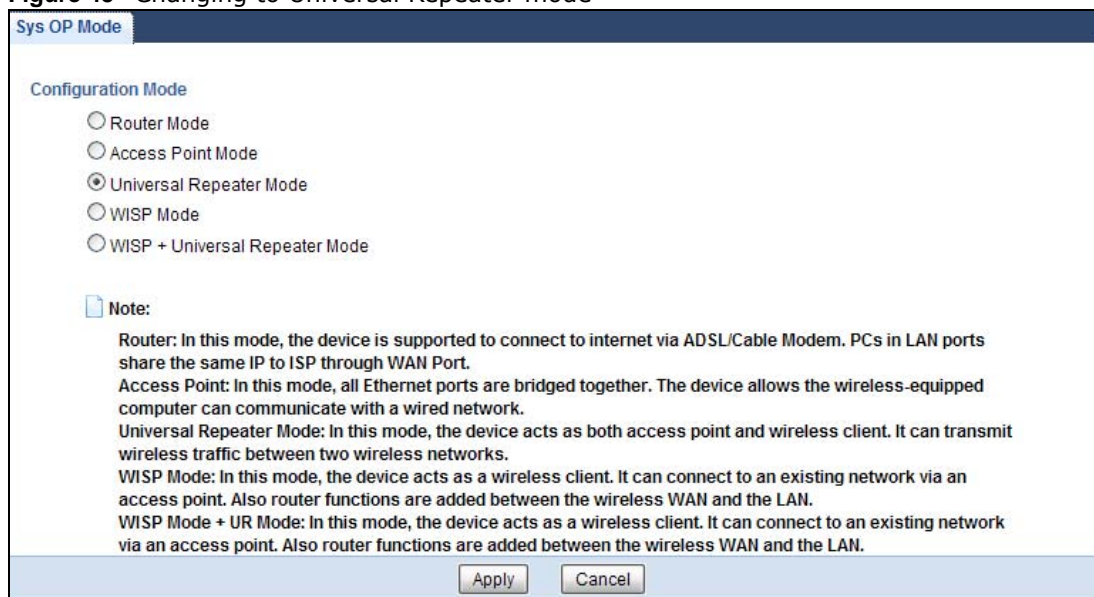
9.3 What You Need to Know

With the exception of the **Wireless LAN > Universal Repeater** and **Site Survey** screens, other configuration screens in **Universal Repeater Mode** are similar to the ones in **Access Point Mode**. See [Chapter 15 on page 135](#) through [Chapter 26 on page 220](#) of this User's Guide.

9.4 Setting your NBG4615 v2 to Universal Repeater Mode

- 1 Connect your computer to the LAN port of the NBG4615 v2.
- 2 The default IP address of the NBG4615 v2 is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".
- 3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see [Appendix C on page 251](#) for information on changing your computer's IP address.
- 4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.2" as the web address in your web browser.
- 5 Enter "1234" (default) as the password and click **Login**.
- 6 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.
- 7 The Easy mode appears. Click **Expert Mode** in the navigation panel.
- 8 To set your NBG4615 v2 to **Universal Repeater Mode**, on the left of the screen, click **Maintenance > Sys OP Mode** and select **Universal Repeater Mode**.

Figure 45 Changing to Universal Repeater mode



Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your NBG4615 v2 is already in Universal Repeater mode.

- 9 When you select **Universal Repeater Mode**, the following pop-up message window appears.

Figure 46 Pop up for Universal Repeater mode



Click **OK**. Then click **Apply**. The Web Configurator refreshes once the change to Universal Repeater mode is successful.

9.5 Universal Repeater Mode Status Screen


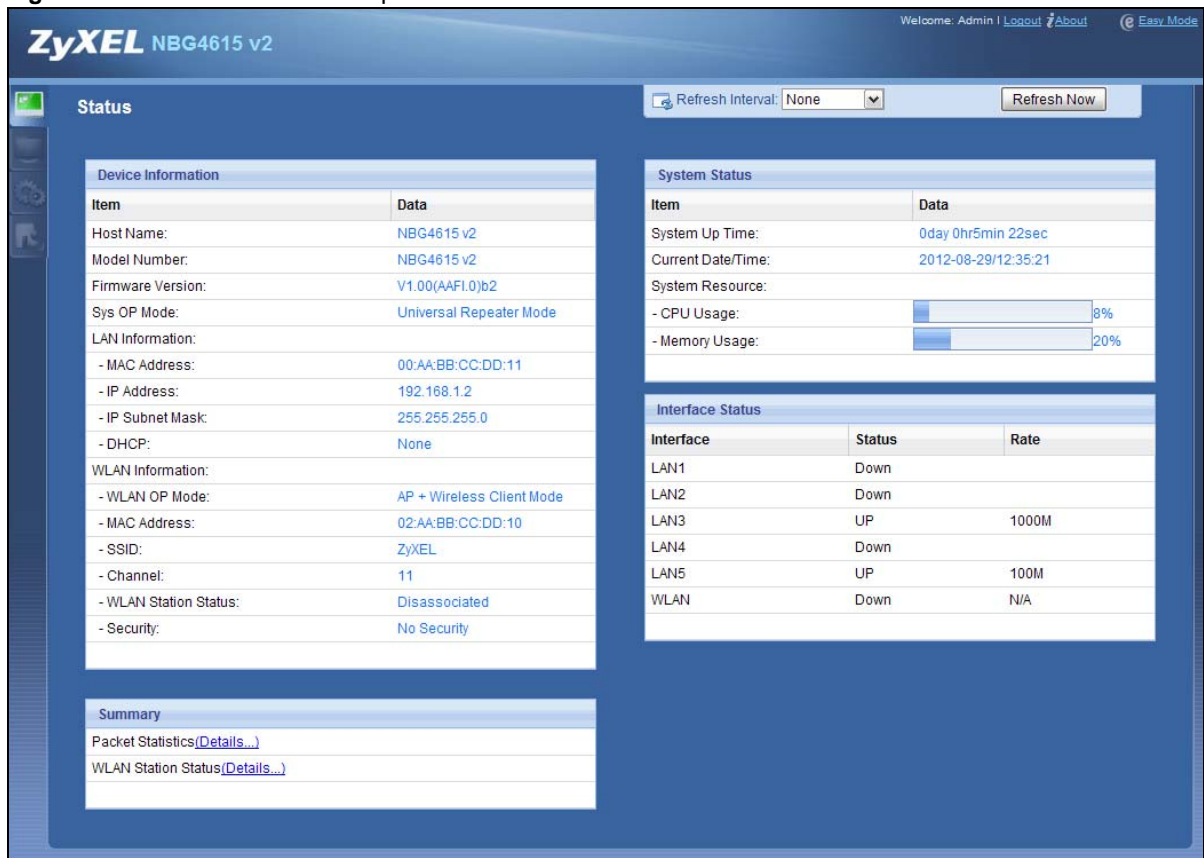
Click  to open the status screen.

Figure 47 Status: Universal Repeater Mode



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

Table 29 Status Screen: Universal Repeater Mode

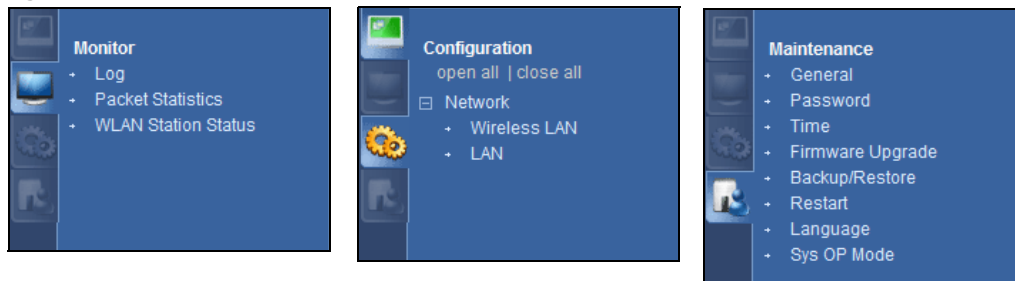
LABEL	DESCRIPTION
Device Information	
Host Name	This is the System Name you enter in the Maintenance > General screen. It is for identification purposes.
Model Number	This is the model name of your device.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode (Section 5.1.2 on page 43) to which the NBG4615 v2 is set - Universal Repeater Mode .
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP	This shows the LAN port's DHCP role - Client or None .
WLAN Information	
WLAN OP Mode	This is the device mode (Section 5.1.2 on page 43) to which the NBG4615 v2's wireless LAN is set - AP + Wireless Client Mode .
MAC Address	This shows the wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the NBG4615 v2 in the wireless LAN.
Channel	This shows the channel number which you select manually.
WLAN Station Status	If the NBG4615 v2 has successfully connected to an AP or wireless router, it displays the SSID and MAC address of the AP or wireless router in this field. Otherwise, it displays Disassociated .
Security	This shows the level of wireless security the NBG4615 v2 is using.
Summary	
Packet Statistics	Click Details... to go to the Monitor > Packet Statistics screen (Section 13.5 on page 121). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click Details... to go to the Monitor > WLAN Station Status screen (Section 13.6 on page 122). Use this screen to view the wireless stations that are currently associated to the NBG4615 v2.
System Status	
Item	This column shows the type of data the NBG4615 v2 is recording.
Data	This column shows the actual data recorded by the NBG4615 v2.
System Up Time	This is the total time the NBG4615 v2 has been on.
Current Date/Time	This field displays your NBG4615 v2's present date and time.
System Resource	
CPU Usage	This displays what percentage of the NBG4615 v2's processing ability is currently used. When this percentage is close to 100%, the NBG4615 v2 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management).
Memory Usage	This shows what percentage of the heap memory the NBG4615 v2 is using.
Interface Status	
Interface	This displays the NBG4615 v2 port types. The port types are: LAN and WLAN .

Table 29 Status Screen: Universal Repeater Mode (continued)

LABEL	DESCRIPTION
Status	For the LAN 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 or N/A when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and N/A when the WLAN is disabled.

9.5.1 Navigation Panel

Use the menu in the navigation panel to configure NBG4615 v2 features in **Universal Repeater Mode**.

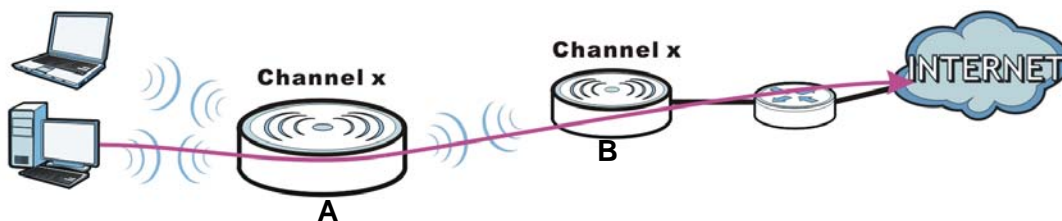
Figure 48 Menu: Universal Repeater Mode

Refer to [Table 26 on page 60](#) for descriptions of the labels shown in the navigation panel.

9.6 Universal Repeater Screen

Use this screen to enter the SSID and select the wireless security mode used by the wireless device to which you want to connect. Go to **Configuration > Network > Wireless LAN > Universal Repeater** to open the **Universal Repeater** screen. The screen varies depending on security mode.

Note: To have wireless clients access or acquire an IP address from another access point or wireless router (**B**) through the NBG4615 v2 (**A**) in universal repeater mode, you must set the channel number in the **Wireless LAN > General** screen to be the same as the one on the wireless router or AP to which the NBG4615 v2 wants to connect.



9.6.1 No Security

Figure 49 Universal Repeater Mode: Wireless LAN > Universal Repeater: No Security

The screenshot shows the 'Universal Repeater Parameters' section with the following fields and values:

- SSID: (empty text box)
- Channel Selection: Channel-11 2462MHz (dropdown menu)
- Security Mode: No Security (dropdown menu)
- Buttons: Apply, Cancel

The following table describes the labels in this screen.

Table 30 Universal Repeater Mode: Wireless LAN > Universal Repeater: No Security

LABEL	DESCRIPTION
Universal Repeater Parameters	
SSID	Enter the name of the access point to which you are connecting.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. Select the channel number used by the access point to which you are connecting.
Security Mode	Select No Security if the access point to which you want to connect does not use encryption.
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

9.6.2 Static WEP

Figure 50 Universal Repeater Mode: Wireless LAN > Universal Repeater: Static WEP

The screenshot shows the 'Universal Repeater Parameters' section with the following fields and values:

- SSID: (empty text box)
- Channel Selection: Channel-11 2462MHz (dropdown menu)
- Security Mode: Static WEP (dropdown menu)
- PassPhrase: (empty text box) with a Generate button
- WEP Encryption: 64-bits (dropdown menu)
- Authentication Method: Open (dropdown menu)
- 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.)
- Radio buttons: ☒ ASCII ☐ Hex
- Key selection:
 - ☒ Key 1 (with text input field)
 - ☐ Key 2 (with text input field)
 - ☐ Key 3 (with text input field)
 - ☐ Key 4 (with text input field)
- Buttons: Apply, Cancel

The following table describes the labels in this screen.

Table 31 Universal Repeater Mode: Wireless LAN > Universal Repeater: Static WEP

LABEL	DESCRIPTION
Universal Repeater Parameters	
SSID	Enter the name of the access point to which you are connecting.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. Select the channel number used by the access point to which you are connecting.
Security Mode	Select Static WEP if the access point to which you want to connect uses WEP 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 NBG4615 v2 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 Open 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 Open unless you want to force a key verification before communication between the wireless client and the NBG4615 v2 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	Select a default WEP key to use for data encryption. The WEP keys are used to encrypt data. Both the NBG4615 v2 and the wireless stations must use the same WEP key for data transmission. If you chose 64-bits , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128-bits , 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 NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

9.6.3 WPA(2)-PSK

Figure 51 Universal Repeater Mode: Wireless LAN > Universal Repeater: WPA(2)-PSK

Universal Repeater Parameters

SSID:

Channel Selection:

Security Mode:

Encryption Type: ☐ TKIP ☒ AES

Pre-Shared Key:

The following table describes the labels in this screen.

Table 32 Universal Repeater Mode: Wireless LAN > Universal Repeater: WPA(2)-PSK

LABEL	DESCRIPTION
Universal Repeater Parameters	
SSID	Enter the name of the access point to which you are connecting.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. Select the channel number used by the access point to which you are connecting.
Security Mode	Select WPA-PSK or WPA2-PSK if the access point to which you want to connect uses WPA-PSK or WPA2-PSK.
Encryption Type	Select the type of wireless encryption employed by the access point to which you want to connect.
Pre-Shared Key	WPA-PSK or WPA2-PSK uses a simple common password for authentication. Type the password employed by the access point to which you want to connect.
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

9.7 Site Survey Screen

Use this screen to scan for and connect to a wireless network automatically. Go to **Configuration > Network > Wireless LAN > Site Survey** to open the following screen.

Figure 52 Configuration > Wireless LAN > Site Survey (Universal Repeater)

Wireless Lan Site Survey

Site Survey

#	SSID	BSSID	Signal Strength	Channel	Security
---	------	-------	-----------------	---------	----------

The following table describes the labels in this screen.

Table 33 Configuration > Wireless LAN > Site Survey (Universal Repeater)

LABEL	DESCRIPTION
Site Survey	
#	<p>Select a wireless device and click Add Profile to open a configuration screen where you can add the selected wireless device to a profile and then enable it.</p> <p>This field is selected if the wireless device is added to an activated profile and the NBG4615 v2 is connecting to it.</p>
SSID	This displays the SSID of the wireless device.
BSSID	This displays the MAC address of the wireless device.
Signal Strength	This displays the strength of the wireless signal. The signal strength mainly depends on the antenna output power and the distance between your NBG4615 v2 and this device.
Channel	This displays the channel number used by this wireless device.
Security	This displays the data encryption and authentication method used by this wireless device.
Rescan	Click this button to search for available wireless devices within transmission range and update this table.
Add Profile	Select a wireless device and click this button to add it to a profile.

WISP Mode

10.1 Overview

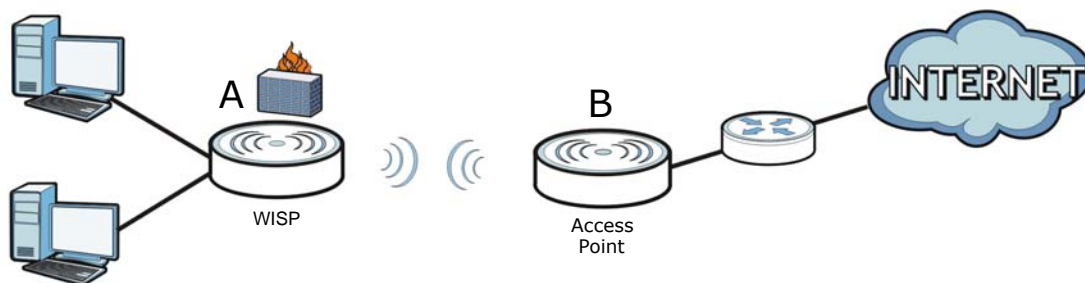
In WISP (Wireless ISP) mode, your NBG4615 v2 can act as a wireless client to wirelessly connect to the Internet or an existing network via an access point. Use this mode if you already have an access point or wireless router in your network.

Note: Make sure your network and the remote network are NOT in the same subnet. If the access point or wireless router is using 192.168.1.x, the NBG4615 v2 in WISP mode needs to use something else, say 192.168.2.x.

Note: When the NBG4615 v2 is in WISP or WISP + Universal Repeater mode, you still need to enter your ISP information in the WAN screen in order to access the Internet.

In the example below, one NBG4615 v2 is configured as a wireless client (**A**) and another is used as an access point (**B**). The wireless client has two clients that need to connect to the Internet. The NBG4615 v2 wirelessly connects to the available access point (**B**).

Figure 53 WISP Mode



After the NBG4615 v2 and the access point connect, the NBG4615 v2 acquires its WAN IP address from the access point. The clients of the NBG4615 v2 can now surf the Internet.

10.2 What You Can Do

- Use the **Status** screen to view read-only information about your NBG4615 v2 ([Section 9.5 on page 73](#)).
- Use the **LAN** screen to set the IP address for your NBG4615 v2 ([Chapter 16 on page 157](#)).
- Use the **Wireless LAN** screen to associate your NBG4615 v2 (acting as a wireless client) with an existing access point ([Section 10.5 on page 85](#)).

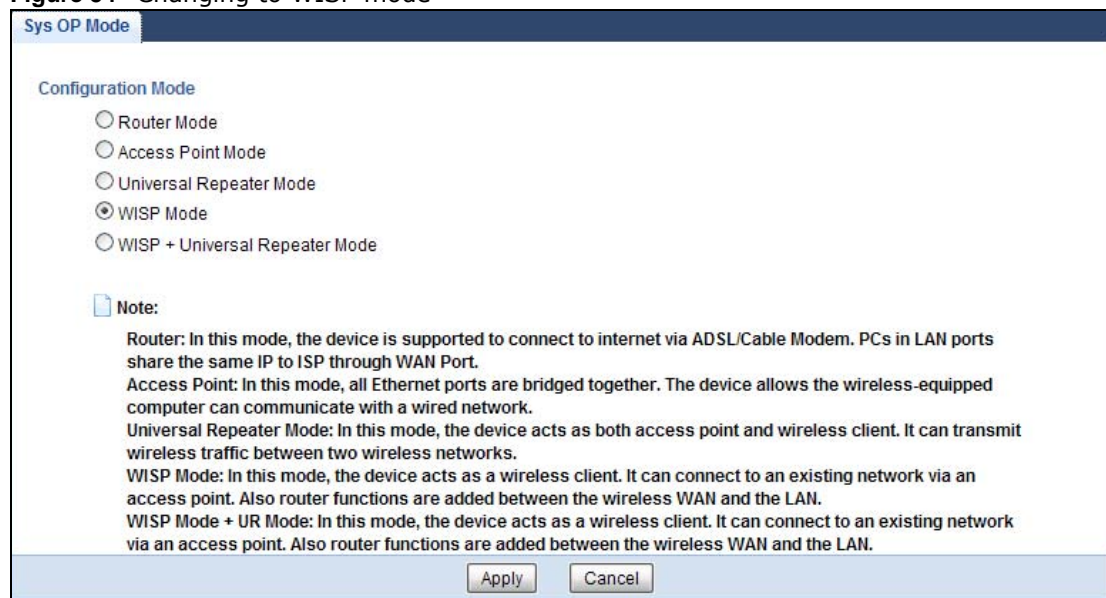
10.3 What You Need to Know

With the exception of the **Wireless LAN** screen, the **Monitor**, **Configuration** and **Maintenance** screens in **WISP Mode** are similar to the ones in **Router Mode**. See [Chapter 15 on page 135](#) through [Chapter 26 on page 220](#) of this User's Guide.

10.3.1 Setting your NBG4615 v2 to WISP Mode

- 1 Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.
- 2 To set your NBG4615 v2 to **WISP Mode**, go to **Maintenance > Sys OP Mode** and select **WISP Mode**.

Figure 54 Changing to WISP mode



Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your NBG4615 v2 is already in WISP mode.

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

Figure 55 Pop up window for WISP mode



Click **OK**. Then click **Apply**. The Web Configurator refreshes once the change to **WISP Mode** is successful.

10.3.2 Accessing the Web Configurator in WISP Mode

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

- 1 Connect your computer to the LAN port of the NBG4615 v2.
- 2 The default IP address of the NBG4615 v2 is "192.168.1.1". If you did not change this, you can use the same IP address in **WISP Mode**. Open a web browser such as Internet Explorer and type "192.168.1.1" as the web address in your web browser.

If you changed the IP address of your NBG4615 v2 while in **Router Mode**, use this IP address in **WISP Mode**. The **WISP Mode** IP address is always the same as the **Router Mode** IP address.

Note: After clicking **Login**, the **Easy Mode** appears. Refer to [Chapter 6 on page 45](#) for the **Easy Mode** screens. Click **Expert Mode** to see the screens described in the sections following this.

10.4 WISP Mode Status Screen


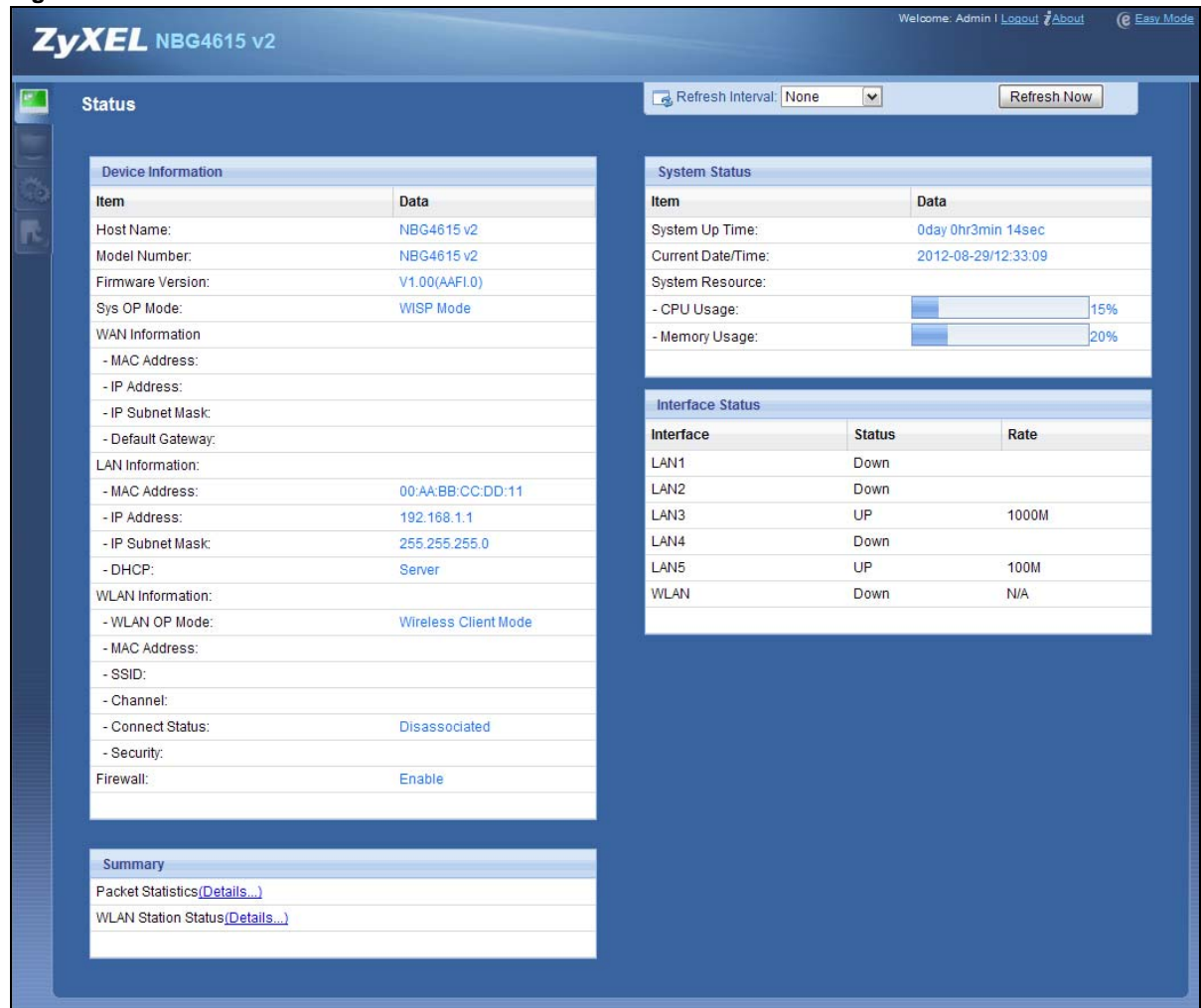
Click  to open the status screen.

Figure 56 Status: WISP Mode



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

Table 34 Status Screen: WISP 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.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode (Section 5.1.2 on page 43) to which the NBG4615 v2 is set - WISP Mode .
WAN Information	
MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
IP Address	This shows the WAN port's IP address.
IP Subnet Mask	This shows the WAN port's subnet mask.
Default Gateway	This shows the WAN port's gateway IP address.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP	This shows the LAN port's DHCP role - Server or Disable .
WLAN Information	
WLAN OP Mode	This is the device mode (Section 5.1.2 on page 43) to which the NBG4615 v2's wireless LAN is set - Wireless Client Mode .
MAC Address	This shows the wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the NBG4615 v2 in the wireless LAN.
Channel	This shows the channel number which you select manually.
Connect Status	This shows whether or not the NBG4615 v2 has successfully associated with an access point - Associated or Disassociated .
Security	This shows the level of wireless security the NBG4615 v2 is using.
Firewall	This shows whether the firewall is enabled or not.
Summary	
Packet Statistics	Click Details... to go to the Monitor > Packet Statistics screen (Section 13.5 on page 121). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click Details... to go to the Monitor > WLAN Station Status screen (Section 13.6 on page 122). Use this screen to view the wireless stations that are currently associated to the NBG4615 v2.
System Status	
Item	This column shows the type of data the NBG4615 v2 is recording.
Data	This column shows the actual data recorded by the NBG4615 v2.
System Up Time	This is the total time the NBG4615 v2 has been on.
Current Date/Time	This field displays your NBG4615 v2's present date and time.
System Resource	

Table 34 Status Screen: WISP Mode (continued)

LABEL	DESCRIPTION
- CPU Usage	This displays what percentage of the NBG4615 v2's processing ability is currently used. When this percentage is close to 100%, the NBG4615 v2 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management).
- Memory Usage	This shows what percentage of the heap memory the NBG4615 v2 is using.
Interface Status	
Interface	This displays the NBG4615 v2 port types. The port types are: LAN and WLAN .
Status	For the LAN 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 WLAN, it displays the maximum transmission rate when the WLAN is enabled and N/A when the WLAN is disabled.

10.4.1 Navigation Panel

Use the menu in the navigation panel to configure NBG4615 v2 features in **WISP Mode**.

Figure 57 Menu: WISP Mode

Refer to [Table 26 on page 60](#) for descriptions of the labels shown in the navigation panel.

10.5 Wireless LAN General Screen

Use this screen to configure the wireless LAN settings of your NBG4615 v2. Go to **Configuration > Network > Wireless LAN > General** to open the following screen.

Figure 58 WISP Mode: Wireless LAN > General

The following table describes the labels in this screen.

Table 35 WISP Mode: Wireless LAN > General

LABEL	DESCRIPTION
WISP Parameters	
SSID	Enter the name of the access point to which you are connecting.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. Select the channel number used by the access point to which you are connecting.
Security Mode	Select the security mode of the access point to which you want to connect.
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.5.1 No Security

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

Figure 59 No Security (WISP)

The following table describes the labels in this screen.

Table 36 No Security (WISP)

LABEL	DESCRIPTION
WISP Parameters	
SSID	Enter the name of the access point to which you are connecting.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. Select the channel number used by the access point to which you are connecting.
Security Mode	Select No Security in this field.
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.5.2 Static WEP

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

Figure 60 WEP (WISP)

The following table describes the labels in this screen.

Table 37 WEP (WISP)

LABEL	DESCRIPTION
WISP Parameters	
SSID	Enter the name of the access point to which you are connecting.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. Select the channel number used by the access point to which you are connecting.
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 NBG4615 v2 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 Open 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 Open unless you want to force a key verification before communication between the wireless client and the NBG4615 v2 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.

Table 37 WEP (WISP) (continued)

LABEL	DESCRIPTION
Key 1 to Key 4	<p>Select a default WEP key to use for data encryption.</p> <p>The WEP keys are used to encrypt data. Both the NBG4615 v2 and the wireless stations must use the same WEP key for data transmission.</p> <p>If you chose 64-bits, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").</p> <p>If you chose 128-bits, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").</p> <p>You must configure at least one key, only one key can be activated at any one time. The default key is key 1.</p>
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.5.3 WPA(2)-PSK

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

Figure 61 WPA-PSK/WPA2-PSK (WISP)

The screenshot shows a configuration window titled 'WISP Parameters'. It has two tabs: 'General' and 'Site Survey'. Under 'General', there are five labeled fields: 'SSID' (text input), 'Channel Selection' (dropdown menu showing 'Channel-11 2462MHz'), 'Security Mode' (dropdown menu showing 'WPA2-PSK'), 'Encryption Type' (radio buttons for 'TKIP' and 'AES', with 'AES' selected), and 'Pre-Shared Key' (text input). At the bottom right are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 38 WPA-PSK/WPA2-PSK (WISP)

LABEL	DESCRIPTION
WISP Parameters	
SSID	Enter the name of the access point to which you are connecting.
Channel Selection	<p>The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel.</p> <p>Select the channel number used by the access point to which you are connecting.</p>
Security Mode	Select WPA-PSK or WPA2-PSK to enable data encryption.
Encryption Type	Select the type of wireless encryption employed by the access point to which you want to connect.
Pre-Shared Key	<p>WPA-PSK/WPA2-PSK uses a simple common password for authentication.</p> <p>Type the pre-shared key employed by the access point to which you want to connect.</p>
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.6 Site Survey Screen

Use this screen to scan for and connect to a wireless network automatically. Go to **Configuration > Network > Wireless LAN > Site Survey** to open the following screen.

Figure 62 Configuration > Wireless LAN > Site Survey (WISP)

The following table describes the labels in this screen.

Table 39 Configuration > Wireless LAN > Site Survey (WISP)

LABEL	DESCRIPTION
Site Survey	
#	Select a wireless device and click Add Profile to open a configuration screen where you can add the selected wireless device to a profile and then enable it. This field is selected if the wireless device is added to an activated profile and the NBG4615 v2 is connecting to it.
SSID	This displays the SSID of the wireless device.
BSSID	This displays the MAC address of the wireless device.
Signal Strength	This displays the strength of the wireless signal. The signal strength mainly depends on the antenna output power and the distance between your NBG4615 v2 and this device.
Channel	This displays the channel number used by this wireless device.
Security	This displays the data encryption and authentication method used by this wireless device.
Rescan	Click this button to search for available wireless devices within transmission range and update this table.
Add Profile	Select a wireless device and click this button to add it to a profile.

WISP + Universal Repeater Mode

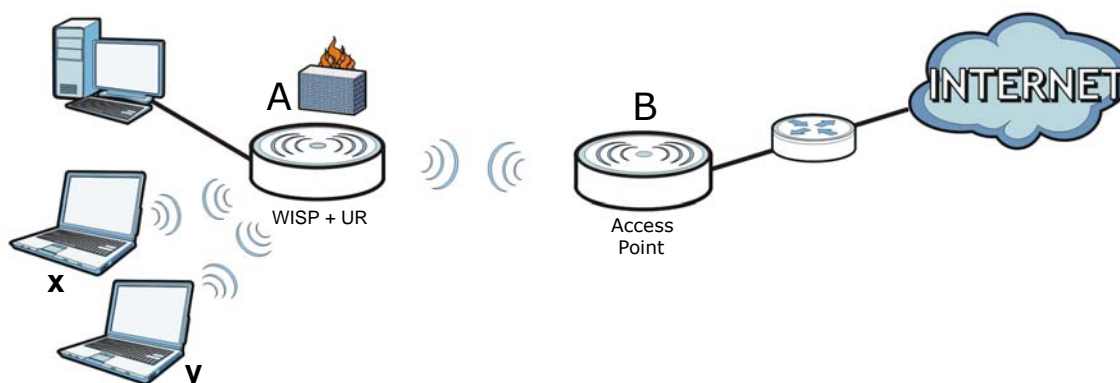
11.1 Overview

In WISP + Universal Repeater (UR) mode, the NBG4615 v2 has the same function as in WISP mode. In addition, it can provide WiFi function to the clients on the LAN side.

Note: When the NBG4615 v2 is in WISP or WISP + Universal Repeater mode, you still need to enter your ISP information in the WAN screen in order to access the Internet.

In the example below, one NBG4615 v2 is configured as WISP + Universal Repeater (UR) mode (**A**) and another is used as an access point (**B**). The NBG4615 v2 (**A**) wirelessly connects to the available access point (**B**), and can allow the clients (**x** and **y**) to access the network through it using a wireless connection.

Figure 63 WISP + UR Mode



11.2 What You Can Do

- Use the **Status** screen to view read-only information about your NBG4615 v2 ([Section 9.5 on page 73](#)).
- Use the **LAN** screen to set the IP address for your NBG4615 v2 ([Section 8.5 on page 67](#)).
- Use the **Wireless LAN > Universal Repeater** screen to associate your NBG4615 v2 (acting as a wireless client) with an existing access point ([Section 9.6 on page 75](#) or [Section 10.5 on page 85](#)).
- Use the **Wireless LAN > Site Survey** screen to scan for available access points within transmission range ([Section 9.6 on page 75](#) or [Section 10.6 on page 89](#)).

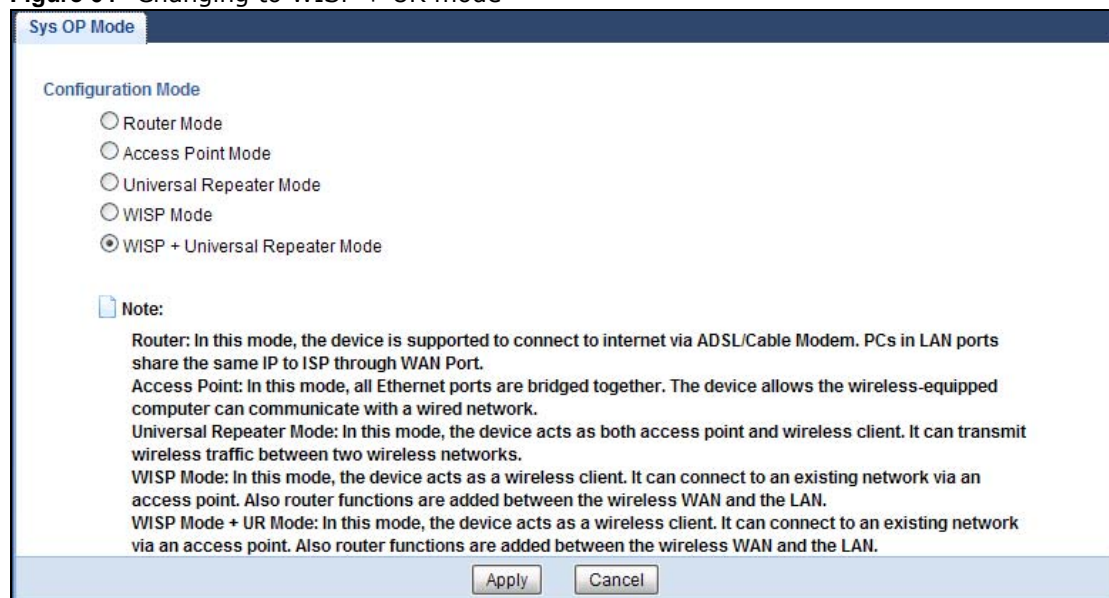
11.3 What You Need to Know

The **Monitor**, **Configuration** and **Maintenance** screens in **WISP + Universal Repeater Mode** are similar to the ones in **Router Mode**. See [Chapter 15 on page 135](#) through [Chapter 26 on page 220](#) of this User's Guide.

11.3.1 Setting your NBG4615 v2 to WISP + UR Mode

- 1 Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.
- 2 To set your NBG4615 v2 to **WISP + Universal Repeater Mode**, go to **Maintenance > Sys OP Mode** and select **WISP + Universal Repeater Mode**.

Figure 64 Changing to WISP + UR mode



Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your NBG4615 v2 is already in **WISP + Universal Repeater Mode**.

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

Figure 65 Pop up window for WISP + UR mode



Click **OK**. Then click **Apply**. The Web Configurator refreshes once the change to **WISP + Universal Repeater Mode** is successful.

11.3.2 Accessing the Web Configurator in WISP + UR Mode

To login to Web Configurator in **WISP + Universal Repeater Mode**, do the following:

- 1 Connect your computer to the LAN port of the NBG4615 v2.
- 2 The default IP address of the NBG4615 v2 is "192.168.1.1". If you did not change this, you can use the same IP address in **WISP + Universal Repeater Mode**. Open a web browser such as Internet Explorer and type "192.168.1.1" as the web address in your web browser.

If you changed the IP address of your NBG4615 v2 while in **Router Mode**, use this IP address in **WISP + Universal Repeater Mode**. The **WISP + Universal Repeater Mode** IP address is always the same as the **Router Mode** IP address.

Note: After clicking Login, the **Easy Mode** appears. Refer to [Section on page 45](#) for the **Easy Mode** screens. Click **Expert Mode** to see the screens described in the sections following this.

11.4 WISP + UR Mode Status Screen


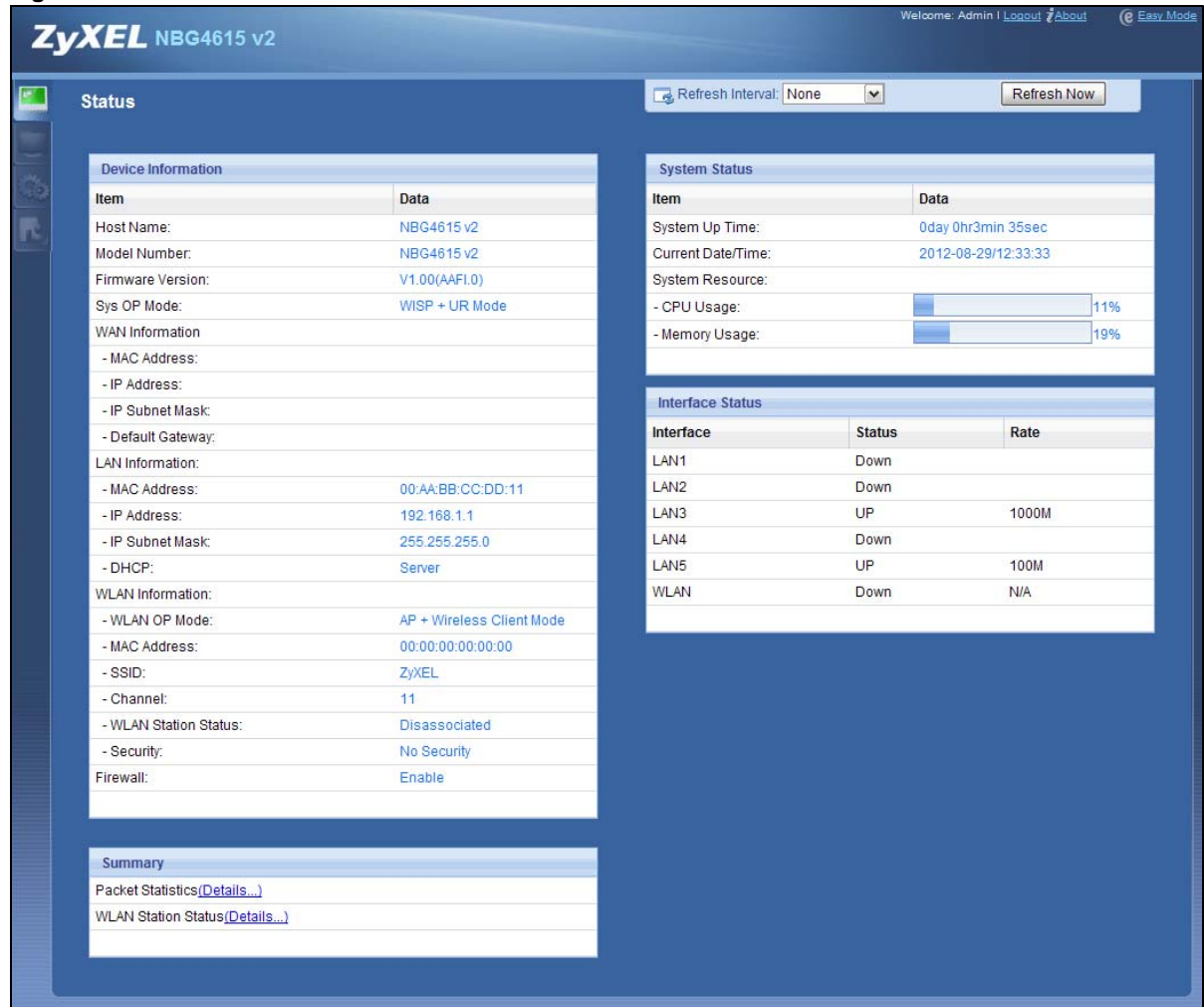
Click  to open the status screen.

Figure 66 Status: WISP + UR Mode

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

Table 40 Status Screen: WISP + UR 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.
Firmware Version	This is the firmware version and the date created.
Sys OP Mode	This is the device mode (Section 5.1.2 on page 43) to which the NBG4615 v2 is set - WISP + UR Mode .
WAN Information	
MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
IP Address	This shows the WAN port's IP address.
IP Subnet Mask	This shows the WAN port's subnet mask.
Default Gateway	This shows the WAN port's gateway IP address.
LAN Information	

Table 40 Status Screen: WISP + UR Mode (continued)

LABEL	DESCRIPTION
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP	This shows the LAN port's DHCP role - Server or Disable .
WLAN Information	
WLAN OP Mode	This is the device mode (Section 5.1.2 on page 43) to which the NBG4615 v2's wireless LAN is set - AP + Wireless Client Mode .
MAC Address	This shows the wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the NBG4615 v2 in the wireless LAN.
Channel	This shows the channel number which you select manually.
WLAN Station Status	If the NBG4615 v2 has successfully connected to an AP or wireless router, it displays the SSID and MAC address of the AP or wireless router in this field. Otherwise, it displays Disassociated .
Security	This shows the level of wireless security the NBG4615 v2 is using.
Firewall	This shows whether the firewall is enabled or not.
Summary	
Packet Statistics	Click Details... to go to the Monitor > Packet Statistics screen (Section 13.5 on page 121). Use this screen to view port status and packet specific statistics.
WLAN Station Status	Click Details... to go to the Monitor > WLAN Station Status screen (Section 13.6 on page 122). Use this screen to view the wireless stations that are currently associated to the NBG4615 v2.
System Status	
Item	This column shows the type of data the NBG4615 v2 is recording.
Data	This column shows the actual data recorded by the NBG4615 v2.
System Up Time	This is the total time the NBG4615 v2 has been on.
Current Date/Time	This field displays your NBG4615 v2's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG4615 v2's processing ability is currently used. When this percentage is close to 100%, the NBG4615 v2 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management).
- Memory Usage	This shows what percentage of the heap memory the NBG4615 v2 is using.
Interface Status	
Interface	This displays the NBG4615 v2 port types. The port types are: LAN and WLAN .
Status	For the LAN 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 WLAN, it displays the maximum transmission rate when the WLAN is enabled and N/A when the WLAN is disabled.

11.4.1 Navigation Panel

Use the menu in the navigation panel to configure NBG4615 v2 features in **WISP + Universal Repeater Mode**.

Figure 67 Menu: WISP +UR Mode



Refer to [Table 26 on page 60](#) for descriptions of the labels shown in the navigation panel.

12.1 Overview

This chapter provides tutorials for setting up your NBG4615 v2.

- [Set Up a Wireless Network with WPS](#)
- [Configure Wireless Security without WPS](#)
- [Using Multiple SSIDs on the NBG4615 v2](#)
- [Connecting the NBG4615 v2 to an AP or Wireless Router](#)
- [Connecting to USB Storage with the ZyXEL NetUSB Share Center Utility](#)
- [Automatically Connecting to a USB Printer](#)

12.2 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 NBG4615 v2 as the AP and NWD210N as the wireless client which connects to a notebook.

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

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

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See [Section 12.2.1 on page 97](#). 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 NBG4615 v2's interface. See [Section 12.2.2 on page 98](#). This is the more secure method, since one device can authenticate the other.

12.2.1 Push Button Configuration (PBC)

- 1 Make sure that your NBG4615 v2 is turned on. Make sure the **WLAN** switch (at the back panel of the NBG4615 v2) is set to **ON**, and that the device is placed within range of your notebook.
- 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 NBG4615 v2's Web Configurator and press the **Push Button** in the **Configuration > Network > Wireless LAN > WPS Station** screen.

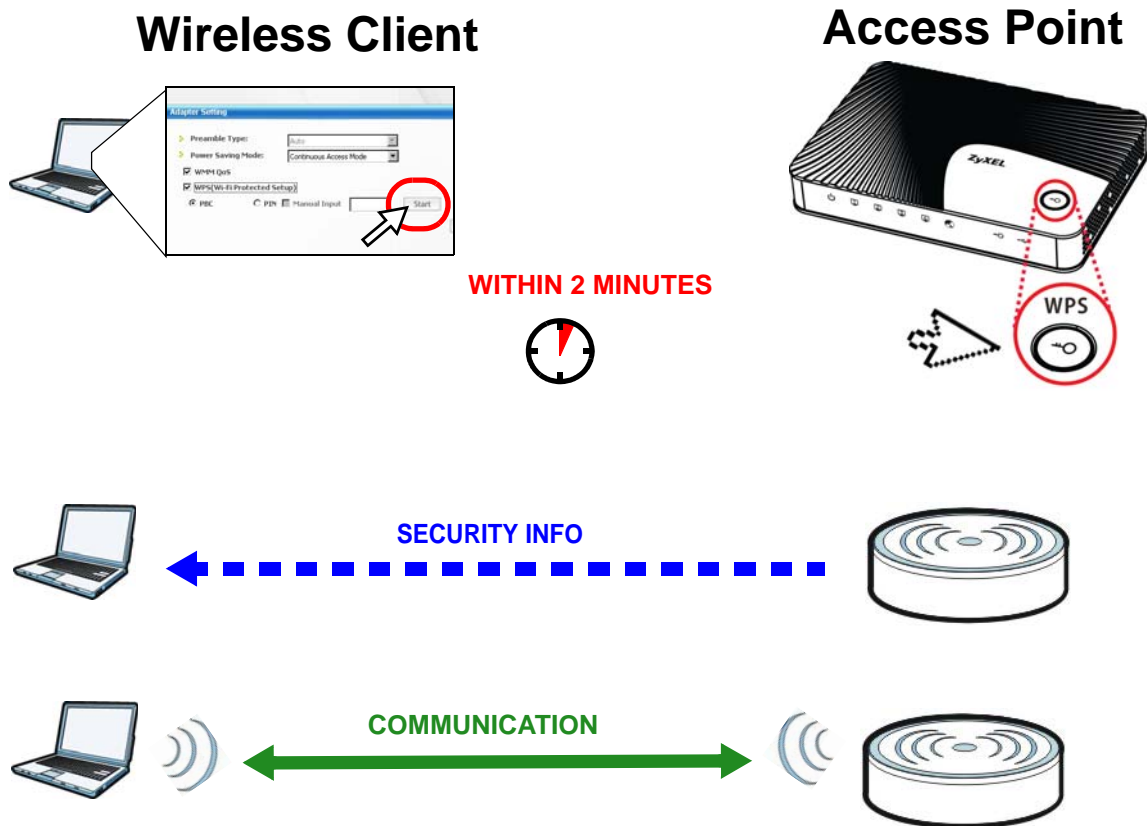
Note: Your NBG4615 v2 has a WPS button located on its panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

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

The NBG4615 v2 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 NBG4615 v2 securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both NBG4615 v2 and wireless client (the NWD210N in this example).

Figure 68 Example WPS Process: PBC Method



12.2.2 PIN Configuration

When you use the PIN configuration method, you need to use both NBG4615 v2's configuration interface and the client's utilities.

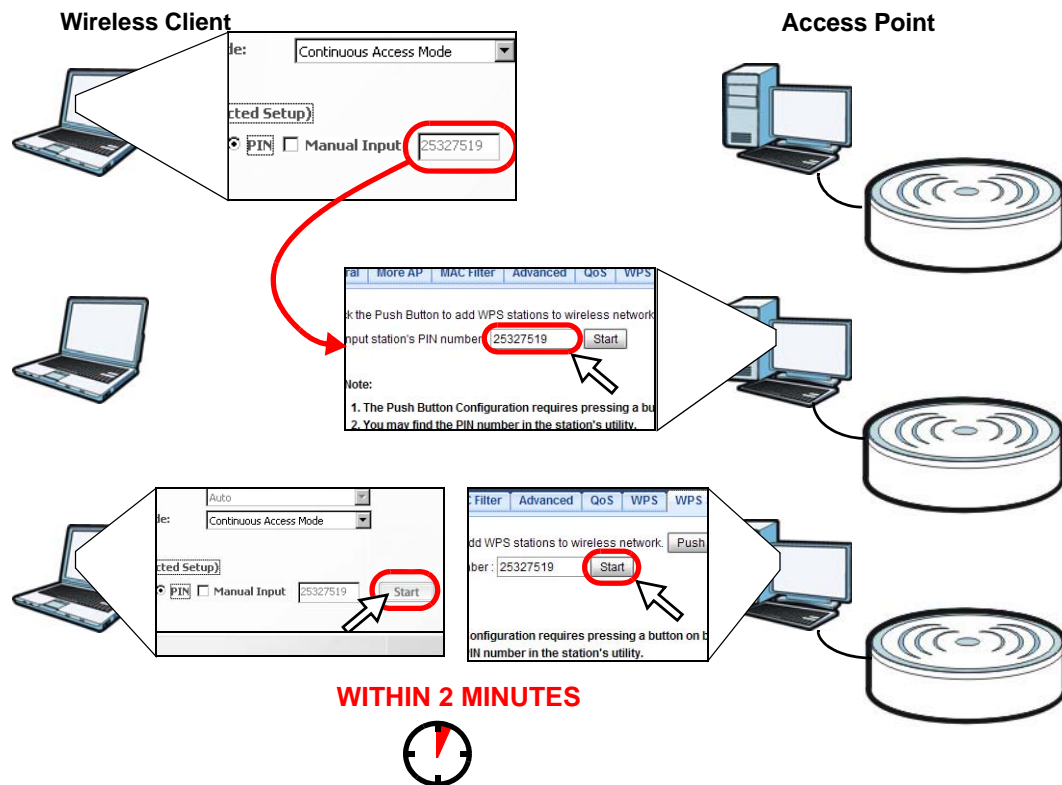
- 1 Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.

- 2 Enter the PIN number to the **PIN** field in the **Configuration > Network > Wireless LAN > WPS Station** screen on the NBG4615 v2.
- 3 Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the NBG4615 v2's **WPS Station** screen within two minutes.

The NBG4615 v2 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 NBG4615 v2 securely.

The following figure shows you the example to set up wireless network and security on NBG4615 v2 and wireless client (ex. NWD210N in this example) by using PIN method.

Figure 69 Example WPS Process: PIN Method



12.3 Configure Wireless Security without WPS

This example shows you how to configure wireless security settings with the following parameters on your NBG4615 v2.

SSID	SSID_Example3
Channel	6
Security	WPA2-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your NBG4615 v2.

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 39](#)).

- 1 Make sure the **WLAN** switch (at the back panel of the NBG4615 v2) is set to **ON**.
- 2 Open the **Configuration > Network > Wireless LAN > General** screen in the AP's Web Configurator.
- 3 Confirm that the status of wireless LAN is **ON**.
- 4 Enter **SSID_Example3** as the SSID and select **Channel-06** as the channel. Set security mode to **WPA2-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

The screenshot displays the 'General' tab of the 'Wireless LAN' configuration page. The 'Wireless Setup' section includes 'Wireless LAN Status' (ON), 'Name (SSID)' (SSID_Example3), and a 'Hide SSID' checkbox. The 'Channel Selection' section shows 'Channel-6 2437MHz' selected, with 'Auto Channel Selection' unchecked. The 'Operating Channel' is 'Channel-', 'Channel Width' is 'Auto 20/40 MHz', and '802.11 Mode' is '802.11bgn'. The 'Security' section shows 'Security Mode' as 'WPA2-PSK', 'WPA-PSK Compatible' checked, 'Pre-Shared Key' as 'ThisismyWPA-PSKpre-sharedkey', and 'Group Key Update Timer' as '3600 seconds'. A note at the bottom states: 'Note: No Security and WPA2-PSK can be configured when WPS enabled.' The 'Apply' and 'Cancel' buttons are at the bottom right.

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

Status

Refresh Interval: None Refresh Now

Item	Data
Host Name:	NBG4615 v2
Model Number:	NBG4615 v2
Firmware Version:	V1.00(AAF1.0)
Sys OP Mode:	ROUTER Mode
WAN Information	
- MAC Address:	00:AA:BB:CC:DD:12
- IP Address:	172.16.37.15
- IP Subnet Mask:	255.255.255.0
- Default Gateway:	172.16.37.254
LAN Information	
- MAC Address:	00:AA:BB:CC:DD:11
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
WLAN Information	
- WLAN OP Mode:	Access Point Mode
- MAC Address:	00:AA:BB:CC:DD:11
- SSID:	SSID_Example3
- Channel:	6
- Security:	WPA-PSK / WPA2-PSK
Firewall:	Enable

Item	Data
System Up Time:	1day 0hr3min 27sec
Current Date/Time:	2012-09-11/01:56:45
System Resource:	
- CPU Usage:	2%
- Memory Usage:	22%

Interface	Status	Rate
WAN	UP	100M
LAN1	Down	
LAN2	Down	
LAN3	UP	1000M
LAN4	Down	
WLAN	UP	300M

Summary

Packet Statistics([Details...](#))

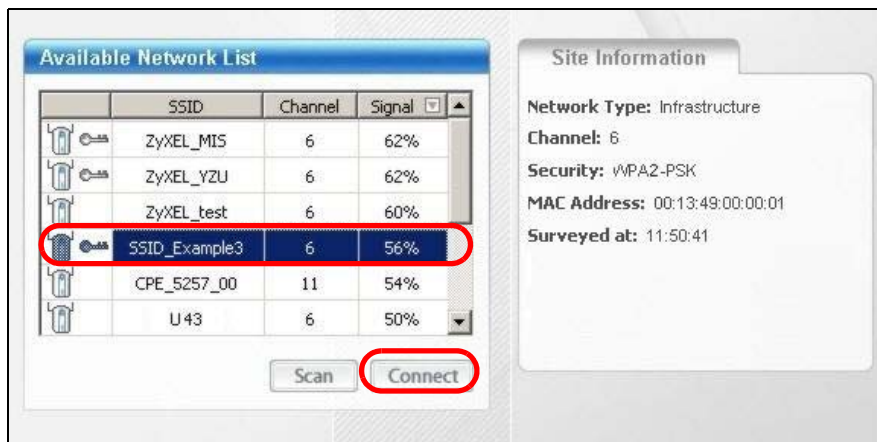
WLAN Station Status([Details...](#))

12.3.1 Configure Your Notebook

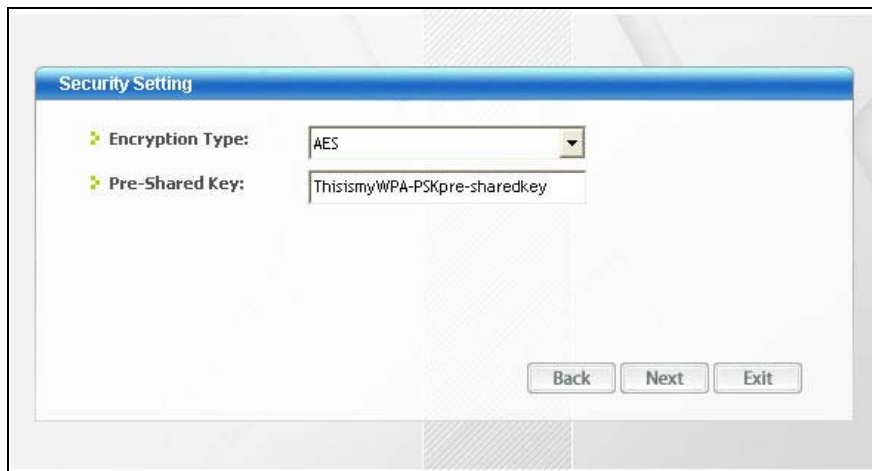
Note: We use the ZyXEL NWD2205 wireless adapter utility screens as an example for the wireless client. The screens may vary for different models.

- 1 The NBG4615 v2 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.

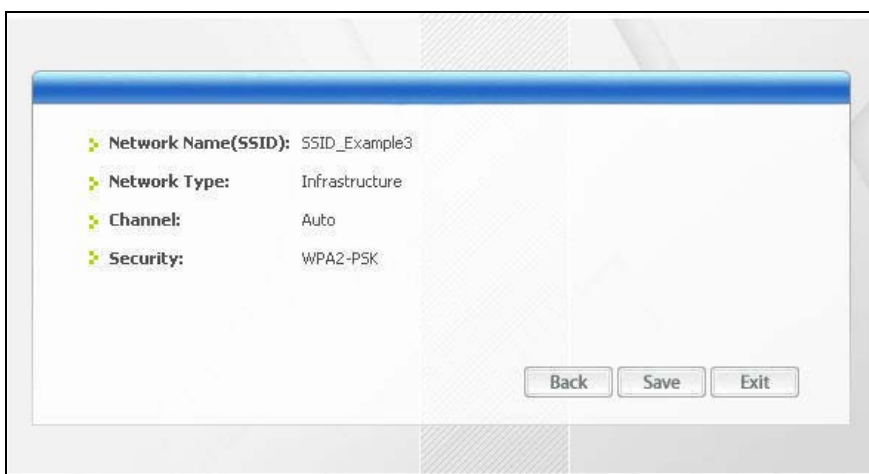
- 4 Select SSID_Example3 and click **Connect**.



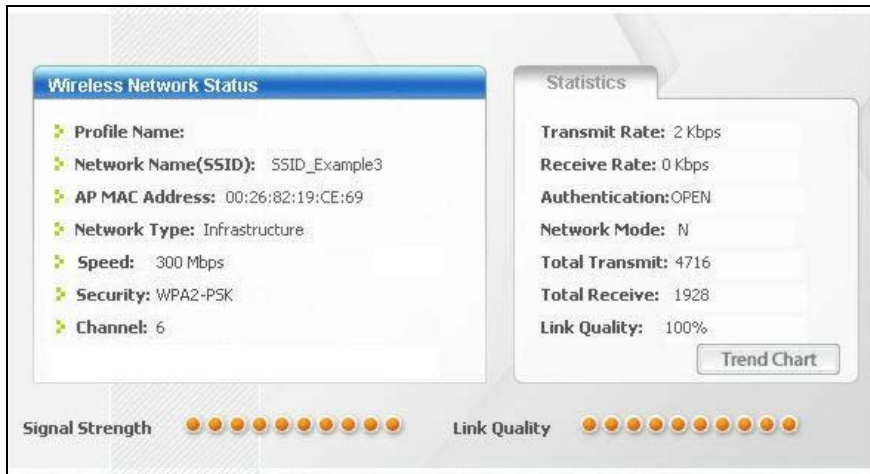
- 5 Select **AES** and type the security key in the following screen. Click **Next**.



- 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.

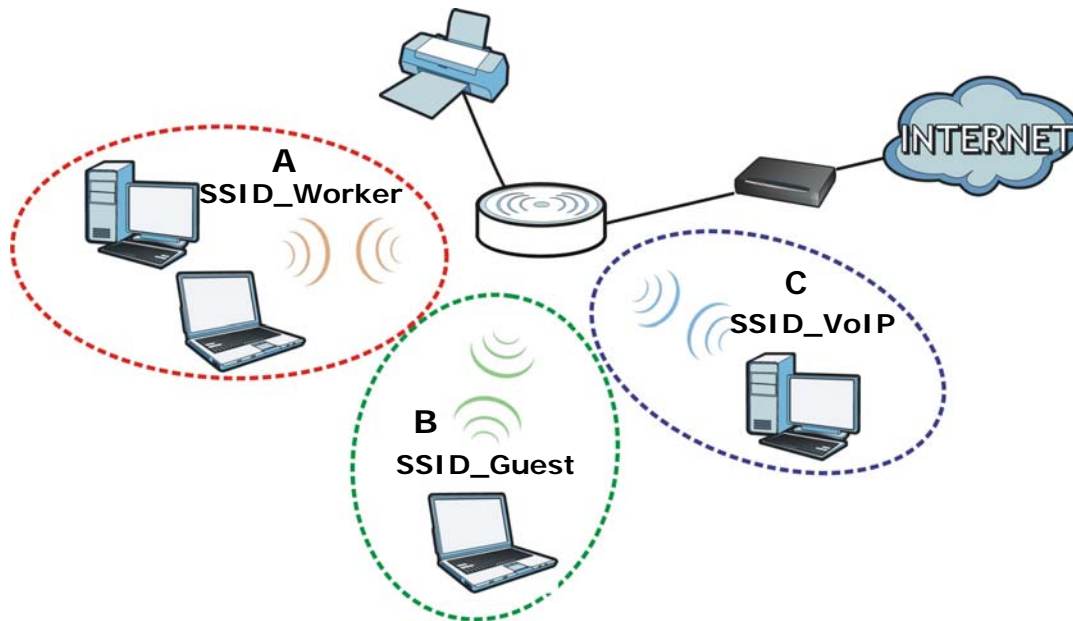
12.4 Using Multiple SSIDs on the NBG4615 v2

You can configure more than one SSID on a NBG4615 v2 when it is operating in certain modes. See [Section 15.4 on page 147](#).

This allows you to configure multiple independent wireless networks on the NBG4615 v2 as if there were multiple APs (virtual APs). Each virtual AP has its own SSID, wireless security type and MAC filtering settings. That is, each SSID on the NBG4615 v2 represents a different access point/wireless network to wireless clients in the network.

Clients can associate only with the SSIDs for which they have the correct security settings. Clients using different SSIDs can access the Internet and the wired network behind the NBG4615 v2 (such as a printer).

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



12.4.1 Configuring Security Settings of Multiple SSIDs

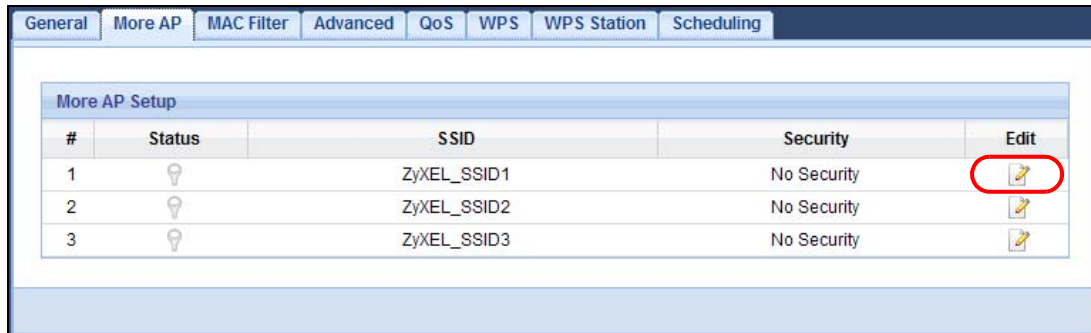
The NBG4615 v2 is in router mode by default.

This example shows you how to configure the SSIDs with the following parameters on your NBG4615 v2 (in router mode).

SSID	SECURITY TYPE	KEY	MAC FILTERING
SSID_Worker	WPA2-PSK WPA Compatible	DoNotStealMyWirelessNetwork	Disable
SSID_VoIP	WPA-PSK	VoIPOnly12345678	Allow 00:A0:C5:01:23:45
SSID_Guest	WPA-PSK	keyexample123	Disable

- 1 Connect your computer to the LAN port of the NBG4615 v2 using an Ethernet cable.
- 2 The default IP address of the NBG4615 v2 in router mode is "192.168.1.1". In this case, your computer must have an IP address in the range between "192.168.1.2" and "192.168.1.254".
- 3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see [Appendix C on page 251](#) for information on changing your computer's IP address.
- 4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.1" as the web address in your web browser.
- 5 Enter "1234" (default) as the password and click **Login**.

- 6 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.
- 7 The **Easy Mode** appears. Click **Expert Mode** in the navigation panel.
- 8 Go to **Configuration > Network > Wireless LAN > More AP**. Click the **Edit** icon of the first entry to configure wireless and security settings for **SSID_Worker**.



- 9 Configure the screen as follows. In this example, you enable **Intra-BSS Traffic** for **SSID_Worker** to allow wireless clients in the same wireless network to communicate with each other. Click **Apply**.

Wireless Setup

Active : ☒

Name (SSID) :

☐ Hide SSID

☒ Intra-BSS Traffic

☒ WMM QoS

Security

Security Mode :

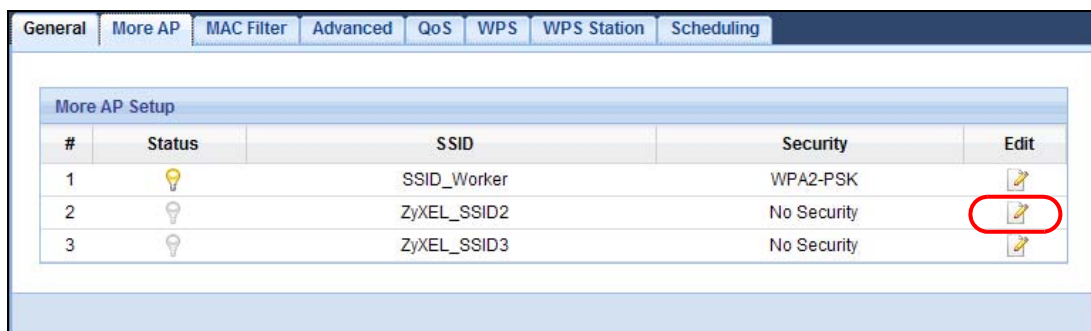
☒ WPA-PSK Compatible

Pre-Shared Key :

Group Key Update Timer : seconds

☐ No Security and WPA2-PSK can be configured when WPS enabled.

- 10 Click the **Edit** icon of the second entry to configure wireless and security settings for **SSID_VoIP**.



- 11 Configure the screen as follows. You do not enable **Intra-BSS Traffic** for **SSID_VoIP**. Click **Apply**.

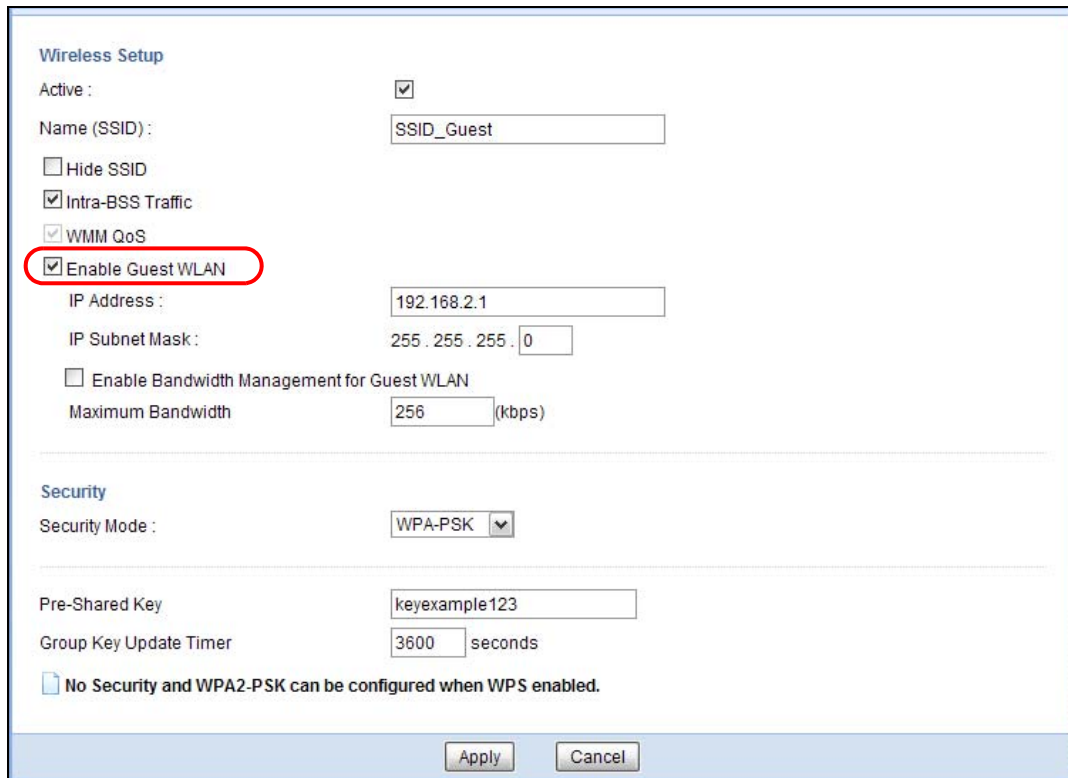
The screenshot shows the 'Wireless Setup' and 'Security' configuration page for a specific SSID. Under 'Wireless Setup', 'Active' is checked, 'Name (SSID)' is 'SSID_VoIP', 'Hide SSID' is unchecked, 'Intra-BSS Traffic' is unchecked, and 'WMM QoS' is checked. Under 'Security', 'Security Mode' is 'WPA-PSK', 'Pre-Shared Key' is 'VoIPOnly12345678', and 'Group Key Update Timer' is '3600 seconds'. A message at the bottom states: 'No Security and WPA2-PSK can be configured when WPS enabled.' 'Apply' and 'Cancel' buttons are at the bottom right.

- 12 Click the **Edit** icon of the third entry to configure wireless and security settings for **SSID_Guest**.

The screenshot shows the 'More AP Setup' table with three entries. The third entry, 'ZyXEL_SSID3', has its 'Edit' icon circled in red.

#	Status	SSID	Security	Edit
1		SSID_Worker	WPA2-PSK	
2		SSID_VoIP	WPA-PSK	
3		ZyXEL_SSID3	No Security	

- 13 Configure the screen as follows. In this example, you enable **Intra-BSS Traffic** for **SSID_Guest** to allow wireless clients in the same wireless network to communicate with each other. Select **Enable Guest WLAN** to allow clients to access the Internet only. Click **Apply**.




The image shows a configuration window with two tabs: "Wireless Setup" and "Security".

Wireless Setup

- Active: ☒
- Name (SSID):
- Hide SSID: ☐
- Intra-BSS Traffic: ☒
- WMM QoS: ☒
- Enable Guest WLAN: ☒**
- IP Address:
- IP Subnet Mask:
- Enable Bandwidth Management for Guest WLAN: ☐
- Maximum Bandwidth: (kbps)

Security

- Security Mode:
- Pre-Shared Key:
- Group Key Update Timer: seconds

 No Security and WPA2-PSK can be configured when WPS enabled.

Buttons:

- 14 Click the **MAC Filter** tab to configure MAC filtering for the **SSID_VoIP** wireless network. Select **SSID_VoIP** from the **SSID Select** drop-down list, enable MAC address filtering and set the **Filter Action** to **Allow**. Enter the VoIP device's MAC address in the **Mac Address** field and click **Apply** to allow only the VoIP device to associate with the NBG4615 v2 using this SSID.

General More AP **MAC Filter** Advanced QoS WPS WPS Station Scheduling

SSID Select:

MAC Address Filter: ☒ Enable ☐ Disable

Filter Action: ☒ Allow ☐ Deny

MAC Filter Summary

Set	MAC Address	Set	MAC Address
1	00:A0:C5:01:23:45	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
5	00:00:00:00:00:00	21	00:00:00:00:00:00
6	00:00:00:00:00:00	22	00:00:00:00:00:00
7	00:00:00:00:00:00	23	00:00:00:00:00:00
8	00:00:00:00:00:00	24	00:00:00:00:00:00
9	00:00:00:00:00:00	25	00:00:00:00:00:00
10	00:00:00:00:00:00	26	00:00:00:00:00:00
11	00:00:00:00:00:00	27	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

12.5 Connecting the NBG4615 v2 to an AP or Wireless Router

If you have an access point or wireless router with Internet access deployed in your network already, and you want to have wireless clients connect to the existing AP or wireless router through the NBG4615 v2, set the NBG4615 v2 to **Universal Repeater Mode** or **WISP + Universal Repeater Mode** and then associate the NBG4615 v2 with the AP or wireless router. The NBG4615 v2 must be within the transmission range of the AP or wireless router.

This example shows you how to configure the NBG4615 v2 in **Universal Repeater Mode**. See [Chapter 11 on page 91](#) for information about **WISP + Universal Repeater Mode**.

- 1 Connect your computer to the LAN port of the NBG4615 v2 using an Ethernet cable.
- 2 The default IP address of the NBG4615 v2 in universal repeater mode is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".
- 3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see [Appendix C on page 251](#) for information on changing your computer's IP address.
- 4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.2" as the web address in your web browser.

- 5 Enter "1234" (default) as the password and click **Login**.
- 6 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.
- 7 The **Easy Mode** appears. Click **Expert Mode** in the navigation panel.
- 8 On the left of the screen, click **Maintenance > Sys OP Mode** and select **Universal Repeater Mode**. Click **Apply**. The NBG4615 v2 restarts.

Sys OP Mode

Configuration Mode

☐ Router Mode
☐ Access Point Mode
☒ Universal Repeater Mode
☐ WISP Mode
☐ WISP + Universal Repeater Mode

Note:

Router: In this mode, the device is supported to connect to internet via ADSL/Cable Modem. PCs in LAN ports share the same IP to ISP through WAN Port.

Access Point: In this mode, all Ethernet ports are bridged together. The device allows the wireless-equipped computer can communicate with a wired network.

Universal Repeater Mode: In this mode, the device acts as both access point and wireless client. It can transmit wireless traffic between two wireless networks.

WISP Mode: In this mode, the device acts as a wireless client. It can connect to an existing network via an access point. Also router functions are added between the wireless WAN and the LAN.

WISP Mode + UR Mode: In this mode, the device acts as a wireless client. It can connect to an existing network via an access point. Also router functions are added between the wireless WAN and the LAN.

Apply Cancel

- 9 Enter the password and click **Login** to access the web configurator again. Click **Expert Mode**.
- 10 Go to **Configuration > Network > Wireless LAN > Universal Repeater** to connect the NBG4615 v2 wirelessly to an AP. Enter the SSID of the existing AP or wireless router to which you want to connect ("SSIDofMyAP" in this example). Select the channel number used by the AP. Enter the wireless security settings which are the same as those on the existing AP or wireless router to access it (WPA-PSK and "KeyofMyWirelessNetwork" in this example). Click **Apply**.

Universal Repeater Parameters

SSID: SSIDofMyAP
 Channel Selection: Channel-5 2432MHz
 Security Mode: WPA-PSK
 Encryption Type: ☒ TKIP ☐ AES
 Pre-Shared Key:

Apply Cancel

- 11 Set the channel number in the **Wireless LAN > General** screen to be the same as the one on the wireless router or AP to which the NBG4615 v2 is connecting. This allows wireless clients access or acquire an IP address from another AP or wireless router through the NBG4615 v2 in universal repeater mode.

The screenshot shows the 'More AP' configuration tab for the NBG4615 v2. The 'Wireless Setup' section includes the following fields:

- Wireless LAN Status : ON
- Name (SSID) : SSID_Example3
- ☐ Hide SSID
- Channel Selection : Channel-5 2432MHz (highlighted with a red circle) ☐ Auto Channel Selection
- Operating Channel : Channel-5
- Channel Width : Auto 20/40 MHz
- 802.11 Mode : 802.11bgn

The 'Security' section includes the following fields:

- Security Mode : WPA2-PSK
- ☒ WPA-PSK Compatible
- Pre-Shared Key : ThisismyWPA-PSKpre-shared!
- Group Key Update Timer : 3600 seconds

A note at the bottom states: 'Note: No Security and WPA2-PSK can be configured when WPS enabled.'

Buttons: Apply, Cancel

- 12 Go to the **Status** screen. If the NBG4615 v2 has successfully connected to an AP or wireless router, it displays **Associated** and the SSID of the AP or wireless router in the field next to **WLAN Station Status** under **Device Information**.

Status

Refresh Interval: None [Refresh Now](#)

Device Information	
Item	Data
Host Name:	NBG4615 v2
Model Number:	NBG4615 v2
Firmware Version:	V1.00(AAF1.0)
Sys OP Mode:	Universal Repeater Mode
LAN Information:	
- MAC Address:	00-AA-BB-CC-DD:11
- IP Address:	192.168.1.2
- IP Subnet Mask:	255.255.255.0
- DHCP:	None
WLAN Information:	
- WLAN OP Mode:	AP + Wireless Client Mode
- MAC Address:	02-AA-BB-CC-DD:10
- SSID:	SSID_Example3
- Channel:	5
- WLAN Station Status:	Associated (SSIDofMyAP)
- Security:	WPA-PSK / WPA2-PSK

System Status	
Item	Data
System Up Time:	0day 0hr10min 1sec
Current Date/Time:	2012-08-29/12:40:06
System Resource:	
- CPU Usage:	5%
- Memory Usage:	21%

Interface Status		
Interface	Status	Rate
LAN1	Down	
LAN2	Down	
LAN3	UP	1000M
LAN4	Down	
LAN5	UP	100M
WLAN	UP	300M

Summary

[Packet Statistics\(Details...\)](#)

[WLAN Station Status\(Details...\)](#)

To check whether a wireless client is currently connecting to the NBG4615 v2, click the **WLAN Station Status (Details...)** hyperlink under **Summary** in the **Status** screen or **Monitor > WLAN Station Status**. See [Chapter 13 on page 119](#) for more information.

Association List

Association List

#	MAC Address	Association Time
1	00:19:CB:32:BE:AC	01:09:05 2000/01/01

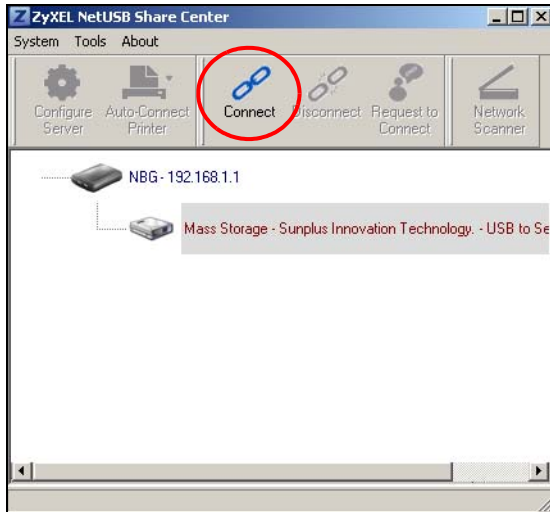
[Refresh](#)

12.6 Connecting to USB Storage with the ZyXEL NetUSB Share Center Utility

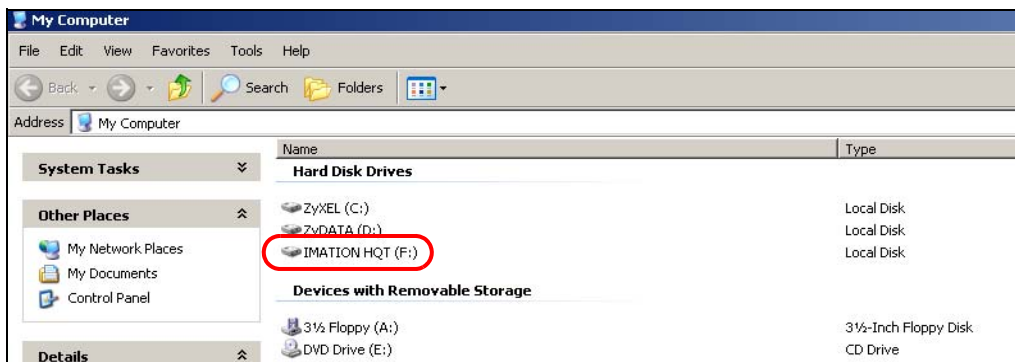
This tutorial shows you how to connect to a USB device over your NBG4615 v2 network by using the ZyXEL NetUSB Share Center Utility.

- 1 Install the ZyXEL NetUSB Share Center Utility on the computer to which you want to connect the USB device. See [Chapter 2 on page 22](#) for details on the installation.

- 2 Connect a USB device to one of the USB ports of the NBG4615 v2.
- 3 Open the **ZyXEL NetUSB Sharing Center Utility** on your computer. The name of the USB device automatically shows in the Utility screen.
- 4 Click on the USB device's name. Then click **Connect**.



- 5 The device mounts on your system.



12.6.1 Multiple Connections to the USB Device

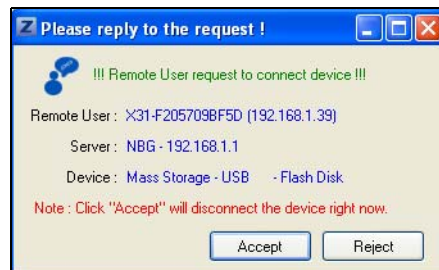
The Utility supports one connection to the NBG4615 v2's USB device at a time. If more than one computer want to connect to the USB device, follow the steps below:

- 1 After the first computer (**A**) finishes using the USB device, click **Disconnect** on the Utility to unmount it.
- 2 Click **Connect** on the Utility of the second computer (**B**) to mount the USB device on **B**.

- 3 If **A** does not disconnect from the USB device, **B** cannot use it. **B** can click the **Request to Connect** button to request **A** to disconnect. **B** will see the following message on its Utility:



- 4 **A** will receive the following message on its Utility screen.



- 5 **A** should click **Accept** to disconnect to the USB device.
- 6 After **A** is disconnected from USB device, **B** will see the following message on its Utility. Now **B** can access the USB device.

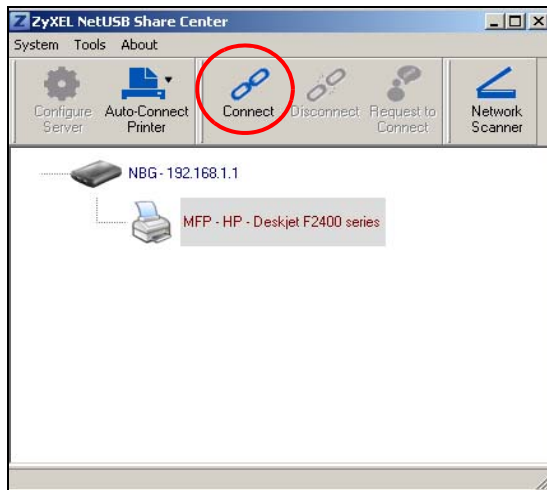


Note: If your computer is connected to a USB device, you must disconnect it and use **Exit** to close the Utility. If you use the X on the Utility screen, it only closes the Utility window. The Utility is still connected. Do not exit the Utility until the USB device is disconnected via the Utility or until you receive a request to disconnect. See [Chapter 2 on page 26](#) for details on how to exit the Utility.

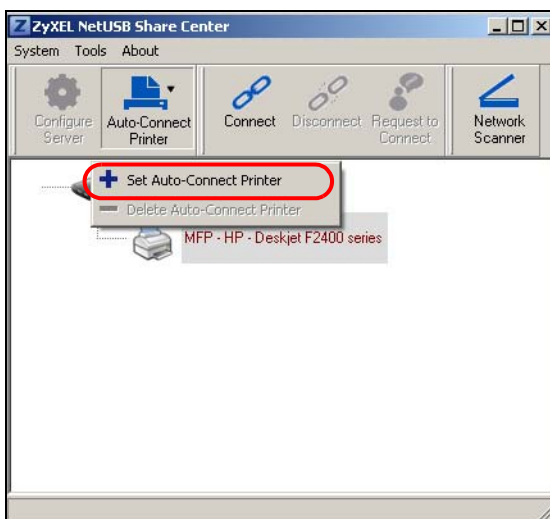
12.7 Automatically Connecting to a USB Printer

Your computer can connect to a shared USB printer by using the ZyXEL NetUSB Share Center Utility. This tutorial shows you how to set your computer to automatically connect to a shared USB printer over your NBG4615 v2 network each time you log into your computer.

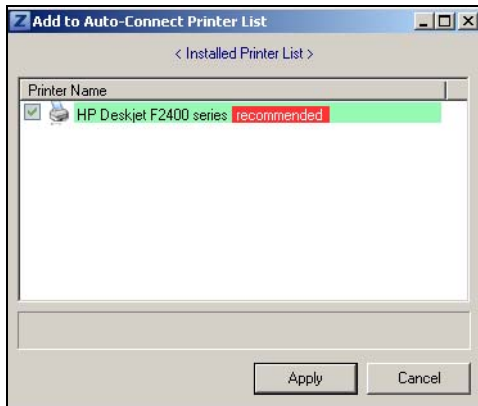
- 1 Install the ZyXEL NetUSB Share Center Utility to your computer. See [Chapter 2 on page 22](#) for details on the installation.
- 2 Connect a USB printer to one of the USB ports of the NBG4615 v2.
- 3 Open the **ZyXEL NetUSB Sharing Center Utility** on your computer. The name of the USB printer automatically shows in the Utility screen.
- 4 Click on the printer name. Then click **Connect**. Your computer will search for the printer driver. You may be prompted to install the driver. Follow the driver's installation steps to finish installing.



- 5 Click the **Auto-Connect Printer** menu and select **Set Auto-Connect Printer** from the menu.



- 6 Select the USB printer you want to connect to and click **Apply**.



- 7 Now your computer can automatically connect to this shared USB printer over your NBG4615 v2 network each time you log into your computer. The printer will be automatically added to your printer list.
- 8 The Utility supports one connection to the NBG4615 v2's USB device at a time. If more than one computer is using the printer and are all auto-connected to the USB device, the second computer automatically starts printing after the first computer finishes its printing task.

PART II

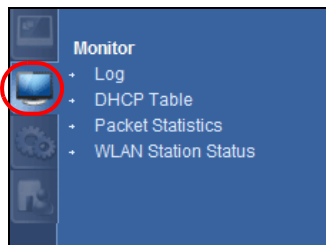
Technical Reference

Monitor

13.1 Overview

This chapter discusses read-only information related to the device state of the NBG4615 v2.

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



You can also click the links in the **Summary** table of the **Status** screen to view the packets sent/received as well as the status of clients connected to the NBG4615 v2.

13.2 What You Can Do

- Use the **Log** screen to see the logs for the activity on the NBG4615 v2 ([Section 13.3 on page 119](#)).
- Use the **DHCP Table** screen to view information related to your DHCP status ([Section 13.4 on page 120](#)).
- use the **Packet Statistics** screen to view port status, packet specific statistics, the "system up time" and so on ([Section 13.5 on page 121](#)).
- Use the **WLAN Station Status** screen to view the wireless stations that are currently associated to the NBG4615 v2 ([Section 13.6 on page 122](#)).

13.3 The Log Screen

The Web Configurator allows you to look at all of the NBG4615 v2's logs in one location.

13.3.1 View Log

Use the **View Log** screen to see the logged messages for the NBG4615 v2. 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 Setting** screen. Click **Refresh** to renew the log screen. Click **Clear Log** to delete all the logs.

Figure 70 View Log

View Log | Log Setting

Display: Access Control [v] Refresh Clear Log

#	Time	Message
1	Aug 22 08:58:02	v2 user.alert kernel: portscan protect:IN=vlan10 OUT=MAC=ff:ff:ff:ff:ff:ff:00:1f:16:0f:69:de:08:00:45:00:01:f0 SRC=172.16.37.17 DST=255.255.255.255 LEN=496 TOS=0x00 PREC=0x00 TTL=128 ID=54908 PROTO=UDP SPT=2872 DPT=43440 LEN=476
2	Aug 22 08:57:58	v2 user.alert kernel: portscan protect:IN=vlan10 OUT=MAC=ff:ff:ff:ff:ff:ff:00:26:55:48:db:dd:08:00:45:00:00:31 SRC=172.16.37.30 DST=255.255.255.255 LEN=49 TOS=0x00 PREC=0x00 TTL=128 ID=5242 PROTO=UDP SPT=1615 DPT=9997 LEN=29
3	Aug 22 08:57:53	v2 user.alert kernel: portscan protect:IN=vlan10 OUT=MAC=ff:ff:ff:ff:ff:ff:00:26:55:48:db:dd:08:00:45:00:00:31 SRC=172.16.37.30 DST=255.255.255.255 LEN=49 TOS=0x00 PREC=0x00 TTL=128 ID=5221 PROTO=UDP SPT=1615 DPT=9997 LEN=29
4	Aug 22 08:57:50	v2 user.alert kernel: portscan protect:IN=vlan10 OUT=MAC=ff:ff:ff:ff:ff:ff:00:1e:33:2a:12:5a:08:00:45:00:00:ad SRC=172.16.37.5 DST=255.255.255.255 LEN=173 TOS=0x00 PREC=0x00 TTL=128 ID=8398 PROTO=UDP SPT=17500 DPT=17500 LEN=153
5	Aug 22 08:57:50	v2 user.alert kernel: portscan protect:IN=vlan10 OUT=MAC=ff:ff:ff:ff:ff:ff:00:1e:33:2a:12:5a:08:00:45:00:00:ad SRC=172.16.37.5 DST=172.16.37.255 LEN=173 TOS=0x00 PREC=0x00 TTL=128 ID=8397 PROTO=UDP SPT=17500 DPT=17500 LEN=153
6	Aug 22 08:57:48	v2 user.alert kernel: portscan protect:IN=vlan10 OUT=MAC=ff:ff:ff:ff:ff:ff:00:26:55:48:db:dd:08:00:45:00:00:31 SRC=172.16.37.30 DST=255.255.255.255 LEN=49 TOS=0x00 PREC=0x00 TTL=128 ID=5220 PROTO=UDP SPT=1615 DPT=9997 LEN=29

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

Figure 71 Log Settings

View Log | Log Setting

Active Log and Alert

Log

- ☒ System Errors
- ☒ On-line Firmware upgrade
- ☒ Access Control

Apply Cancel

13.4 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 NBG4615 v2's LAN as a DHCP server or disable it. When configured as a server, the NBG4615 v2 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 **Configuration > Network > DHCP Server > Client List**. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **MAC Address**, and **IP Address**) of all network clients using the NBG4615 v2's DHCP server.

Figure 72 Monitor > DHCP Table

The screenshot shows a web interface titled "DHCP Table". It contains a table with the following data:

#	Status	Host Name	IP Address	MAC Address	Reserve
1		twpc	192.168.1.46	00:21:85:0c:44:4b	<input type="checkbox"/>

At the bottom of the interface are two buttons: "Apply" and "Cancel".

The following table describes the labels in this screen.

Table 41 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 NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

13.5 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 73 Summary: Packet Statistics

Packet Statistics							
Packet Statistics							
Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100M	20845	41896	0	767	2588	1: 39: 11
LAN	1000M	54849	65710	0	3565	3580	1: 39: 11
WLAN	Down	0	0	0	0	0	1: 39: 11

System Up Time : 1: 39: 11

Poll Interval(s) :

The following table describes the labels in this screen.

Table 42 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the NBG4615 v2'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 NBG4615 v2 has been for each session.
System Up Time	This is the total time the NBG4615 v2 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.

13.6 WLAN Station Status

Click **Monitor > WLAN Station Status** or the **WLAN Station Status (Details...)** hyperlink in the **Status** screen. View the wireless stations that are currently associated to the NBG4615 v2 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 74 Summary: Wireless Association List

Association List		
Association List		
#	MAC Address	Association Time
1	00:22:FB:65:9A:F4	03:39:07 1970/01/01

The following table describes the labels in this screen.

Table 43 Summary: Wireless Association List

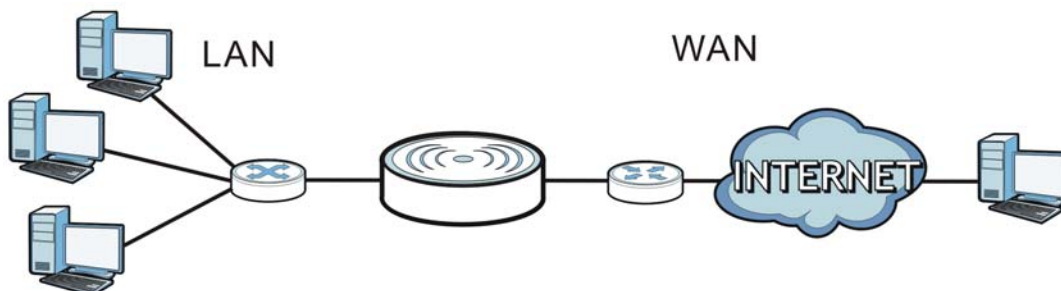
LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the NBG4615 v2's WLAN network.

14.1 Overview

This chapter discusses the NBG4615 v2's **WAN** screens. Use these screens to configure your NBG4615 v2 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 75 LAN and WAN



14.2 What You Can Do

- Use the **Internet Connection** screen to enter your ISP information and set how the computer acquires its IP, DNS and WAN MAC addresses ([Section 14.4 on page 127](#)).
- Use the **Advanced** screen to enable multicasting, configure Windows networking and bridge ([Section 14.5 on page 134](#)).

14.3 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 NBG4615 v2.

14.3.1 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 NBG4615 v2, which makes it accessible from an outside network. It is used by the NBG4615 v2 to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the NBG4615 v2 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 NBG4615 v2 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 NBG4615 v2's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

WAN MAC Address

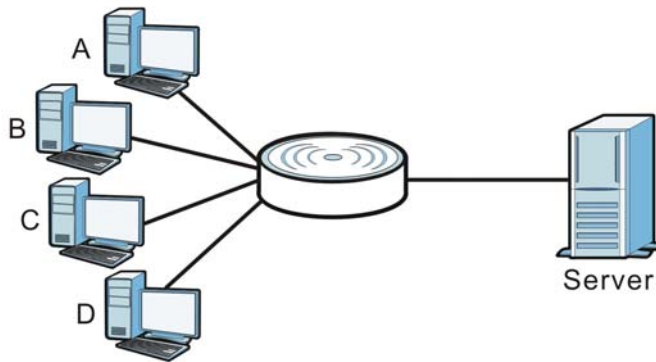
The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

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.

14.3.2 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 76 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 NBG4615 v2 supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**).

At start up, the NBG4615 v2 queries all directly connected networks to gather group membership. After that, the NBG4615 v2 periodically updates this information. IP multicasting can be enabled/disabled on the NBG4615 v2 WAN interface in the Web Configurator (**WAN**). Select **None** to disable IP multicasting on these interfaces.

14.4 Internet Connection

Use this screen to change your NBG4615 v2's Internet access settings. Click **WAN** from the **Configuration** menu. The screen differs according to the encapsulation you choose.

14.4.1 IPoE Encapsulation

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

Figure 77 Network > WAN > Internet Connection: IPoE Encapsulation

Internet Connection

Advanced

ISP Parameters for Internet Access

Encapsulation : IPoE

IP Address

☒ Obtain an IP Address Automatically

☐ Static IP Address

IP Address :

Subnet Mask :

DNS Server

First DNS Server : Obtained From ISP

Second DNS Server : Obtained From ISP

Third DNS Server : Obtained From ISP

WAN MAC Address

☒ Factory default

☐ Clone the computer's MAC address - IP Address

☐ Set WAN MAC Address

Apply

Cancel

The following table describes the labels in this screen.

Table 44 Network > WAN > Internet Connection: IPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the IPoE option when the WAN port is used as a regular Ethernet.
IP Address	
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.
MTU Size	Enter the MTU (Maximum Transmission Unit) size for each packet. If a larger packet arrives, the NBG4615 v2 divides it into smaller fragments.
DNS Server	

Table 44 Network > WAN > Internet Connection: IPoE Encapsulation (continued)

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the NBG4615 v2's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined , but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply . If you set a second choice to User-Defined , and enter the same IP address, the second User-Defined changes to None after you click Apply . Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG4615 v2's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select Factory default to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select Clone the computer's MAC address - IP Address and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

14.4.2 PPPoE Encapsulation

The NBG4615 v2 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 NBG4615 v2 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG4615 v2 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 78 Network > WAN > Internet Connection: PPPoE Encapsulation

The screenshot shows the 'Internet Connection' tab of the WAN configuration interface. The 'Encapsulation' is set to 'PPPoE'. Under 'PPP Information', the username is 'sagasg', the password is masked with dots, and the MTU size is 1454. The 'PPP Auto Connect' checkbox is unchecked. In the 'WAN IP Address Assignment' section, the radio button for 'Get automatically from ISP' is selected. The 'DNS Server' section shows three servers, all with the dropdown set to 'Obtained From ISP'. The 'WAN MAC Address' section has the 'Factory default' radio button selected. At the bottom, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 45 Network > WAN > Internet Connection: PPPoE Encapsulation

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.
MTU Size	Enter the Maximum Transmission Unit (MTU) or the largest packet size per frame that your NBG4615 v2 can receive and process.
PPP Auto Connect	Select this option if you do not want the connection to time out.
Idle Timeout (second)	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server.
PPPoE Service Name	Enter the PPPoE service name specified in the ISP account.
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.

Table 45 Network > WAN > Internet Connection: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
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	<p>Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the NBG4615 v2's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
Second DNS Server	
Third DNS Server	
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the NBG4615 v2's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select Factory default to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select Clone the computer's MAC address - IP Address and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

14.4.3 PPTP Encapsulation

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

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

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

Figure 79 Network > WAN > Internet Connection: PPTP Encapsulation

Internet Connection

Advanced

ISP Parameters for Internet Access

Encapsulation : PPTP

PPTP Information

PPTP Username :

PPTP Password :

MTU Size : 1454

PPTP Auto Connect : ☐

IDLE Timeout [second] : 300

PPTP CONFIGURATION

PPTP Server IP Address :

☒ Obtain an IP Address Automatically

☐ Static IP Address

IP Address : 1.2.3.4

Subnet Mask : 255.255.255.0

Gateway IP address :

WAN IP Address Assignment

☒ Get automatically from ISP

☐ Use Fixed IP Address

My WAN IP Address :

DNS Server

First DNS Server : Obtained From ISP

Second DNS Server : Obtained From ISP

Third DNS Server : Obtained From ISP

WAN MAC Address

☒ Factory default

☐ Clone the computer's MAC address - IP Address

☐ Set WAN MAC Address

Apply

Cancel

The following table describes the labels in this screen.

Table 46 Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	To configure a PPTP client, you must configure the User Name and Password fields for a PPP connection and the PPTP parameters for a PPTP connection.
PPTP Information	
PPTP Username	Type the user name given to you by your ISP.

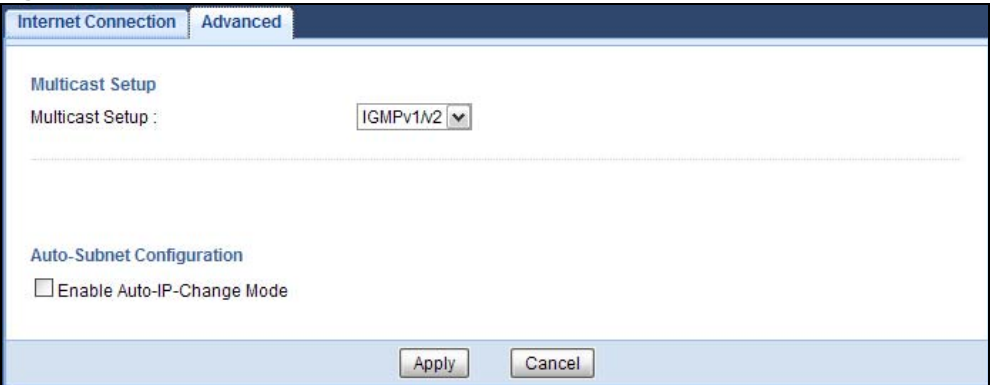
Table 46 Network > WAN > Internet Connection: PPTP Encapsulation (continued)

LABEL	DESCRIPTION
PPTP Password	Type the password associated with the User Name above.
MTU Size	Enter the Maximum Transmission Unit (MTU) or the largest packet size per frame that your NBG4615 v2 can receive and process.
PPPTP 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 NBG4615 v2 automatically disconnects from the PPTP server.
PPTP Configuration	
PPTP Server IP Address	Type the IP address of the PPTP server.
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 Use Fixed IP Address .
Subnet Mask	Your NBG4615 v2 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 NBG4615 v2.
Gateway IP Address	Enter a Gateway IP Address (if your ISP gave you one) in this field.
WAN IP Address Assignment	
Get automatically from ISP	Select this to get your WAN IP address from your ISP.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected Use Fixed IP Address .
DNS Server	
First DNS Server Second DNS Server Third DNS Server	<p>Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the NBG4615 v2's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG4615 v2's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select Factory default to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select Clone the computer's MAC address - IP Address and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

14.5 Advanced WAN Screen

To change your NBG4615 v2’s advanced WAN settings, click **Network > WAN > Advanced**. The screen appears as shown.

Figure 80 Network > WAN > Advanced



The following table describes the labels in this screen.

Table 47 Network > WAN > Advanced

LABEL	DESCRIPTION
Multicast Setup	
Multicast	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.
Auto-Subnet Configuration	
Enable Auto-IP-Change mode	Select this option to have the NBG4615 v2 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG4615 v2 gets a dynamic WAN IP address in the same subnet as the LAN IP address 192.168.1.1 or 10.0.0.1. The NAT, DHCP server and firewall functions on the NBG4615 v2 are still available in this mode.
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

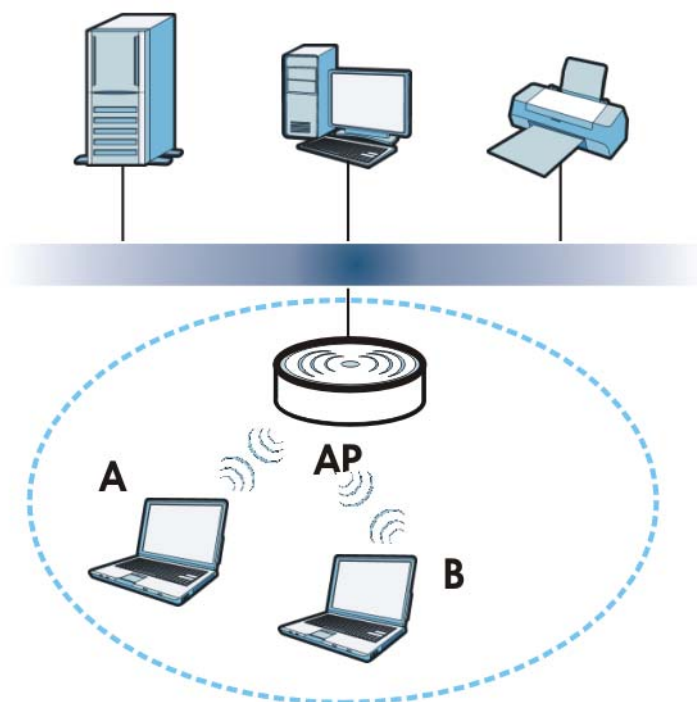
Wireless LAN

15.1 Overview

This chapter discusses how to configure the wireless network settings in your NBG4615 v2. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 81 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 NBG4615 v2 is the AP.

15.1.1 What You Can Do

- Use the **General** screen to turn the wireless connection on or off, set up wireless security between the NBG4615 v2 and the wireless clients, and make other basic configuration changes ([Section 15.2 on page 140](#)).
- Use the **More AP** screen to set up multiple wireless networks on your NBG4615 v2 ([Section 15.4 on page 147](#)).
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the NBG4615 v2 ([Section 15.5 on page 150](#)).
- Use the **Advanced** screen to allow intra-BSS networking and set the RTS/CTS Threshold ([Section 15.6 on page 152](#)).
- Use the **QoS** screen to ensure Quality of Service (QoS) in your wireless network ([Section 15.7 on page 152](#)).
- Use the **WPS** screen to quickly set up a wireless network with strong security, without having to configure security settings manually ([Section 15.8 on page 153](#)).
- Use the **WPS Station** screen to add a wireless station using WPS ([Section 15.9 on page 155](#)).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off ([Section 15.10 on page 155](#)).

15.1.2 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.

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.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.

2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

The types of encryption you can choose depend on the type of user authentication. (See [page 137](#) for information about this.)

Table 48 Types of Encryption for Each Type of Authentication

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

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

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

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

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

When you select **WPA2** or **WPA2-PSK** in your NBG4615 v2, 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 NBG4615 v2.

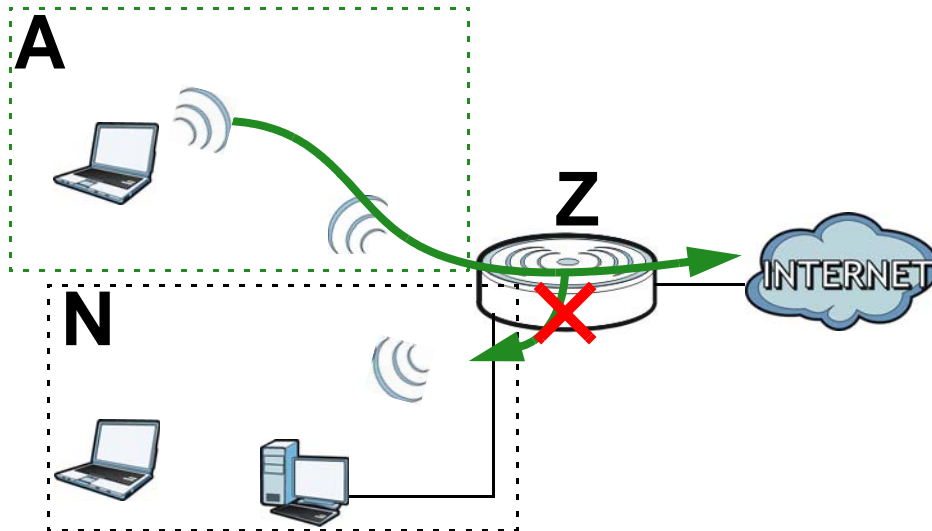
Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

Guest WLAN

Guest WLAN allows you to set up a wireless network where users can access to Internet via the NBG4615 v2 (**Z**), but not other networks connected to the **Z**. In the following figure, a guest user can access the Internet from the guest wireless network **A** via **Z** but not the home or company network **N**.

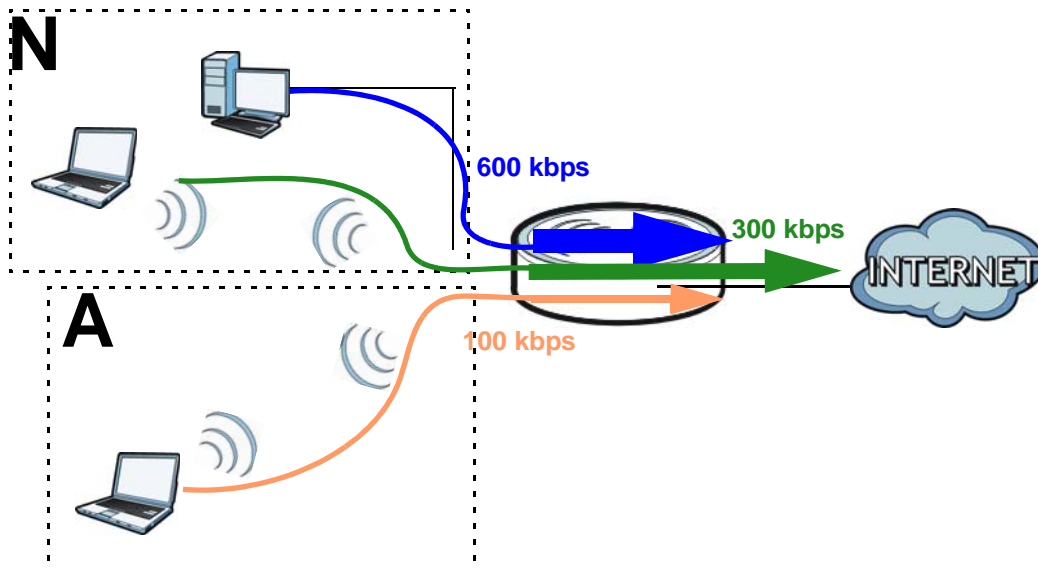
Note: The home or company network **N** and Guest WLAN network are independent networks.

Note: Only Router mode supports guest WLAN. AP mode, Universal Repeater mode, WISP mode and WISP + Universal Repeater mode don't support guest WLAN.

Figure 82 Guest Wireless LAN Network

Guest WLAN Bandwidth

The Guest WLAN Bandwidth function allows you to restrict the maximum bandwidth for the guest wireless network. Additionally, you can also define bandwidth for your home or office network. An example is shown next to define maximum bandwidth for your networks (**A** is Guest WLAN and **N** is home or company network.)

Figure 83 Example: Bandwidth for Different Networks

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 12.2 on page 97](#).

15.2 General Wireless LAN Screen

Use this screen to configure the SSID and wireless security of the wireless LAN.

Note: If you are configuring the NBG4615 v2 from a computer connected to the wireless LAN and you change the NBG4615 v2'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 NBG4615 v2's new settings.

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

Figure 84 Network > Wireless LAN > General

The screenshot shows the 'General' configuration page for the wireless LAN. It includes tabs for various settings like 'More AP', 'MAC Filter', 'Advanced', 'QoS', 'WPS', 'WPS Station', and 'Scheduling'. The 'Wireless Setup' section contains fields for 'Wireless LAN Status' (OFF), 'Name (SSID)' (ZyXEL), 'Hide SSID' (unchecked), 'Channel Selection' (Channel-1 2412MHz), 'Auto Channel Selection' (checked), 'Operating Channel' (Channel-), 'Channel Width' (Auto 20/40 MHz), and '802.11 Mode' (802.11bgn). The 'Security' section shows 'Security Mode' set to 'No Security'. A note at the bottom indicates that 'No Security and WPA2-PSK can be configured when WPS enabled.' The page concludes with 'Apply' and 'Cancel' buttons.

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

Table 49 Network > Wireless LAN > General

LABEL	DESCRIPTION
Wireless LAN	This shows whether the wireless LAN is ON or OFF . You can enable or disable the wireless LAN by using the WLAN switch located on the back panel of the NBG4615 v2.
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.

Table 49 Network > Wireless LAN > General (continued)

LABEL	DESCRIPTION
Channel Selection	<p>Set the operating frequency/channel depending on your particular region.</p> <p>Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in.</p> <p>Refer to the Connection Wizard chapter for more information on channels. This option is only available if Auto Channel Selection is disabled.</p>
Auto Channel Selection	<p>Select this check box for the NBG4615 v2 to automatically choose the channel with the least interference. Deselect this check box if you wish to manually select the channel using the Channel Selection field.</p>
Operating Channel	<p>This displays the channel the NBG4615 v2 is currently using.</p>
Channel Width	<p>Select the wireless channel width used by NBG4615 v2.</p> <p>A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps.</p> <p>Because not all devices support 40 MHz channels, select Auto 20/40MHz to allow the NBG4615 v2 to adjust the channel bandwidth automatically.</p> <p>40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.</p> <p>Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.</p>
802.11 Mode	<p>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 NBG4615 v2. 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 NBG4615 v2 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 NBG4615 v2. The NBG4615 v2 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 NBG4615 v2. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the NBG4615 v2. I • 802.11gn: allows either IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the NBG4615 v2. The transmission rate of your NBG4615 v2 might be reduced. • 802.11 bgn: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the NBG4615 v2. The transmission rate of your NBG4615 v2 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 15.3 on page 142 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 and WPA2-PSK are available in this field.</p> <p>Note: If you select Static WEP, WPA, WPA-PSK or WPA2, the WPS features are not available on the NBG4615 v2.</p>
Apply	<p>Click Apply to save your changes back to the NBG4615 v2.</p>
Cancel	<p>Click Cancel to reload the previous configuration for this screen.</p>

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

15.3 Wireless Security

The screen varies depending on what you select in the **Security Mode** field.

15.3.1 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 NBG4615 v2, your network is accessible to any wireless networking device that is within range.

Figure 85 Network > Wireless LAN > General: No Security

The screenshot shows the 'General' tab of the 'Wireless LAN' configuration page. The 'Wireless Setup' section includes: 'Wireless LAN Status' set to 'OFF'; 'Name (SSID)' set to 'ZyXEL'; an unchecked 'Hide SSID' checkbox; 'Channel Selection' set to 'Channel-1 2412MHz' with 'Auto Channel Selection' checked; 'Operating Channel' set to 'Channel-'; 'Channel Width' set to 'Auto 20/40 MHz'; and '802.11 Mode' set to '802.11bgn'. The 'Security' section shows 'Security Mode' set to 'No Security'. A note at the bottom states: 'Note: No Security and WPA2-PSK can be configured when WPS enabled.' At the bottom are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 50 Network > Wireless LAN > General: 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 NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

15.3.2 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 NBG4615 v2 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 86 Network > Wireless LAN > General: Static WEP

Wireless Setup

Wireless LAN Status : OFF

Name (SSID) : ZyXEL

☐ Hide SSID

Channel Selection : Channel-1 2412MHz ☒ Auto Channel Selection

Operating Channel : Channel-

Channel Width : Auto 20/40 MHz

802.11 Mode : 802.11bgn

Security

Security Mode : Static WEP

PassPhrase : abcde

WEP Encryption : 64-bits

Authentication Method : Auto

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: 11111

☐ Key 2: 22222

☐ Key 3: 33333

☐ Key 4: 44444

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

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

Table 51 Network > Wireless LAN > General: 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 NBG4615 v2 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.

Table 51 Network > Wireless LAN > General: Static WEP (continued)

LABEL	DESCRIPTION
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 NBG4615 v2 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 NBG4615 v2 and the wireless stations must use the same WEP key for data transmission. If you chose 64-bits , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose 128-bits , 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 NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

15.3.3 WPA-PSK/WPA2-PSK

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

Figure 87 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

General | More AP | MAC Filter | Advanced | QoS | WPS | WPS Station | Scheduling

Wireless Setup

Wireless LAN Status : OFF

Name (SSID) : ZyXEL

☐ Hide SSID

Channel Selection : Channel-1 2412MHz ☒ Auto Channel Selection

Operating Channel : Channel-

Channel Width : Auto 20/40 MHz

802.11 Mode : 802.11bgn

Security

Security Mode : WPA2-PSK

☒ WPA-PSK Compatible

Pre-Shared Key : 9R7KV4ECYF9VA

Group Key Update Timer : 3600 seconds

☐ Note: No Security and WPA2-PSK can be configured when WPS enabled.

Apply Cancel

The following table describes the labels in this screen.

Table 52 Network > Wireless LAN > General: 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 NBG4615 v2.
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 NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

15.3.4 WPA/WPA2

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

Note: WPA or WPA2 is not available if you enable WPS before you configure WPA or WPA2 in the **Wireless LAN > General** screen.

Figure 88 Network > Wireless LAN > General: WPA/WPA2

General | More AP | MAC Filter | Advanced | QoS | WPS | WPS Station | Scheduling

Wireless Setup

Wireless LAN Status : OFF

Name (SSID) : ZyXEL

☐ Hide SSID

Channel Selection : Channel-1 2412MHz ☒ Auto Channel Selection

Operating Channel : Channel-

Channel Width : Auto 20/40 MHz

802.11 Mode : 802.11bgn

Security

Security Mode : WPA2

☐ WPA Compatible

Group Key Update Timer : 3600 seconds

PMK Cache Period : 10 minutes

Pre-Authentication : ☐ Enable ☒ Disable

Authentication Server

IP Address : 192.168.2.3

Port Number : 1812

Shared Secret : 12345678

Session Timeout(0 or 60~) : 0 seconds

☐ Note: No Security and WPA2-PSK can be configured when WPS enabled.

Apply Cancel

The following table describes the labels in this screen.

Table 53 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 NBG4615 v2 even when the NBG4615 v2 is using WPA2-PSK or WPA2.
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.

Table 53 Network > Wireless LAN > General: WPA/WPA2 (continued)

LABEL	DESCRIPTION
PMK Cache Period	<p>This field is available only when you select WPA2.</p> <p>Specify how often wireless clients have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 999999 minutes.</p> <p>Note: If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.</p>
Pre-Authentication	<p>This field is available only when you select WPA2.</p> <p>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.</p>
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	<p>Enter the port number of the external authentication server.</p> <p>You need not change this value unless your network administrator instructs you to do so with additional information.</p>
Shared Secret	<p>Enter a password (up to 127 alphanumeric characters) as the key to be shared between the external authentication server and the NBG4615 v2.</p> <p>The key must be the same on the external authentication server and your NBG4615 v2. The key is not sent over the network.</p>
Session Timeout	<p>The NBG4615 v2 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.</p> <p>Enter the time in seconds from 0 to 999999.</p>
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

15.4 More AP Screen

This screen allows you to enable and configure multiple wireless networks and guest wireless network settings on the NBG4615 v2.

You can configure up to four SSIDs to enable multiple BSSs (Basic Service Sets) on the NBG4615 v2. This allows you to use one access point to provide several BSSs simultaneously. You can then assign varying security types to different SSIDs. Wireless clients can use different SSIDs to associate with the same access point.

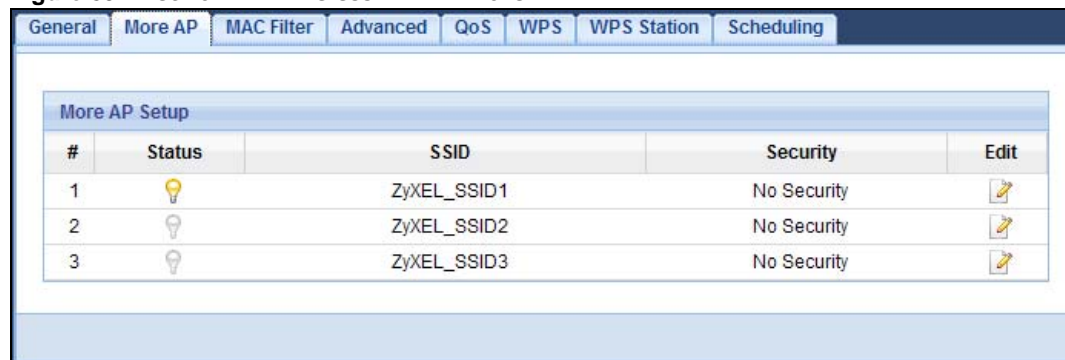
Table 54 Multiple SSIDs and Modes

MODE	MULTIPLE SSIDS
Router Mode	Yes
Access Point Mode	Yes
Universal Repeater Mode	Yes

Table 54 Multiple SSIDs and Modes

MODE	MULTIPLE SSIDS
WISP	No
WISP + Universal Repeater Mode	Yes

Click **Network > Wireless LAN > More AP**. The following screen displays.

Figure 89 Network > Wireless LAN > More AP

The following table describes the labels in this screen.

Table 55 Network > Wireless LAN > More AP

LABEL	DESCRIPTION
#	This is the index number of each SSID profile.
Status	This shows whether the SSID profile is active (a yellow bulb) or not (a gray bulb).
SSID	An SSID profile is the set of parameters relating to one of the NBG4615 v2's BSSs. The SSID (Service Set Identifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Edit	Click the Edit icon to configure the SSID profile.

15.4.1 More AP Edit

Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **More AP** screen. The following screen displays.

Figure 90 Network > Wireless LAN > More AP: Edit

Wireless Setup

Active : ☐

Name (SSID) :

☐ Hide SSID

☒ Intra-BSS Traffic

☒ WMM QoS

Security

Security Mode :

No Security, WPA-PSK and WPA2-PSK can be configured when WPS enabled.

Figure 91 Network > Wireless LAN > More AP: Edit (the last SSID)

Wireless Setup

Active : ☐

Name (SSID) :

☐ Hide SSID

☒ Intra-BSS Traffic

☒ WMM QoS

☒ Enable Guest WLAN

IP Address :

IP Subnet Mask :

☐ Enable Bandwidth Management for Guest WLAN

Maximum Bandwidth (kbps)

Security

Security Mode :

No Security and WPA2-PSK can be configured when WPS enabled.

The following table describes the labels in this screen.

Table 56 Network > Wireless LAN > More AP: Edit

LABEL	DESCRIPTION
Active	Select this to activate the SSID profile.
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.

Table 56 Network > Wireless LAN > More AP: Edit (continued)

LABEL	DESCRIPTION
Intra-BSS Traffic	<p>A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).</p> <p>Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless 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.</p>
WMM QoS	<p>Check this to have the NBG4615 v2 automatically give a service a priority level according to the ToS value in the IP header of packets it sends.</p> <p>WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.</p>
Enable Guest WLAN	<p>Select the check box to activate guest wireless LAN. This is available only for the last SSID on the NBG4615 v2.</p> <p>Note: Only Router mode supports guest WLAN. AP mode, Universal Repeater mode, WISP mode and WISP + Universal Repeater mode don't support guest WLAN.</p>
IP Address	Type an IP address for the devices on the Guest WLAN using this as the gateway IP address.
IP Subnet Mask	Type the subnet mask for the guest wireless LAN.
Enable Bandwidth Management for Guest WLAN	Select this to turn on bandwidth management for the Guest WLAN network.
Maximum Bandwidth	Enter a number to specify maximum bandwidth the Guest WLAN network can use.
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 15.3 on page 142 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 and WPA2-PSK are available in this field.</p>
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

15.5 MAC Filter Screen

The MAC filter screen allows you to configure the NBG4615 v2 to give exclusive access to devices (**Allow**) or exclude devices from accessing the NBG4615 v2 (**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 NBG4615 v2's MAC filter settings, click **Network > Wireless LAN > MAC Filter**. The screen appears as shown.

Figure 92 Network > Wireless LAN > MAC Filter

General More AP **MAC Filter** Advanced QoS WPS WPS Station Scheduling

SSID Select : ZyXELCCDD10

MAC Address Filter : ☐ Enable ☒ Disable

Filter Action : ☒ Allow ☐ Deny

MAC Filter Summary			
Set	MAC Address	Set	MAC Address
1	00:00:00:00:00:00	17	00:00:00:00:00:00
2	00:00:00:00:00:00	18	00:00:00:00:00:00
3	00:00:00:00:00:00	19	00:00:00:00:00:00
4	00:00:00:00:00:00	20	00:00:00:00:00:00
5	00:00:00:00:00:00	21	00:00:00:00:00:00
6	00:00:00:00:00:00	22	00:00:00:00:00:00
7	00:00:00:00:00:00	23	00:00:00:00:00:00
8	00:00:00:00:00:00	24	00:00:00:00:00:00
9	00:00:00:00:00:00	25	00:00:00:00:00:00
10	00:00:00:00:00:00	26	00:00:00:00:00:00
11	00:00:00:00:00:00	27	00:00:00:00:00:00
12	00:00:00:00:00:00	28	00:00:00:00:00:00
13	00:00:00:00:00:00	29	00:00:00:00:00:00
14	00:00:00:00:00:00	30	00:00:00:00:00:00
15	00:00:00:00:00:00	31	00:00:00:00:00:00
16	00:00:00:00:00:00	32	00:00:00:00:00:00

Apply Cancel

The following table describes the labels in this menu.

Table 57 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
SSID Select	Select the SSID for which you want to configure MAC filtering.
MAC Address Filter	Select to turn on (Enable) or off (Disable) MAC address filtering.
Filter Action	<p>Define the filter action for the list of MAC addresses in the MAC Filter Summary table.</p> <p>Select Allow to permit access to the NBG4615 v2, MAC addresses not listed will be denied access to the NBG4615 v2.</p> <p>Select Deny to block access to the NBG4615 v2, MAC addresses not listed will be allowed to access the NBG4615 v2.</p>
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 NBG4615 v2.
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

15.6 Wireless LAN Advanced Screen

Use this screen to allow wireless advanced features, such as the output power, RTS/CTS Threshold settings.

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

Figure 93 Network > Wireless LAN > Advanced

The following table describes the labels in this screen.

Table 58 Network > Wireless LAN > Advanced

LABEL	DESCRIPTION
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. This field is not configurable and the NBG4615 v2 automatically changes to use the maximum value if you select 802.11n , 802.11gn or 802.11bgn in the Wireless LAN > General screen.
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. This field is not configurable and the NBG4615 v2 automatically changes to use the maximum value if you select 802.11n , 802.11gn or 802.11bgn in the Wireless LAN > General screen.
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.
Tx Power	Set the output power of the NBG4615 v2 in this field. If there is a high density of APs in an area, decrease the output power of the NBG4615 v2 to reduce interference with other APs. Select one of the following 100% , 90% , 75% , 50% , 25% or 10% .
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

15.7 Quality of Service (QoS) Screen

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

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

Figure 94 Network > Wireless LAN > QoS

The following table describes the labels in this screen.

Table 59 Network > Wireless LAN > QoS

LABEL	DESCRIPTION
WMM QoS	<p>Select Enable to have the NBG4615 v2 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.</p> <p>This field is not configurable and the NBG4615 v2 automatically enables WMM QoS if you select 802.11n, 802.11gn or 802.11bgn in the Wireless LAN > General screen.</p>
Apply	Click Apply to save your changes to the NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

15.8 WPS Screen

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

Note: With WPS, wireless clients can only connect to the wireless network using the first SSID on the NBG4615 v2.

Figure 95 Network > Wireless LAN > WPS

WPS Setup

WPS : ☒ Enable ☐ Disable

PIN Code : ☒ Enable ☐ Disable

PIN Number :

WPS Status

Status : Unconfigured

802.11 Mode :

SSID :

Security :

Note:
If you enable WPS, the UPnP service will be turned on automatically.

The following table describes the labels in this screen.

Table 60 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
WPS Setup	
WPS	Select Enable to turn on the WPS feature. Otherwise, select Disable .
PIN Code	Select Enable and click Apply to allow the PIN Configuration method. If you select Disable , you cannot create a new PIN number.
PIN Number	This is the WPS PIN (Personal Identification Number) of the NBG4615 v2. Enter this PIN in the configuration utility of the device you want to connect to the NBG4615 v2 using WPS. The PIN is not necessary when you use WPS push-button method. Click Generate to generate a new PIN number.
WPS Status	
Status	This displays Configured when the NBG4615 v2 has connected to a wireless network using WPS or when WPS Enable 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 NBG4615 v2 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 NBG4615 v2.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the NBG4615 v2.
SSID	This is the name of the wireless network (the NBG4615 v2's first SSID).
Security	This is the type of wireless security employed by the network.

Table 60 Network > Wireless LAN > WPS (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

15.9 WPS Station Screen

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

Note: 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 96 Network > Wireless LAN > WPS Station

The following table describes the labels in this screen.

Table 61 Network > Wireless LAN > WPS Station

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

15.10 Scheduling Screen

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

Figure 97 Network > Wireless LAN > Scheduling

GeneralMore APMAC FilterAdvancedQoSWPSPS StationScheduling

Wireless LAN Scheduling :

☒ Enable☐ Disable

Scheduling

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

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

ApplyCancel

The following table describes the labels in this screen.

Table 62 Network > Wireless LAN > Scheduling

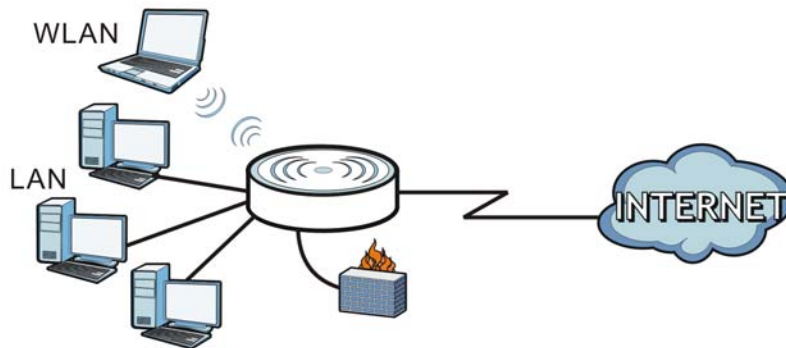
LABEL	DESCRIPTION
Wireless LAN Scheduling	
Wireless LAN Scheduling	Select Enable to activate the wireless LAN scheduling feature. Select Disable to turn it off.
Scheduling	
WLAN Status	Select On or Off to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the Day and For the following times fields.
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.
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 NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

16.1 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 98 LAN Example



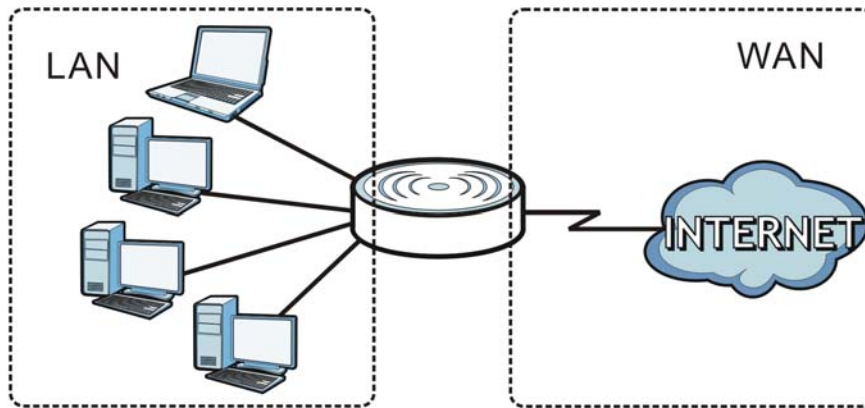
The LAN screens can help you manage IP addresses.

16.2 What You Can Do

- Use the **IP** screen to change the IP address for your ([Section 16.4 on page 158](#)).
- Use the **IP Alias** screen to have the NBG4615 v2 apply IP alias to create LAN subnets ([Section 16.5 on page 159](#)).

16.3 What You Need To Know

The actual physical connection determines whether the NBG4615 v2 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 99 LAN and WAN IP Addresses

The LAN parameters of the NBG4615 v2 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.

16.3.1 IP Pool Setup

The NBG4615 v2 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 NBG4615 v2 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.

16.3.2 LAN TCP/IP

The NBG4615 v2 has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

16.3.3 IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The NBG4615 v2 supports three logical LAN interfaces via its single physical Ethernet interface with the NBG4615 v2 itself as the gateway for each LAN network.

16.4 LAN IP Screen

Use this screen to change the IP address for your NBG4615 v2. Click **Network > LAN > IP**.

Figure 100 Network > LAN > IP

The following table describes the labels in this screen.

Table 63 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your NBG4615 v2 in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG4615 v2 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 NBG4615 v2.
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

16.5 IP Alias Screen

Use this screen to have the NBG4615 v2 apply IP alias to create LAN subnets. Click **LAN > IP Alias**.

Figure 101 Network > LAN > IP Alias

The following table describes the labels in this screen.

Table 64 Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias 1, 2	Check this to enable IP alias to configure another LAN network for the NBG4615 v2.
IP Address	Type the IP alias address of your NBG4615 v2 in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG4615 v2 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 NBG4615 v2.
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

DHCP Server

17.1 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 NBG4615 v2's LAN as a DHCP server or disable it. When configured as a server, the NBG4615 v2 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.

17.1.1 What You Can Do

- Use the **General** screen to enable the DHCP server ([Section 17.2 on page 161](#)).
- Use the **Advanced** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses ([Section 17.3 on page 162](#)).
- Use the **Client List** screen to view the current DHCP client information ([Section 17.4 on page 164](#)).

17.1.2 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.

17.2 DHCP Server General Screen

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

Figure 102 Network > DHCP Server > General

The screenshot shows the 'General' tab of the DHCP Server configuration. The 'DHCP Server' option is set to 'Enable'. The 'IP Pool Starting Address' is '192.168.1.33' and the 'Pool Size' is '32'. The 'Apply' and 'Cancel' buttons are at the bottom right.

The following table describes the labels in this screen.

Table 65 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 NBG4615 v2 acting as a DHCP server. When configured as a server, the NBG4615 v2 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 NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

17.3 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 NBG4615 v2 sends to the DHCP clients.

To change your NBG4615 v2's static DHCP settings, click **Network > DHCP Server > Advanced**. The following screen displays.

Figure 103 Network > DHCP Server > Advanced

Static DHCP Table

#	MAC Address	IP Address
1	00:00:00:00:00:00	0.0.0.0
2	00:00:00:00:00:00	0.0.0.0
3	00:00:00:00:00:00	0.0.0.0
4	00:00:00:00:00:00	0.0.0.0
5	00:00:00:00:00:00	0.0.0.0
6	00:00:00:00:00:00	0.0.0.0
7	00:00:00:00:00:00	0.0.0.0
8	00:00:00:00:00:00	0.0.0.0

DNS Server

DNS Servers Assigned by DHCP Server

First DNS Server :

Second DNS Server :

Third DNS Server :

The following table describes the labels in this screen.

Table 66 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 NBG4615 v2 passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The NBG4615 v2 only passes this information to the LAN DHCP clients when you enable DHCP Server . When you disable DHCP Server , DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.

Table 66 Network > DHCP Server > Advanced (continued)

LABEL	DESCRIPTION
First DNS Server	<p>Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the NBG4615 v2's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you click Apply.</p> <p>Select DNS Relay to have the NBG4615 v2 act as a DNS proxy. The NBG4615 v2's LAN IP address displays in the field to the right (read-only). The NBG4615 v2 tells the DHCP clients on the LAN that the NBG4615 v2 itself is the DNS server. When a computer on the LAN sends a DNS query to the NBG4615 v2, the NBG4615 v2 forwards the query to the NBG4615 v2's system DNS server (configured in the WAN > Internet Connection screen) and relays the response back to the computer. You can only select DNS Relay for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
Second DNS Server	
Third DNS Server	
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

17.4 DHCP Client List Screen

The DHCP table shows current DHCP client information (including IP Address, Host Name and MAC Address) of network clients using the NBG4615 v2'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 **Monitor > DHCP Server**.

Figure 104 Network > DHCP Server > Client List

#	Status	Host Name	IP Address	MAC Address	Reserve
1		twpc	192.168.1.46	00:21:85:0c:44:4b	<input type="checkbox"/>

The following table describes the labels in this screen.

Table 67 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).

Table 67 Network > DHCP Server > Client List (continued)

LABEL	DESCRIPTION
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	<p>This field shows the MAC address of the computer with the name in the Host Name field.</p> <p>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.</p>
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 NBG4615 v2.
Cancel	Click Cancel to reload the previous configuration for this screen.

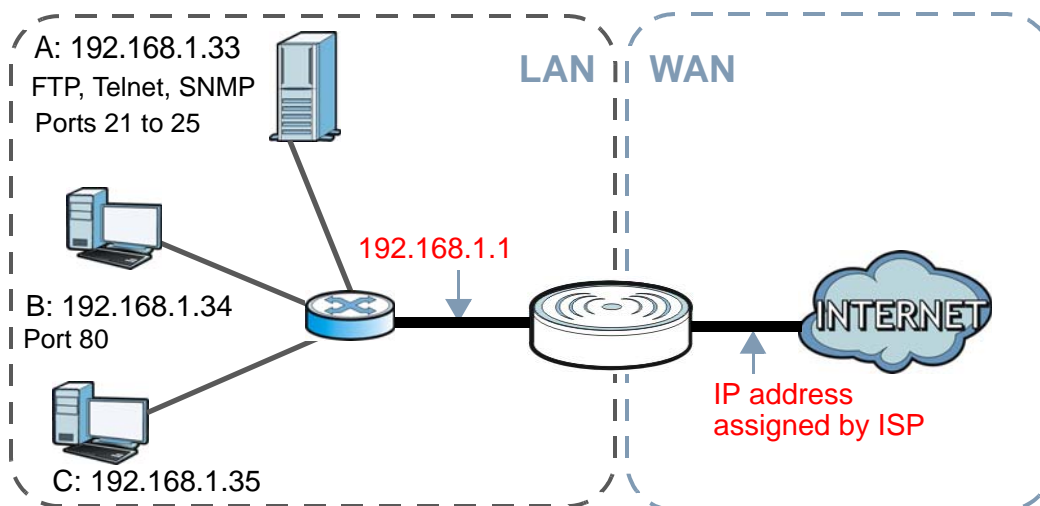
18.1 Overview

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 NBG4615 v2. 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 NBG4615 v2, which is 192.168.1.1.

Figure 105 NAT Example



This chapter discusses how to configure NAT on the NBG4615 v2.

Note: You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the NBG4615 v2.

18.1.1 What You Can Do

- Use the **General** screen to enable NAT ([Section 18.2 on page 169](#)).

- Use the **Port Forwarding** screen to set a default server and change your NBG4615 v2's port forwarding settings to forward incoming service requests to the server(s) on your local network ([Section 18.3 on page 170](#)).
- Use the **Port Trigger** screen to change your NBG4615 v2's trigger port settings ([Section 18.5.3 on page 175](#)).

18.1.2 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 NBG4615 v2, 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 68 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.

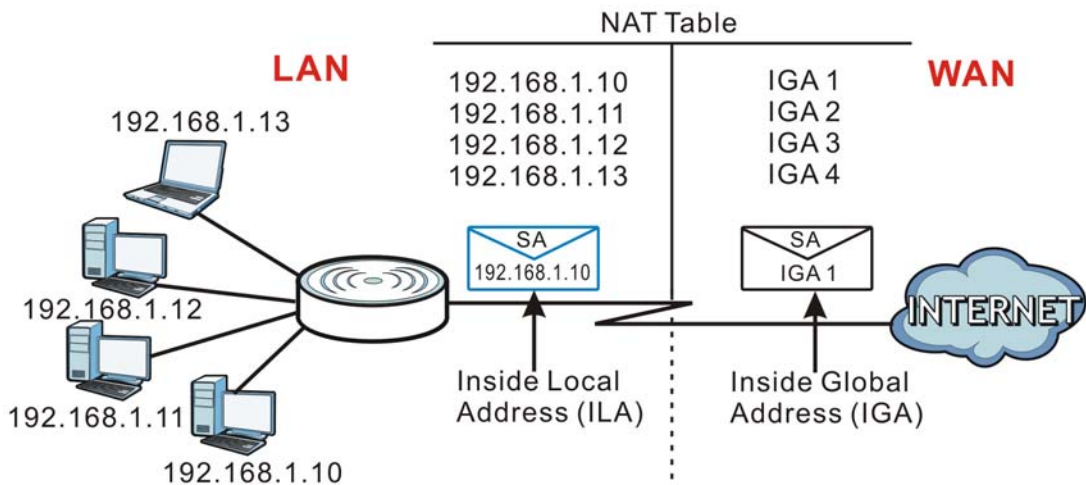
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local

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 NBG4615 v2 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 NBG4615 v2 keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

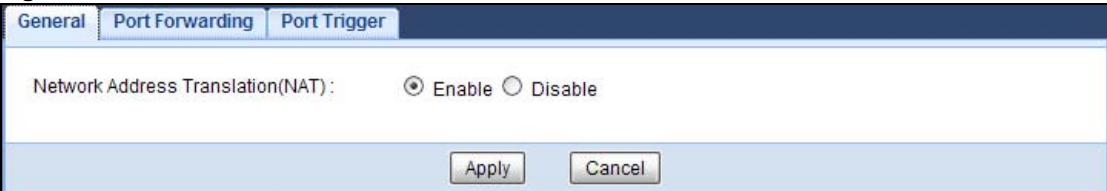
Figure 106 How NAT Works



18.2 General

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

Figure 107 Network > NAT > General



The following table describes the labels in this screen.

Table 69 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.
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

18.3 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 NBG4615 v2's port forwarding settings, click **Network > NAT > Port Forwarding**. The screen appears as shown.

Note: If you do not assign a **Default Server**, the NBG4615 v2 discards all packets received for ports that are not specified in this screen or remote management.

Refer to [Appendix E on page 293](#) for port numbers commonly used for particular services.

Figure 108 Network > NAT > Port Forwarding

The following table describes the labels in this screen.

Table 70 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.
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 table. 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 table.
#	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 Delete icon to remove a rule.

Table 70 Network > NAT > Port Forwarding (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

18.3.1 Port Forwarding Edit Screen

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

Figure 109 Network > NAT > Port Forwarding Edit

The following table describes the labels in this screen.

Table 71 Network > 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-.
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 NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

18.4 Port Trigger Screen

To change your NBG4615 v2's trigger port settings, click **Network > NAT > Port Trigger**. The screen appears as shown.

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

Figure 110 Network > NAT > Port Trigger

#	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 72 Network > NAT > Port Trigger

LABEL	DESCRIPTION
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The NBG4615 v2 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 NBG4615 v2 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 NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

18.5 Technical Reference

The following section contains additional technical information about the NBG4615 v2 features described in this chapter.

18.5.1 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 **Port Forwarding** 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.

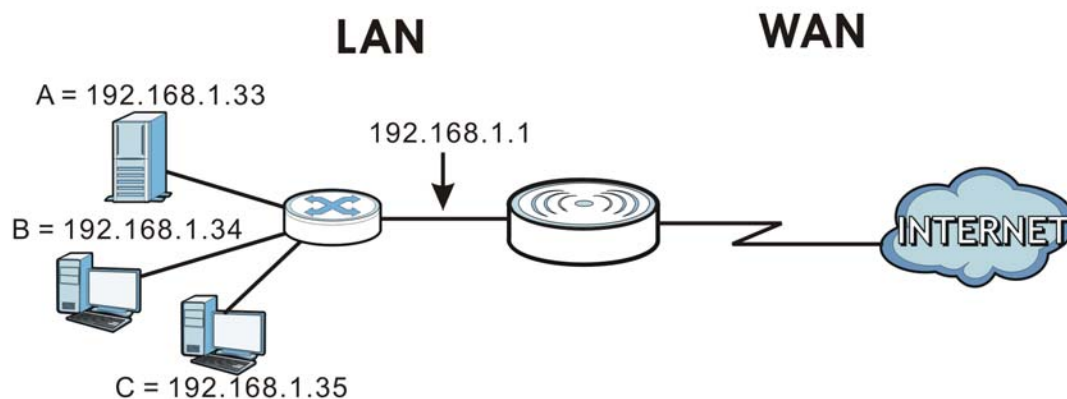
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

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.

18.5.2 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 111 Multiple Servers Behind NAT Example



18.5.3 Trigger Port Forwarding

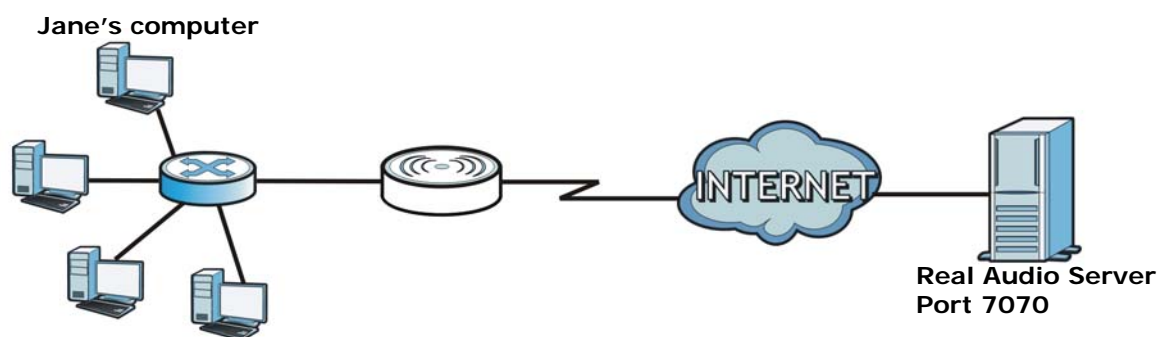
Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem 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 NBG4615 v2 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 NBG4615 v2's WAN port receives a response with a specific port number and protocol ("incoming" port), the NBG4615 v2 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.

18.5.4 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 112 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 NBG4615 v2 to record Jane's computer IP address. The NBG4615 v2 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 NBG4615 v2 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 NBG4615 v2 times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

18.5.5 Two Points To Remember About Trigger Ports

- 1 Trigger events only happen on data that is going coming from inside the NBG4615 v2 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.

19.1 Overview

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

19.1.1 What You Need To Know

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

What is DDNS?

Dynamic Domain Name Service (DDNS) services let you use a fixed domain name with a dynamic IP address. Users can always use the same domain name instead of a different dynamic IP address that changes each time to connect to the NBG4615 v2 or a server in your network.

Note: The NBG4615 v2 must have a public global IP address and you should have your registered DDNS account information on hand.

19.2 General

To change your NBG4615 v2's DDNS, click **Network > DDNS**. The screen appears as shown.

Figure 113 Dynamic DNS



The screenshot shows the 'Dynamic DNS' configuration window. At the top, there is a tab labeled 'Dynamic DNS'. Below it, the section is titled 'Dynamic DNS Setup'. The 'Dynamic DNS' checkbox is currently unchecked, with 'Enable' and 'Disable' radio buttons. The 'Service Provider' dropdown menu is set to 'www.DynDNS.org'. Below this, there are four input fields for 'Host Name', 'Username', and 'Password', each followed by a small downward arrow icon. At the bottom of the window, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 73 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 NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

Static Route

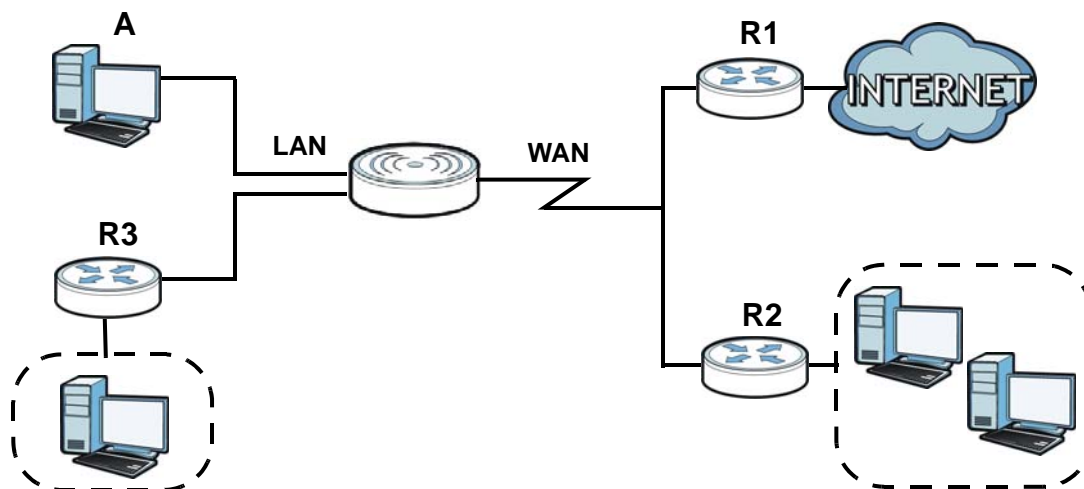
20.1 Overview

This chapter shows you how to configure static routes for your NBG4615 v2.

The NBG4615 v2 usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the NBG4615 v2 send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the NBG4615 v2's LAN interface. The NBG4615 v2 routes most traffic from **A** to the Internet through the NBG4615 v2's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 114 Example of Static Routing Topology



20.2 IP Static Route Screen

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

Figure 115 Network > Static Route

Static Route

Add Static Route

#	Status	Name	Destination	Gateway	Subnet Mask	Modify
1	On	example	10.1.2.3	10.1.2.86	255.255.255.0	Edit Delete

The following table describes the labels in this screen.

Table 74 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.
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.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Modify	Click the Edit icon to open a screen where you can modify an existing rule. Click the Delete icon to remove a rule from the NBG4615 v2.
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

20.2.1 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 116 Network > Static Route: Add/Edit

Static Route : ☐ Enable ☒ Disable

Route Name :

Destination IP Address :

IP Subnet Mask :

Gateway IP Address :

Back Apply Cancel

The following table describes the labels in this screen.

Table 75 Network > 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 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 NBG4615 v2's interface(s). The gateway helps forward packets to their destinations.
Back	Click Back to return to the previous screen without saving.
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to set every field in this screen to its last-saved value.

Firewall

21.1 Overview

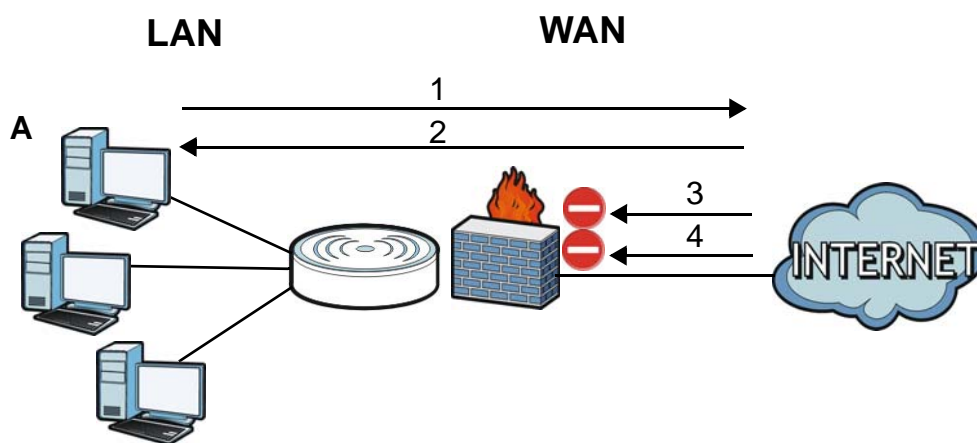
Use these screens to enable and configure the firewall that protects your NBG4615 v2 and your LAN from unwanted or malicious traffic.

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 117 Default Firewall Action



21.1.1 What You Can Do

- Use the **General** screen to enable or disable the NBG4615 v2's firewall ([Section 21.2 on page 185](#)).
- 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 21.3 on page 185](#)).

21.1.2 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 NBG4615 v2 Firewall

The NBG4615 v2'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 NBG4615 v2's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG4615 v2 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 NBG4615 v2 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 NBG4615 v2 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

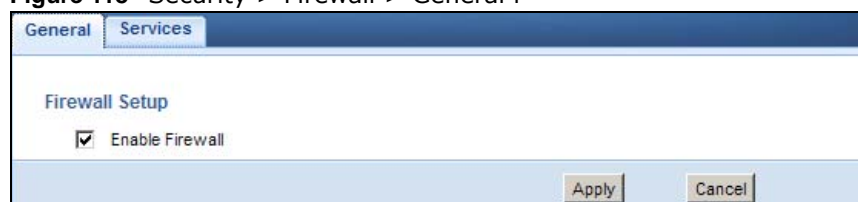
- 1 Change the default password via Web Configurator.
- 2 Think about access control before you connect to the network in any way, including attaching a modem to the port.
- 3 Limit who can access your router.

- 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.

21.2 General Screen

Use this screen to enable or disable the NBG4615 v2's firewall, and set up firewall logs. Click **Security** > **Firewall** to open the **General** screen.

Figure 118 Security > Firewall > General I



The following table describes the labels in this screen.

Table 76 Security > Firewall > General

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The NBG4615 v2 performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Apply	Click Apply to save the settings.
Cancel	Click Cancel to start configuring this screen again.

21.3 Services Screen

If an outside user attempts to probe an unsupported port on your NBG4615 v2, an ICMP response packet is automatically returned. This allows the outside user to know the NBG4615 v2 exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your NBG4615 v2 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 119 Security > Firewall > Services I

General

Services

ICMP

Respond to Ping on:

Disable

Apply

Enable Firewall Rule

☒ Enable Firewall Rule

Apply

Add Firewall Rule

Service Name :

MAC Address :

Dest IP Address :

Source IP Address :

Protocol :

TCP

DestPortRange :

SourcePortRange :

Add Rule

Firewall Rule

#	ServiceName	MACaddresse	DestIP	SourceIP	Protocol	DestPortRange	SourcePortRange	Action	Delete
1	test	AA:BB:AA:BB:AA:BB	192.168.1.88	10.1.2.3	TCP	-	-	DROP	

Cancel

The following table describes the labels in this screen.

Table 77 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 NBG4615 v2 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 NBG4615 v2 applies the firewall rule to traffic initiating from this computer.

Table 77 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 NBG4615 v2 applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol (TCP , UDP or ICMP) 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 (TCP , UDP or ICMP) 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.
Cancel	Click Cancel to start configuring this screen again.

See [Appendix E on page 293](#) for commonly used services and port numbers.

Content Filtering

22.1 Overview

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

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

22.1.1 What You Need To Know

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

Content Filtering Profiles

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

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

Keyword Blocking URL Checking

The NBG4615 v2 checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

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

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

Since the NBG4615 v2 checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the NBG4615 v2 would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path (news/pressroom.php) but it would not find "tw/news".

22.2 Content Filter

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

Figure 120 Security > Content Filter

Content Filter

Trusted IP Setup
A trusted computer has full access to all blocked resources. 0.0.0.0 means there is no trusted computer.
Trusted Computer IP Address:

Restrict Web Features
☐ ActiveX ☐ Java ☐ Cookies ☐ Web Proxy

Keyword Blocking
☐ Enable URL Keyword Blocking
 Keyword
 Keyword List

The following table describes the labels in this screen.

Table 78 Security > Content Filter

LABEL	DESCRIPTION
Trusted IP Setup	To enable this feature, type an IP address of any one of the computers in your network that you want to have as a trusted computer. This allows the trusted computer to have full access to all features that are configured to be blocked by content filtering. Leave this field blank to have no trusted computers.
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	The NBG4615 v2 can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL http://www.website.com/bad.html would be blocked. Select this check box to enable this feature.
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Add	Click Add after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.

Table 78 Security > Content Filter (continued)

LABEL	DESCRIPTION
Keyword List	This list displays the keywords already added.
Delete	Highlight a keyword in the lower box and click Delete to remove it. The keyword disappears from the text box after you click Apply .
Clear All	Click this button to remove all of the listed keywords.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to begin configuring this screen afresh

22.3 Technical Reference

The following section contains additional technical information about the NBG4615 v2 features described in this chapter.

22.3.1 Customizing Keyword Blocking URL Checking

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

Domain Name or IP Address URL Checking

By default, the NBG4615 v2 checks the URL's domain name or IP address when performing keyword blocking.

This means that the NBG4615 v2 checks the characters that come before the first slash in the URL.

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

Full Path URL Checking

Full path URL checking has the NBG4615 v2 check the characters that come before the last slash in the URL.

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

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

File Name URL Checking

Filename URL checking has the NBG4615 v2 check all of the characters in the URL.

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

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

Bandwidth Management

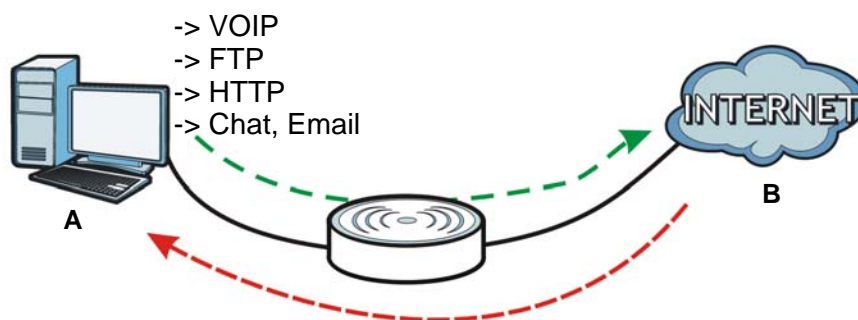
23.1 Overview

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 121 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).

23.2 What You Can Do

- Use the **General** screen to enable bandwidth management and assign bandwidth values ([Section 23.4 on page 194](#)).
- Use the **Advanced** screen to configure bandwidth managements rule for the pre-defined services and applications ([Section 23.5 on page 194](#)).

23.3 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 23.5 on page 194](#)).

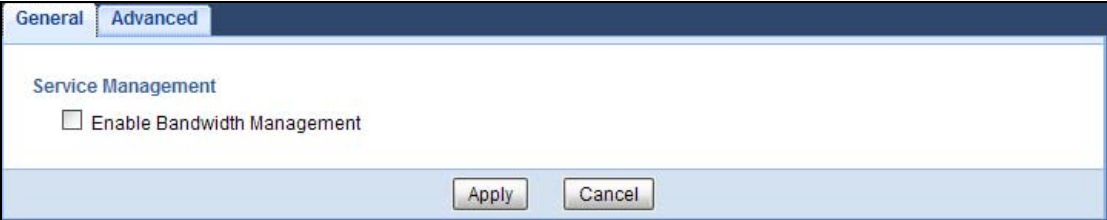
The sum of the bandwidth allotments that apply to the LAN interface (WAN to LAN, WAN to WLAN) must be less than or equal to the **Downstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen [Section 23.5 on page 194](#).

23.4 General Screen

Use this screen to have the NBG4615 v2 apply bandwidth management.

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

Figure 122 Management > Bandwidth Management > General



The following table describes the labels in this screen.

Table 79 Management > Bandwidth Management > General

LABEL	DESCRIPTION
Enable Bandwidth Management	This field allows you to have NBG4615 v2 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.
Cancel	Click Cancel to begin configuring this screen afresh.

23.5 Advanced Screen

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

You can also use this screen to configure bandwidth management rule for other services or applications that are not on the pre-defined list of NBG4615 v2. 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 > Advanced** to open the bandwidth management **Advanced** screen.

Figure 123 Management > Bandwidth Management > Advanced

General

Advanced

Management Bandwidth

Upstream Bandwidth

10000

(Kbps)

User Defined

Downstream Bandwidth
(Kbps)

User Defined

Application List

#	Priority	Category	Service	
1	High	Game Console	<input type="checkbox"/> Xbox Live	
			<input type="checkbox"/> PlayStation	
			<input type="checkbox"/> MSN Game Zone	
			<input type="checkbox"/> Battlenet	
2	High	VoIP	<input type="checkbox"/> VoIP	
3	High	Instant Messenger	<input type="checkbox"/> Instant Messenger	
4	High	Web Surfing	<input type="checkbox"/> Web Surfing	
5	High	P2P/FTP	<input type="checkbox"/> FTP	
			<input type="checkbox"/> eMule	
			<input type="checkbox"/> BitTorrent	
6	High	E-Mail	<input type="checkbox"/> E-Mail	

User-defined Service

#	Enable	Direction	Service Name	Category	Modify
1	<input type="checkbox"/>	To LAN&WLAN		Game Console	
2	<input type="checkbox"/>	To LAN&WLAN		Game Console	
3	<input type="checkbox"/>	To LAN&WLAN		Game Console	
4	<input type="checkbox"/>	To LAN&WLAN		Game Console	
5	<input type="checkbox"/>	To LAN&WLAN		Game Console	
6	<input type="checkbox"/>	To LAN&WLAN		Game Console	
7	<input type="checkbox"/>	To LAN&WLAN		Game Console	
8	<input type="checkbox"/>	To LAN&WLAN		Game Console	

Apply

Cancel

The following table describes the labels in this screen.

Table 80 Management > Bandwidth Management > Advanced

LABEL	DESCRIPTION
Management Bandwidth	
Upstream Bandwidth	<p>Select the total amount of bandwidth from a drop-down list box that you want to dedicate to uplink traffic. Otherwise, select User Defined and manually specify the amount of bandwidth in kilobits per second.</p> <p>This is traffic from LAN/WLAN to WAN.</p>
Downstream Bandwidth	<p>Select the total amount of bandwidth from a drop-down list box that you want to dedicate to uplink traffic. Otherwise, select User Defined and manually specify the amount of bandwidth in kilobits per second.</p> <p>This is traffic from WAN to LAN/WLAN.</p>
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.
Priority	<p>Select a priority from the drop down list box. Choose High, Mid or Low.</p> <ul style="list-style-type: none"> • High - Select this for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay). • Mid - Select this for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay. • Low - Select this 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	<p>This is the name of the service.</p> <p>Select the check box to have the NBG4615 v2 apply this bandwidth management rule.</p>
	Click the Edit icon to open the Rule Configuration screen where you can modify the rule.
User-defined Service	Use this table to allocate specific amounts of bandwidth to specific applications or services you specify.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the NBG4615 v2 apply this bandwidth management rule.
Direction	<p>Select To LAN&WLAN to apply bandwidth management to traffic from WAN to LAN and WLAN.</p> <p>Select To WAN to apply bandwidth management to traffic from LAN/WLAN to WAN.</p>
Service Name	Enter a descriptive name for the bandwidth management rule.
Category	This is the category where a service belongs.
Modify	<p>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 23.5.2 on page 197 for more information.</p> <p>Click the Remove icon to delete a rule.</p>
Apply	Click Apply to save your customized settings.
Cancel	Click Cancel to begin configuring this screen afresh.

23.5.1 Rule Configuration: Application Rule Configuration

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

Figure 124 Bandwidth Management Rule Configuration: Application List

#	Enable	Direction	Bandwidth	Destination Port	Source Port	Protocol
1	<input checked="" type="checkbox"/>	LAN	Minimum Bandwidth 50 (kbps)	-	-	TCP
2	<input checked="" type="checkbox"/>	LAN	Minimum Bandwidth 50 (kbps)	-	-	UDP
3	<input checked="" type="checkbox"/>	WAN	Minimum Bandwidth 10 (kbps)	-	-	TCP
4	<input checked="" type="checkbox"/>	WAN	Minimum Bandwidth 10 (kbps)	-	-	UDP

The following table describes the labels in this screen.

Table 81 Bandwidth Management Rule Configuration: Application List

LABEL	DESCRIPTION
#	This is the number of an individual bandwidth management rule.
Enable	Select an interface's check box to enable bandwidth management on that interface.
Direction	These read-only labels represent the physical interfaces. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source. Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the NBG4615 v2 and be managed by bandwidth management.
Bandwidth	Select Maximum Bandwidth or Minimum Bandwidth and specify the maximum or minimum bandwidth allowed for the rule in kilobits per second.
Destination Port	This is the port number of the destination that define the traffic type, for example TCP port 80 defines web traffic. See Appendix E on page 293 for some common services and port numbers.
Source Port	This is the port number of the source that define the traffic type, for example TCP port 80 defines web traffic. See Appendix E on page 293 for some common services and port numbers.
Protocol	This is the protocol (TCP , UDP or user-defined) used for the service.
Apply	Click Apply to save your customized settings.
Cancel	Click Cancel to exit this screen without saving.

23.5.2 Rule Configuration: User Defined Service Rule Configuration

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

Figure 125 Bandwidth Management Rule Configuration: User-defined Service

General Advanced

Rule Configuration> -

BW Budget Minimum Bandwidth ▼ 10 (kbps)

Destination Address Start 0.0.0.0

Destination Address End 0.0.0.0

Destination Port 0

Source Address Start 0.0.0.0

Source Address End 0.0.0.0

Source Port 0

Protocol TCP ▼

Apply Cancel

The following table describes the labels in this screen.

Table 82 Bandwidth Management Rule Configuration: User-defined Service

LABEL	DESCRIPTION
BW Budget	Select Maximum Bandwidth or Minimum Bandwidth and specify the maximum or minimum bandwidth allowed for the rule in kilobits per second.
Destination Address Start	Enter the starting IP address of the destination computer. The NBG4615 v2 applies bandwidth management to the service or application that is entering this computer.
Destination Address End	Enter the ending IP address of the destination computer. The NBG4615 v2 applies bandwidth management to the service or application that is entering this computer.
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 Start	Enter the starting IP address of the computer that initializes traffic for the application or service. The NBG4615 v2 applies bandwidth management to traffic initiating from this computer.
Source Address End	Enter the ending IP address of the computer that initializes traffic for the application or service. The NBG4615 v2 applies bandwidth management to traffic initiating from this computer.
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 , BOTH) for which the bandwidth management rule applies. If you select BOTH , enter the protocol for which the bandwidth management rule applies. For example, ICMP for ping traffic.
Apply	Click Apply to save your customized settings.
Cancel	Click Cancel to exit this screen without saving.

See [Appendix E on page 293](#) for commonly used services and port numbers.

23.5.3 Predefined Bandwidth Management Services

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

Table 83 Media Bandwidth Management Setup: Services

SERVICE	DESCRIPTION
FTP	File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail.
WWW	The World Wide Web (WWW) is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser.
E-Mail	Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail:
VoIP (SIP)	Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP. SIP is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is transported primarily over UDP but can also be transported over TCP.
BitTorrent	BitTorrent is a free P2P (peer-to-peer) sharing tool allowing you to distribute large software and media files. BitTorrent requires you to search for a file with a searching engine yourself. It distributes files by corporation and trading, that is, the client downloads the file in small pieces and share the pieces with other peers to get other half of the file.
Gaming	Online gaming services lets you play multiplayer games on the Internet via broadband technology. As of this writing, your NBG4615 v2 supports Xbox, Playstation, Battlenet and MSN Game Zone.

Remote Management

24.1 Overview

This chapter provides information on the Remote Management screens.

Remote Management allows you to manage your NBG4615 v2 from a remote location through the following interfaces:

- LAN and WAN
- LAN only
- WAN only

Note: The NBG4615 v2 is managed using the Web Configurator.

24.2 What You Can Do in this Chapter

- Use the **WWW** screen to define the interface/s from which the NBG4615 v2 can be managed remotely using the web and specify a secure client that can manage the NBG4615 v2 ([Section 24.4 on page 202](#)).
- Use the **Telnet** screen to define the interface/s from which the NBG4615 v2 can be managed remotely using Telnet service and specify a secure client that can manage the NBG4615 v2 ([Section 24.5 on page 203](#)).
- Use the **Wake On LAN** screen to enable Wake on LAN and remotely turn on a device on the local network ([Section 24.6 on page 203](#)).

24.3 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 24.4 on page 202](#)) does not match the client IP address. If it does not match, the NBG4615 v2 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.

24.3.1 Remote Management and NAT

When NAT is enabled:

- Use the NBG4615 v2's WAN IP address when configuring from the WAN.
- Use the NBG4615 v2's LAN IP address when configuring from the LAN.

24.3.2 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The NBG4615 v2 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 **Maintenance > General** screen

24.4 WWW Screen

To change your NBG4615 v2's remote management settings, click **Management > Remote MGMT > WWW**.

Figure 126 Management > Remote Management > WWW

The screenshot shows the 'WWW' configuration page. At the top, there are three tabs: 'WWW', 'Telnet', and 'Wake On LAN'. The 'WWW' tab is selected. Below the tabs, there are three main configuration sections: 'Port' with a text box containing '80', 'Access Status' with a dropdown menu showing 'LAN', and 'Secured Client IP Address' with radio buttons for 'All' (selected) and 'Selected' (unselected), followed by an empty text box. Below these is a 'Note' section with a blue icon and two numbered points: '1. For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.' and '2. You may also need to create a Firewall rule.' At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 84 Management > Remote Management > 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 NBG4615 v2 using this service.
Secured Client IP Address	Select All to allow all computes to access the NBG4615 v2. Otherwise, check Selected and specify the IP address of the computer that can access the NBG4615 v2.
Apply	Click Apply to save your customized settings.
Cancel	Click Cancel to begin configuring this screen afresh.

24.5 Telnet Screen

To change your NBG4615 v2's remote management settings, click **Management > Remote MGMT > Telnet** to open the **Telnet** screen.

Figure 127 Management > Remote MGMT > Telnet

The screenshot shows the 'Telnet' configuration window. It has a header bar with 'WWW', 'Telnet', and 'Wake On LAN' tabs. Below the tabs, there are three main configuration sections: 'Port' with a text box containing '23', 'Access Status' with a dropdown menu showing 'LAN', and 'Secured Client IP Address' with radio buttons for 'All' (selected) and 'Selected' (unselected), followed by an empty text box. A 'Note' icon is followed by the text 'You may also need to create a Firewall rule.' At the bottom of the window are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 85 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 NBG4615 v2 using this service.
Secured Client IP Address	Select All to allow all computes to access the NBG4615 v2. Otherwise, check Selected and specify the IP address of the computer that can access the NBG4615 v2.
Apply	Click Apply to save your customized settings.
Cancel	Click Cancel to begin configuring this screen afresh.

24.6 Wake On LAN Screen

Wake On LAN (WoL) allows you to remotely turn on a device on the network, such as a computer, storage device or media server. To use this feature the remote hardware (for example the network adapter on a computer) must support Wake On LAN using the "Magic Packet" method.

You need to know the MAC address of the remote device. It may be on a label on the device.

Use this screen to remotely turn on a device on the network. Click the **Management > Remote MGMT > Wake On LAN** to open the following screen.

Figure 128 Management > Remote MGMT > Wake On LAN

WWW Telnet Wake On LAN

Wake On LAN over WAN Settings

☒ Enable WOL over WAN

Port 9

Wake On LAN

Wake MAC Address Start

Note:
Please insert the MAC Address in this format 00:00:00:00:00:00

Apply Cancel

The following table describes the labels in this screen.

Table 86 Management > Remote MGMT > Wake On LAN

LABEL	DESCRIPTION
Wake On LAN over WAN Settings	
Enable WOL over WAN	Select this option to have the NBG4615 v2 forward a WoL "Magic Packet" to all devices on the LAN if the packet comes from the WAN or remote network and uses the port number specified in the Port field. A LAN device whose hardware supports Wake on LAN then will be powered on if it is turned off previously.
Port	Type a port number from which a WoL packet is forwarded to the LAN.
Wake On LAN	
Wake MAC Address	Enter the MAC Address of the device on the network that will be turned on. A MAC address consists of six hexadecimal character pairs.
Start	Click this to have the NBG4615 v2 generate a WoL packet and forward it to turn the specified device on. A screen pops up displaying MAC address error if you input the MAC address incorrectly.
Apply	Click Apply to save the setting to the NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

Universal Plug-and-Play (UPnP)

25.1 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.

25.2 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.

25.2.1 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.

25.2.2 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 NBG4615 v2 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.

25.3 UPnP Screen

Use this screen to enable UPnP on your NBG4615 v2.

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

Figure 129 Management > UPnP



The following table describes the fields in this screen.

Table 87 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 NBG4615 v2's IP address (although you must still enter the password to access the web configurator).
Apply	Click Apply to save the setting to the NBG4615 v2.
Cancel	Click Cancel to return to the previously saved settings.

25.4 Technical Reference

The sections show examples of using UPnP.

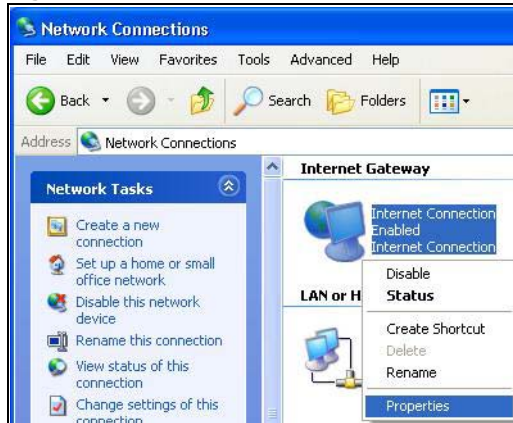
25.4.1 Using UPnP in Windows XP Example

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 NBG4615 v2.

Make sure the computer is connected to a LAN port of the NBG4615 v2. Turn on your computer and the NBG4615 v2.

25.4.1.1 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 130 Network Connections

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

Figure 131 Internet Connection Properties

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

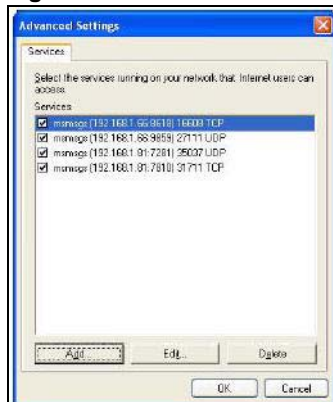
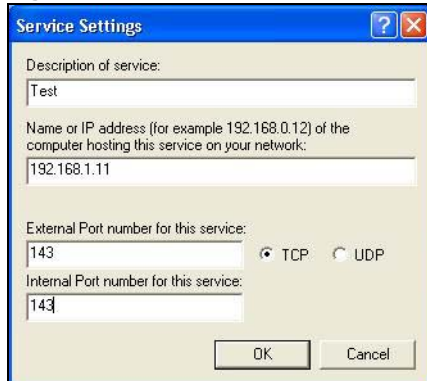
Figure 132 Internet Connection Properties: Advanced Settings

Figure 133 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 134 System Tray Icon

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

Figure 135 Internet Connection Status

25.4.2 Web Configurator Easy Access

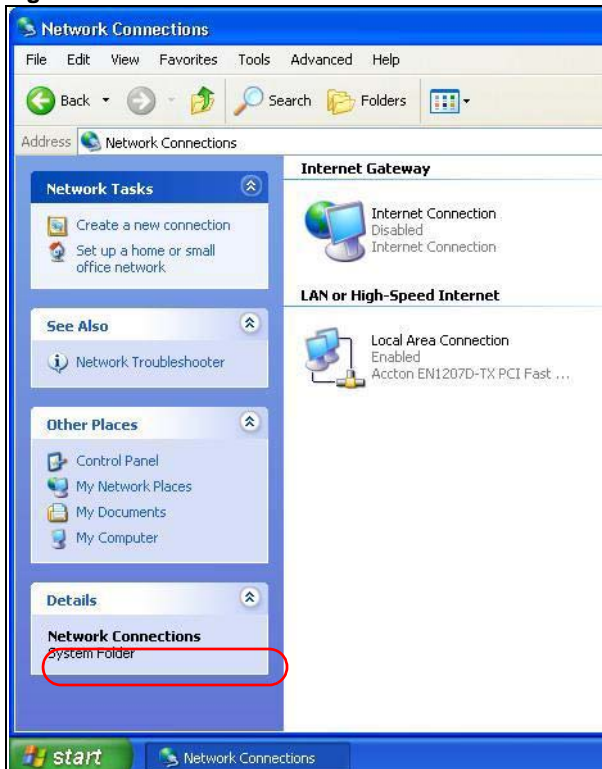
With UPnP, you can access the web-based configurator on the NBG4615 v2 without finding out the IP address of the NBG4615 v2 first. This comes helpful if you do not know the IP address of the NBG4615 v2.

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 136 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 NBG4615 v2 and select **Invoke**. The web configurator login screen displays.

Figure 137 Network Connections: My Network Places



6 Right-click on the icon for your NBG4615 v2 and select **Properties**. A properties window displays with basic information about the NBG4615 v2.

Figure 138 Network Connections: My Network Places: Properties: Example



Maintenance

26.1 Overview

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

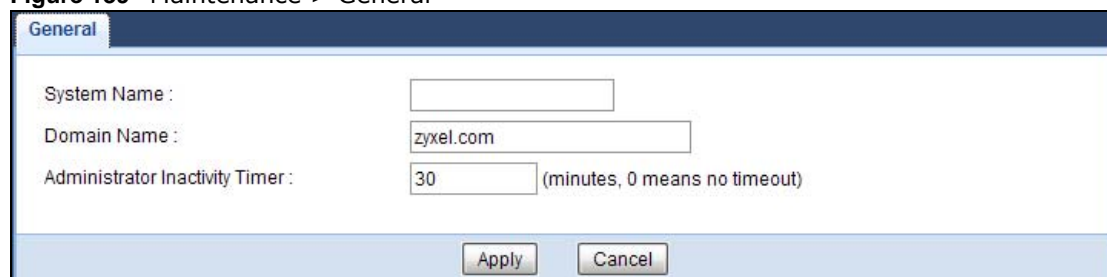
26.2 What You Can Do

- Use the **General** screen to set the timeout period of the management session ([Section 26.3 on page 211](#)).
- Use the **Password** screen to change your NBG4615 v2's system password ([Section 26.4 on page 212](#)).
- Use the **Time** screen to change your NBG4615 v2's time and date ([Section 26.5 on page 213](#)).
- Use the **Firmware Upgrade** screen to upload firmware to your NBG4615 v2 ([Section 26.6 on page 214](#)).
- Use the **Backup/Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration ([Section 26.8 on page 217](#)).
- Use the **Restart** screen to reboot the NBG4615 v2 without turning the power off ([Section 26.8 on page 217](#)).
- Use the **Language** screen to change the language for the Web Configurator ([Section 26.9 on page 217](#)).
- Use the **Sys OP Mode** screen to select how you want to use your NBG4615 v2 ([Section 26.11 on page 220](#)).

26.3 General Screen

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

Figure 139 Maintenance > General



The screenshot shows the 'General' tab of the Maintenance screen. It contains three input fields: 'System Name' (empty), 'Domain Name' (containing 'zyxel.com'), and 'Administrator Inactivity Timer' (containing '30'). The timer field has a unit label '(minutes, 0 means no timeout)'. At the bottom, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 88 Maintenance > General

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the NBG4615 v2 in an Ethernet network.
Domain Name	Enter the domain name you want to give to the NBG4615 v2.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click Apply to save your changes back to the NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

26.4 Password Screen

It is strongly recommended that you change your NBG4615 v2's password.

If you forget your NBG4615 v2's password (or IP address), you will need to reset the device. See [Section 26.8 on page 217](#) for details.

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

Figure 140 Maintenance > Password

The following table describes the labels in this screen.

Table 89 Maintenance > Password

LABEL	DESCRIPTION
Password Setup	Change your NBG4615 v2'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 NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

26.5 Time Setting Screen

Use this screen to configure the NBG4615 v2's time based on your local time zone. To change your NBG4615 v2's time and date, click **Maintenance > Time**. The screen appears as shown.

Figure 141 Maintenance > Time

The following table describes the labels in this screen.

Table 90 Maintenance > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your NBG4615 v2. Each time you reload this page, the NBG4615 v2 synchronizes the time with the time server.
Current Date	This field displays the date of your NBG4615 v2. Each time you reload this page, the NBG4615 v2 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 .

Table 90 Maintenance > Time (continued)

LABEL	DESCRIPTION
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you select Manual , enter the new date in this field and then click Apply .
Get from Time Server	Select this radio button to have the NBG4615 v2 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 NBG4615 v2.
Cancel	Click Cancel to begin configuring this screen afresh.

26.6 Firmware Upgrade Screen

Find firmware at www.zyxel.com in a file that uses the version number and project code with a "*.bin" extension, e.g., "V1.00(AAFI.0).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 NBG4615 v2.

Figure 142 Maintenance > Firmware Upgrade

The following table describes the labels in this screen.

Table 91 Maintenance > Firmware Upgrade

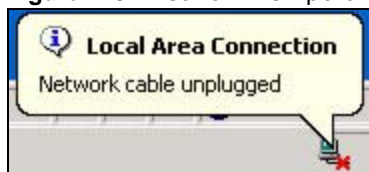
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse... to find it.
Browse...	Click Browse... to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click Upload to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

Note: Do not turn off the NBG4615 v2 while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the NBG4615 v2 again.

The NBG4615 v2 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 143 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.

26.7 Configuration Backup/Restore Screen

Backup configuration allows you to back up (save) the NBG4615 v2’s current configuration to a file on your computer. Once your NBG4615 v2 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 NBG4615 v2.

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

Figure 144 Maintenance > Backup/Restore

Backup/Restore

Backup Configuration

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

Restore Configuration

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

File Path : **Browse...** **Upload**

Back to Factory Defaults

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

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

Reset

The following table describes the labels in this screen.

Table 92 Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup	Click Backup to save the NBG4615 v2’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.

Table 92 Maintenance > Backup/Restore (continued)

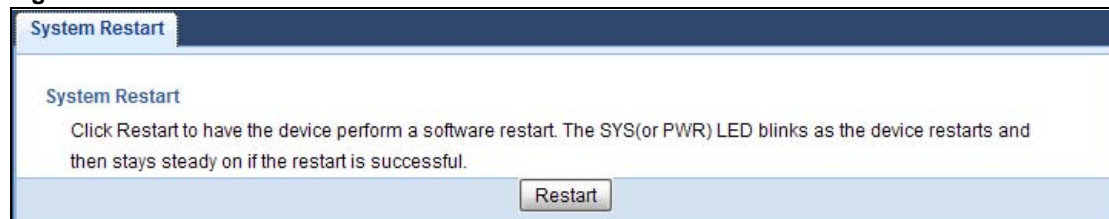
LABEL	DESCRIPTION
Upload	<p>Click Upload to begin the upload process.</p> <p>Note: Do not turn off the NBG4615 v2 while configuration file upload is in progress.</p> <p>After you see a "configuration upload successful" screen, you must then wait one minute before logging into the NBG4615 v2 again. The NBG4615 v2 automatically restarts in this time causing a temporary network disconnect.</p> <p>If you see an error screen, click Back to return to the Backup/Restore screen.</p>
Reset	<p>Pressing the Reset button in this section clears all user-entered configuration information and returns the NBG4615 v2 to its factory defaults.</p> <p>You can also press the RESET button on the rear panel to reset the factory defaults of your NBG4615 v2. Refer to the chapter about introducing the Web Configurator for more information on the RESET button.</p>

Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default NBG4615 v2 IP address (192.168.1.2). See [Appendix C on page 251](#) for details on how to set up your computer's IP address.

26.8 Restart Screen

System restart allows you to reboot the NBG4615 v2 without turning the power off.

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

Figure 145 Maintenance > Restart

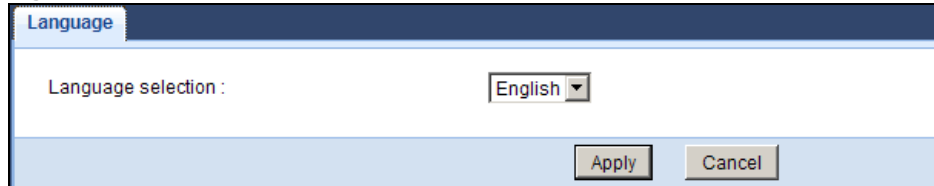
Click **Restart** to have the NBG4615 v2 reboot. This does not affect the NBG4615 v2's configuration.

26.9 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 NBG4615 v2.

Figure 146



26.10 System Operation Mode Overview

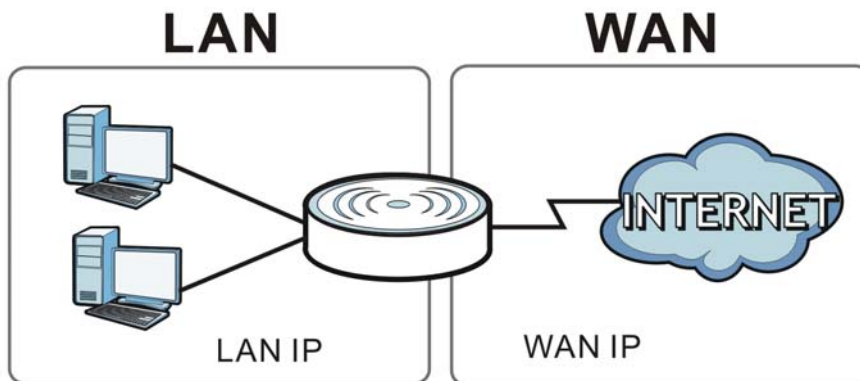
The **Sys OP Mode** (System Operation Mode) function lets you configure your NBG4615 v2 as an access point, wireless client or both at the same time. You can choose between **Router**, **Access Point Mode**, **Universal Repeater Mode**, **WISP Mode** and **WISP + Universal Repeater Mode** depending on your network topology and the features you require from your device.

The following describes the device modes available in your NBG4615 v2.

Router

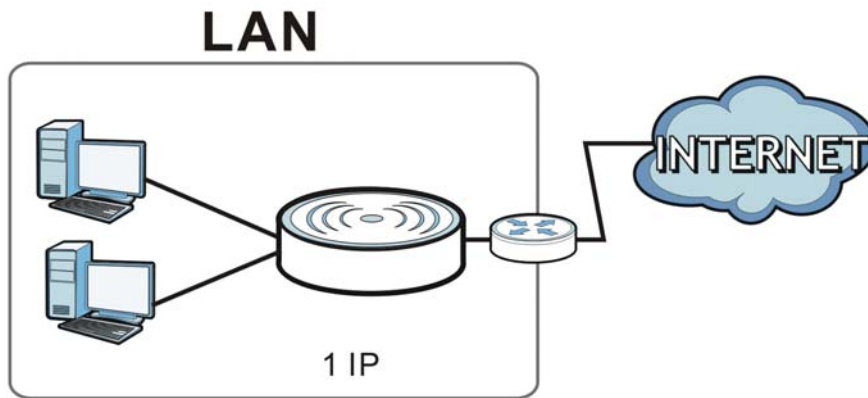
A router connects your local network with another network, such as the Internet. The router has two IP addresses, the LAN IP address and the WAN IP address.

Figure 147 LAN and WAN IP Addresses in Router Mode



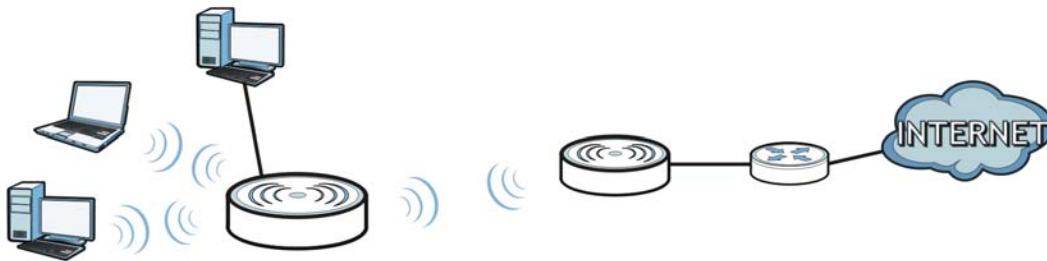
Access Point

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

Figure 148 Access Point Mode

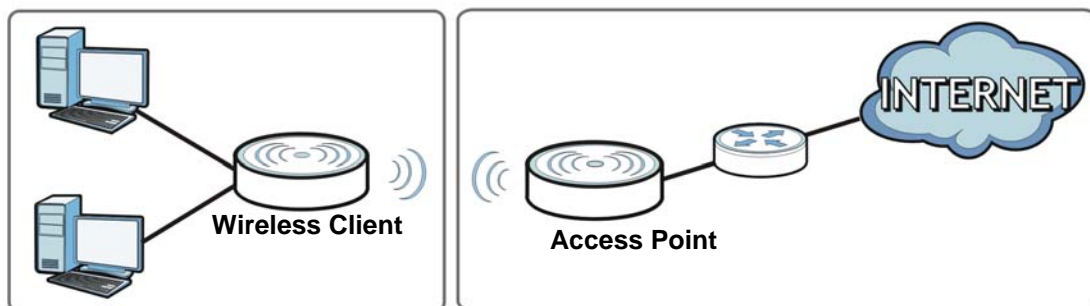
Universal Repeater

NBG4615 v2 in Universal Repeater mode work as an access point and wireless client simultaneously.

Figure 149 Universal Repeater Mode

WISP

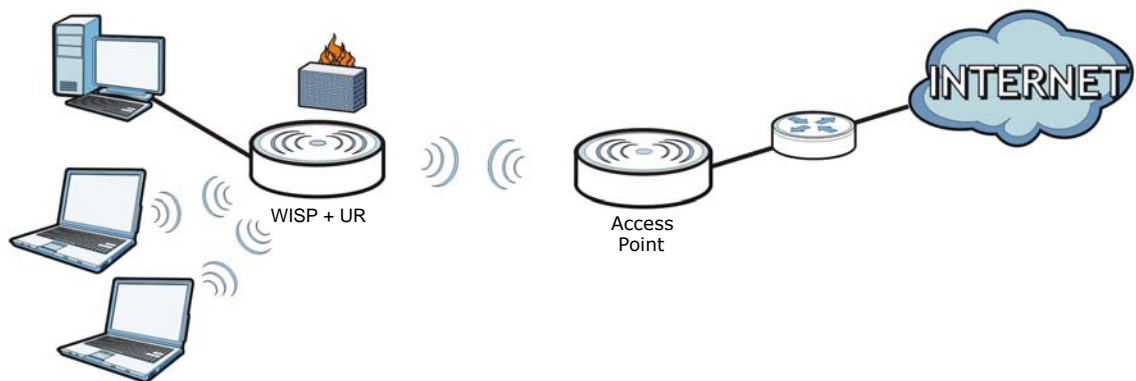
In WISP mode, the NBG4615 v2 acts as a wireless client to connect to an existing access point wirelessly. It acts just like a wireless client in notebooks/computers.

Figure 150 WISP Mode

WISP + Universal Repeater

In this mode, the NBG4615 v2 has the same function as in WISP mode, and can also provide WiFi function to the clients on the LAN side.

Figure 151 WISP + UR Mode



26.11 Sys OP Mode Screen

Use this screen to select how you want to use your NBG4615 v2.

Figure 152 Maintenance > Sys OP Mode

Sys OP Mode

Configuration Mode

☐ Router Mode

☐ Access Point Mode

☒ Universal Repeater Mode

☐ WISP Mode

☐ WISP + Universal Repeater Mode

Note:

Router: In this mode, the device is supported to connect to internet via ADSL/Cable Modem. PCs in LAN ports share the same IP to ISP through WAN Port.

Access Point: In this mode, all Ethernet ports are bridged together. The device allows the wireless-equipped computer can communicate with a wired network.

Universal Repeater Mode: In this mode, the device acts as both access point and wireless client. It can transmit wireless traffic between two wireless networks.

WISP Mode: In this mode, the device acts as a wireless client. It can connect to an existing network via an access point. Also router functions are added between the wireless WAN and the LAN.

WISP Mode + UR Mode: In this mode, the device acts as a wireless client. It can connect to an existing network via an access point. Also router functions are added between the wireless WAN and the LAN.

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

Table 93 Maintenance > Sys OP Mode

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

Table 93 Maintenance > Sys OP Mode (continued)

LABEL	DESCRIPTION
Access Point Mode	<p>Select Access Point Mode if your device bridges traffic between clients on the same network.</p> <ul style="list-style-type: none"> • In Access Point Mode, all Ethernet ports have the same IP address. • All ports on the rear panel of the device are LAN ports, including the port labeled WAN. There is no WAN port. • The DHCP server on your device is disabled. • Router functions (such as NAT, bandwidth management, remote management, firewall and so on) are not available when the NBG4615 v2 is in Access Point Mode. • The IP address of the device on the local network is set to 192.168.1.2.
Universal Repeater Mode	<p>Select Universal Repeater Mode if you want to have wireless clients associate with the NBG4615 v2 and also want to connect the NBG4615 v2 to an existing access point.</p> <ul style="list-style-type: none"> • In addition to wireless LAN settings between the NBG4615 v2 and wireless clients, you also need to configure security and wireless settings between the NBG4615 v2 and another access point. • Router functions (such as NAT, bandwidth management, remote management, firewall and so on) are not available when the NBG4615 v2 is in Universal Repeater Mode. • The IP address of the device on the local network is the same as the IP address given to the NBG4615 v2 while in Access Point Mode (default is 192.168.1.2).
WISP Mode	<p>Select WISP Mode if your device needs a wireless client to connect to an existing access point.</p> <ul style="list-style-type: none"> • You cannot configure Wireless LAN settings (including WPS) and scheduling in the WISP Mode. • The IP address of the device on the local network is the same as the IP address given to the NBG4615 v2 while in router mode (default is 192.168.1.1).
WISP + Universal Repeater Mode	<p>Select WISP + Universal Repeater Mode if your NBG4615 v2 needs a wireless client to connect to an existing access point, still have router functions, and also allow wireless clients to associate with the NBG4615 v2.</p> <ul style="list-style-type: none"> • The IP address of the device on the local network is the same as the IP address given to the NBG4615 v2 while in router mode (default is 192.168.1.1).
Apply	Click Apply to save your settings.
Cancel	Click Cancel to return your settings to the default (Router).

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

Troubleshooting

27.1 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](#)
- [NBG4615 v2 Access and Login](#)
- [Internet Access](#)
- [Resetting the NBG4615 v2 to Its Factory Defaults](#)
- [Wireless Router/AP Troubleshooting](#)
- [USB Device Problems](#)
- [ZyXEL Share Center Utility Problems](#)

27.2 Power, Hardware Connections, and LEDs

The NBG4615 v2 does not turn on. None of the LEDs turn on.

- 1 Make sure you are using the power adaptor or cord included with the NBG4615 v2.
- 2 Make sure the power adaptor or cord is connected to the NBG4615 v2 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 NBG4615 v2.
- 4 If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.7 on page 17](#).
- 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 NBG4615 v2.
- 5 If the problem continues, contact the vendor.

27.3 NBG4615 v2 Access and Login

I don't know the IP address of my NBG4615 v2.

- 1 The default IP address of the NBG4615 v2 in **Router Mode**, **WISP Mode**, or **WISP + Universal Repeater Mode** is **192.168.1.1**. The default IP address of the NBG4615 v2 in **Access Point Mode** or **Universal Repeater Mode** is **192.168.1.2**.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the NBG4615 v2 in **Router Mode**, **WISP Mode**, or **WISP + Universal Repeater Mode** 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 NBG4615 v2 (it depends on the network), so enter this IP address in your Internet browser.
- 3 If your NBG4615 v2 in **Access Point Mode** or **Universal Repeater Mode** 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 NBG4615 v2 to change all settings back to their default. This means your current settings are lost. See [Section 27.5 on page 227](#) in the **Troubleshooting** for information on resetting your NBG4615 v2.

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 27.5 on page 227](#).

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 of the NBG4615 v2 in **Router Mode**, **WISP Mode**, or **WISP + Universal Repeater Mode** is **192.168.1.1**. The default IP address of the NBG4615 v2 in **Access Point Mode** or **Universal Repeater Mode** is **192.168.1.2**.

- If you changed the IP address ([Section 16.4 on page 158](#)), 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 NBG4615 v2](#).
- 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 A on page 231](#).
 - 4 Make sure your computer is in the same subnet as the NBG4615 v2. (If you know that there are routers between your computer and the NBG4615 v2, skip this step.)
 - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See [Section 16.4 on page 158](#).
 - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG4615 v2. See [Section 16.4 on page 158](#).
 - 5 Reset the device to its factory defaults, and try to access the NBG4615 v2 with the default IP address. See [Section 1.5 on page 16](#).
 - 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the NBG4615 v2 using another service, such as Telnet. If you can access the NBG4615 v2, check the remote management settings and firewall rules to find out why the NBG4615 v2 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 NBG4615 v2.](#)

- 1 Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.
- 2 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.
- 3 Disconnect and re-connect the power adaptor or cord to the NBG4615 v2.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 27.5 on page 227](#).

27.4 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 Go to **Maintenance > Sys OP Mode**. Check your System Operation Mode setting.
 - If the NBG4615 v2 is in **Router Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access. Your computer and the NBG4615 v2 should be in the same subnet.
 - If the NBG4615 v2 is in **Access Point Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access and your computer is set to obtain an dynamic IP address.
 - If the NBG4615 v2 is in **Universal Repeater Mode**, make sure the NBG4615 v2 is wirelessly connected to an access point or wireless router with Internet access. Your computer should be set to obtain an dynamic IP address.
 - If the NBG4615 v2 is in **WISP Mode** or **WISP + Universal Repeater Mode**, make sure the NBG4615 v2 is wirelessly connected to an access point or wireless router with Internet access.
- 3 If the NBG4615 v2 is in **Router Mode**, make sure you entered your ISP account information correctly in the wizard or the WAN screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 4 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.
- 5 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 6 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NBG4615 v2), 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 1.7 on page 17](#).
- 2 Reboot the NBG4615 v2.
- 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 1.7 on page 17](#). If the NBG4615 v2 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 NBG4615 v2 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 NBG4615 v2.
- 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.

27.5 Resetting the NBG4615 v2 to Its Factory Defaults

If you reset the NBG4615 v2, you lose all of the changes you have made. The NBG4615 v2 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 NBG4615 v2:

- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for one to four seconds to restart/reboot the NBG4615 v2.
- 3 Press the **RESET** button for longer than five seconds to set the NBG4615 v2 back to its factory-default configurations.

If the NBG4615 v2 restarts automatically, wait for the NBG4615 v2 to finish restarting, and log in to the Web Configurator. The password is "1234".

If the NBG4615 v2 does not restart automatically, disconnect and reconnect the NBG4615 v2's power. Then, follow the directions above again.

27.6 Wireless Router/AP Troubleshooting

I cannot access the NBG4615 v2 or ping any computer from the WLAN (wireless AP or router).

- 1 Make sure the wireless LAN is enabled on the NBG4615 v2.
- 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 NBG4615 v2.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG4615 v2.
- 5 Check that both the NBG4615 v2 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 NBG4615 v2.
- 7 Make sure you allow the NBG4615 v2 to be remotely accessed through the WLAN interface. Check your remote management settings.
 - See the chapter on [Wireless LAN](#) in the User's Guide for more information.

[I set up URL keyword blocking, but I can still access a website that should be blocked.](#)

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

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

[I cannot access the Web Configurator after I switched to AP or universal repeater mode.](#)

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

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

[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.

27.7 USB Device Problems

I cannot access or see a USB device that is connected to the NBG4615 v2.

- 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 NBG4615 v2.
- 3 Ensure that the USB device has power.
- 4 Check your cable connections.
- 5 Restart the NBG4615 v2 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 NBG4615 v2 and try to connect to it again with your computer.
- 7 If the problem persists, contact your vendor.

What kind of USB devices do the NBG4615 v2 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 NBG4615 v2.

27.8 ZyXEL Share Center Utility Problems

I cannot access or see a USB device that is connected to the NBG4615 v2.

- 1 Disconnect the problematic USB device, then reconnect it to the NBG4615 v2.
- 2 Ensure that the USB device in question has power.
- 3 Check your cable connections.
- 4 Restart the NBG4615 v2 by disconnecting the power and then reconnecting it.
- 5 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 NBG4615 v2 and try to connect to it again with your computer.
- 6 If the problem persists, contact your vendor.

I cannot install the ZyXEL 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 download site for a newer version of the utility.

Two computers cannot connect the USB storage at the same time using the ZyXEL Share Center Utility.

Only one computer can connect to the USB storage through the ZyXEL Share Center Utility at a time. If two computers (**A** and **B**) want to connect to the USB storage by using the Utility, do the following:

- 1 After **A** finishes connection to the USB storage, disconnect it by clicking **Disconnect** in **A**'s Utility.
- 2 Connect **B** to the USB storage (through the Utility) by clicking **Connect** in **B**'s Utility.
- 3 If **A** does not disconnect the USB storage, **B** should click **Request to Connect** in the Utility to request **A** to disconnect. **B** cannot access the USB storage until **A** disconnects.
 - See [Chapter 12 on page 111](#) for more details on connecting to USB storage by the Utility.

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

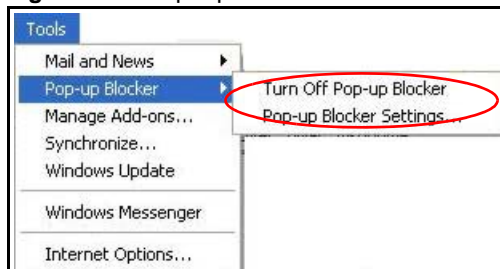
You may have to disable pop-up blocking to log into your device.

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

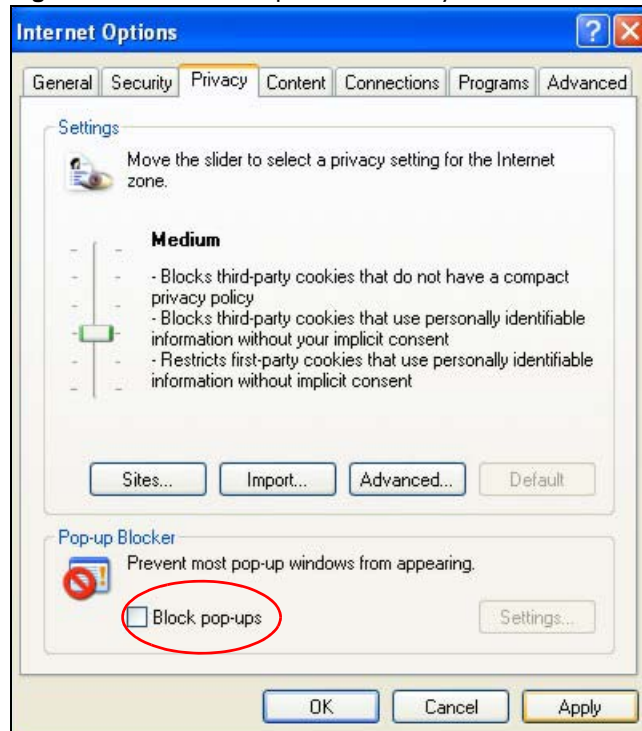
- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 153 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.

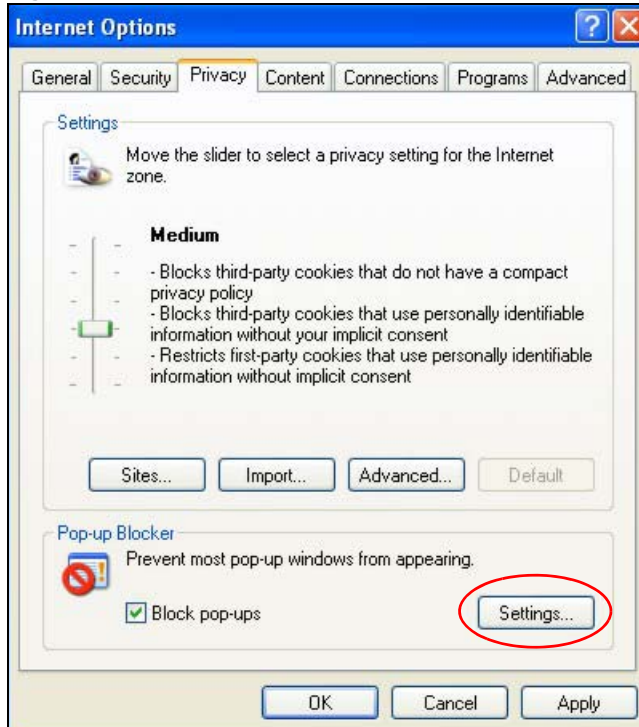
Figure 154 Internet Options: Privacy

- 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 155 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 156 Pop-up Blocker Settings

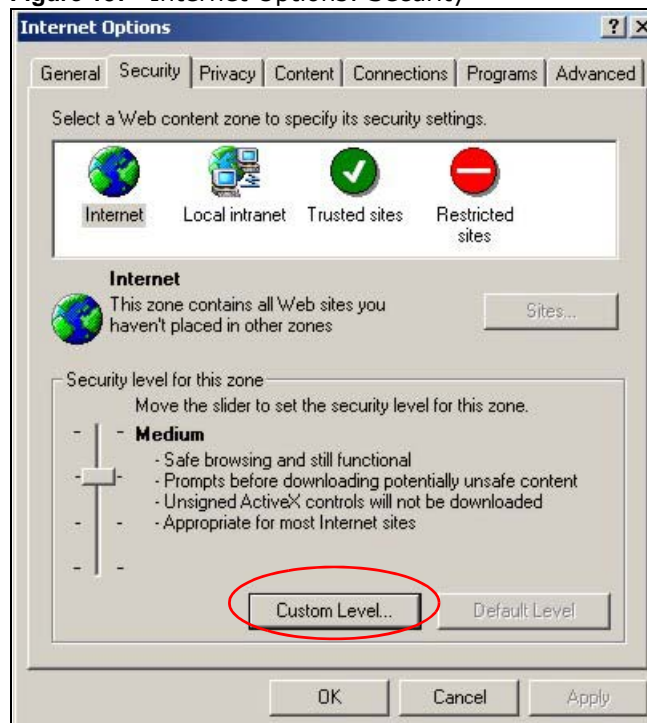
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

JavaScript

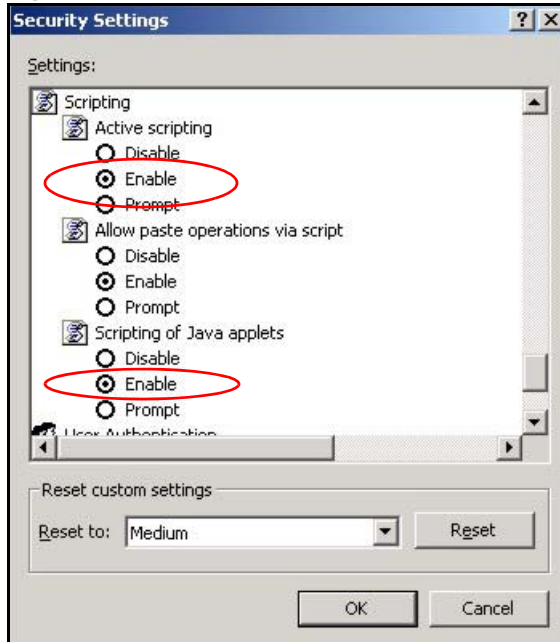
If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

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

Figure 157 Internet Options: Security

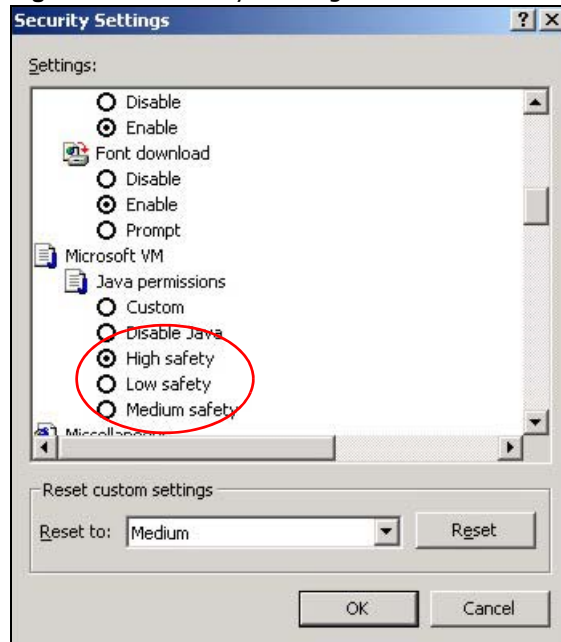


- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6 Click **OK** to close the window.

Figure 158 Security Settings - Java Scripting

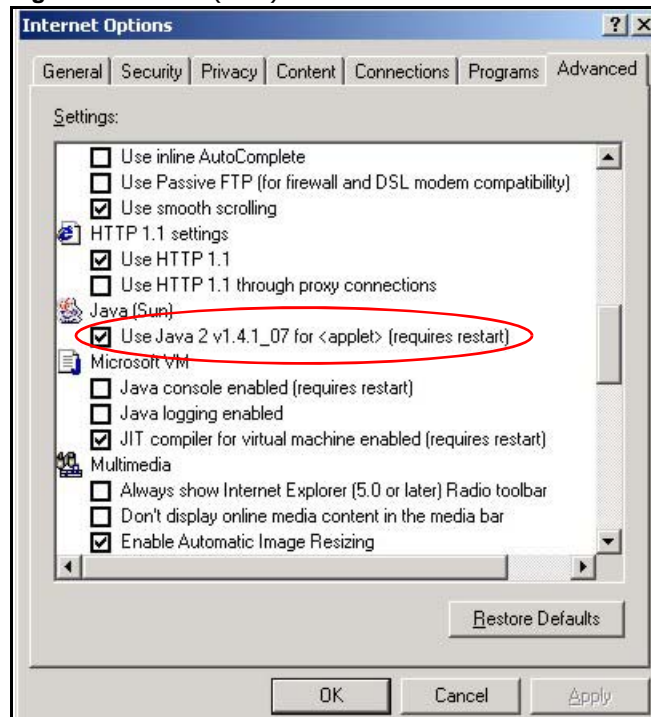
Java Permissions

- 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 159 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.

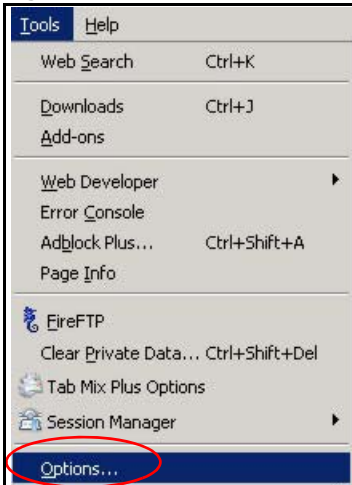
Figure 160 Java (Sun)

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.

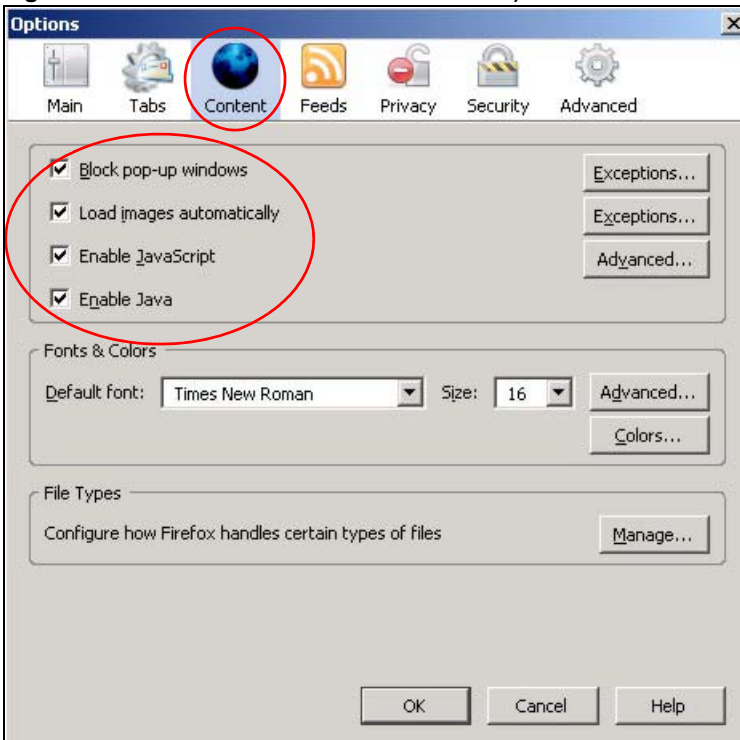
You can enable Java, Javascript and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

Figure 161 Mozilla Firefox: TOOLS > Options



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

Figure 162 Mozilla Firefox Content Security



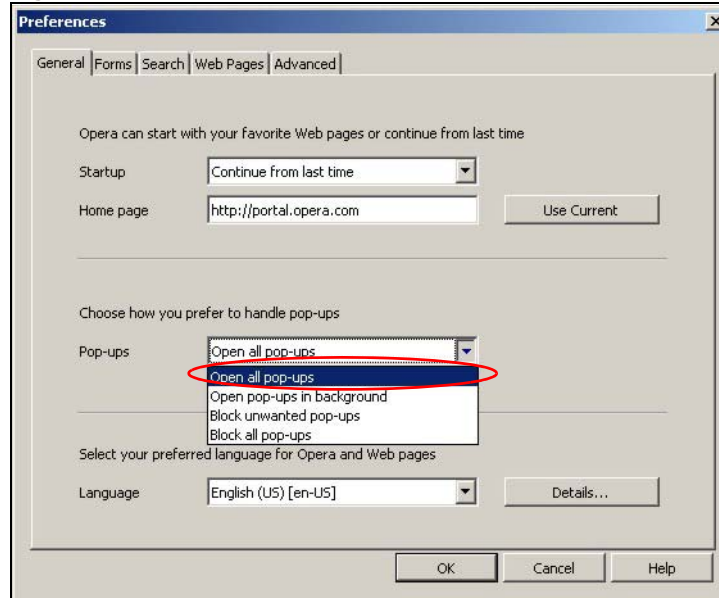
Opera

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

Allowing Pop-Ups

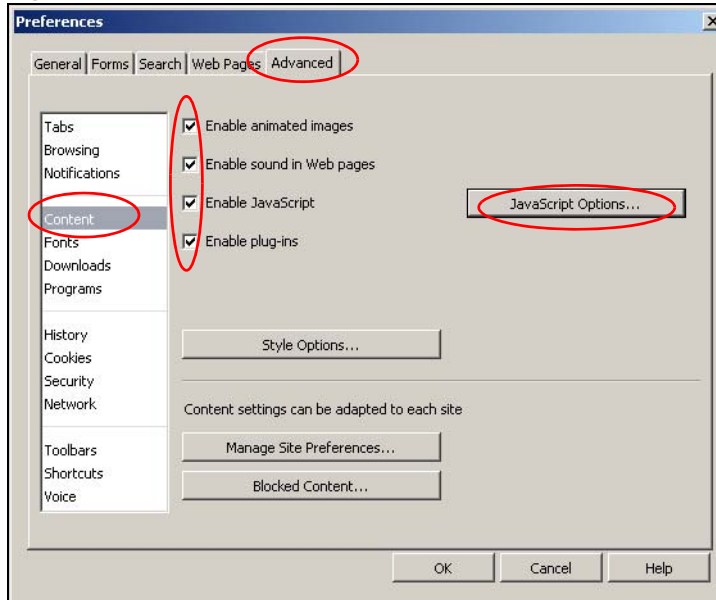
From Opera, click **Tools**, then **Preferences**. In the **General** tab, go to **Choose how you prefer to handle pop-ups** and select **Open all pop-ups**.

Figure 163 Opera: Allowing Pop-Ups

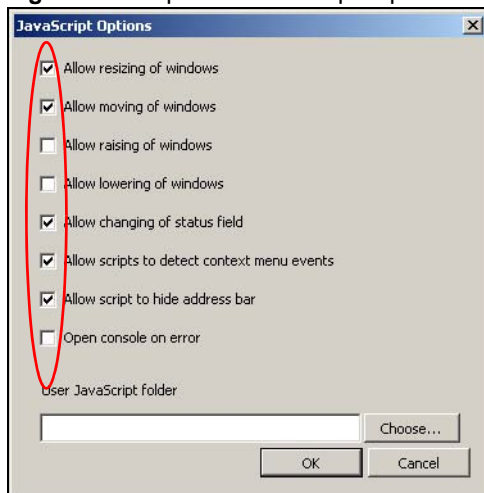


Enabling Java

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 164 Opera: Enabling Java

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

Figure 165 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.

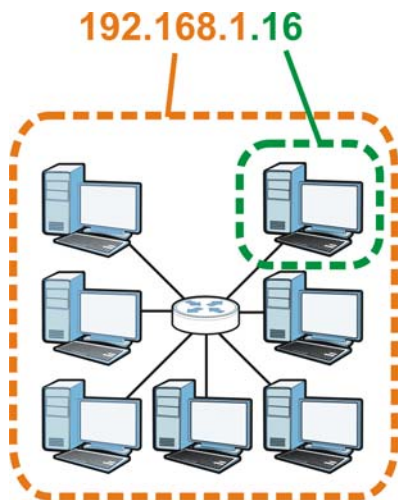
Structure

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 166 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 94 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 95 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 96 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 97 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 97 Alternative Subnet Mask Notation (continued)

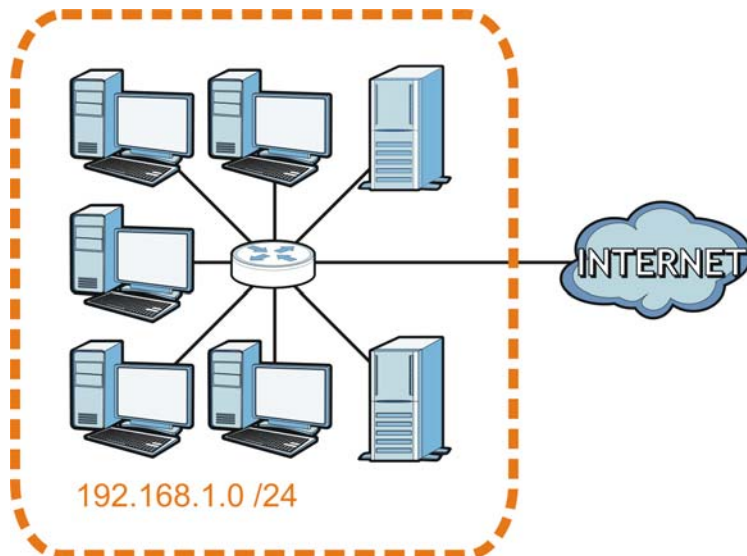
SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

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.

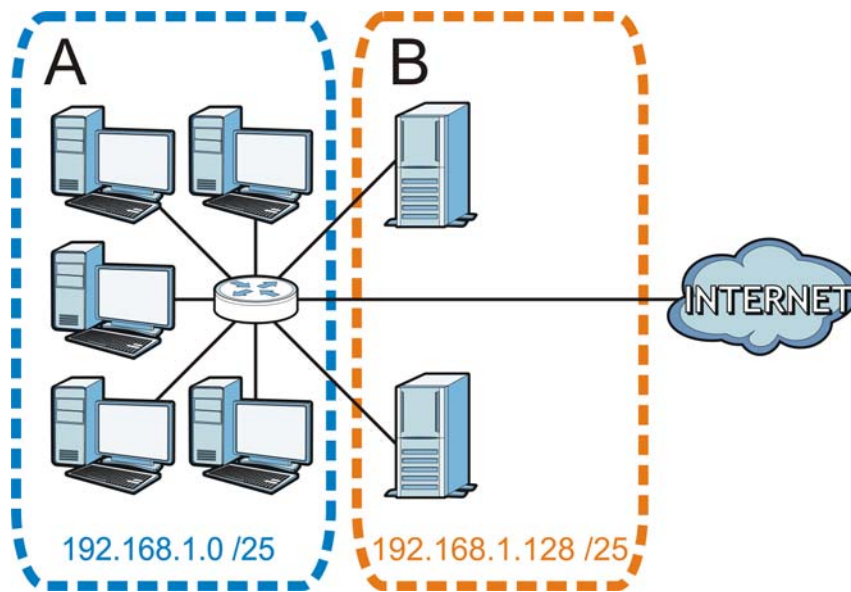
The following figure shows the company network before subnetting.

Figure 167 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 168 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 98 Subnet 1

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

Table 99 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 100 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 101 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 102 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

Table 102 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
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 103 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 104 16-bit Network Number Subnet Planning

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

Configuring IP Addresses

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the NBG4615 v2.

Once you have decided on the network number, pick an IP address for your NBG4615 v2 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 NBG4615 v2 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 NBG4615 v2 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.

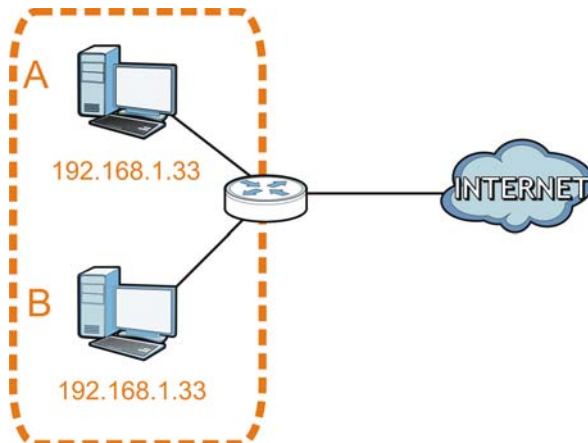
IP Address Conflicts

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.

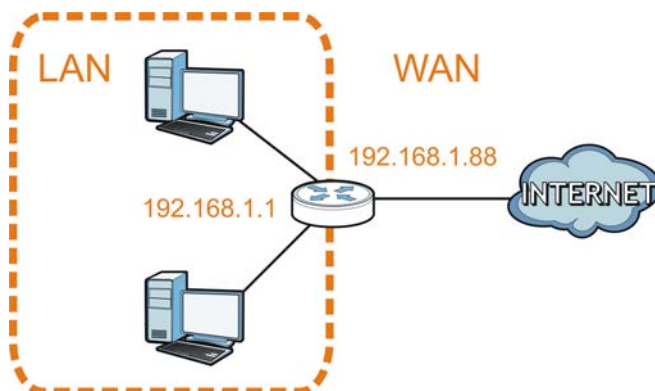
Figure 169 Conflicting Computer IP Addresses Example



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.

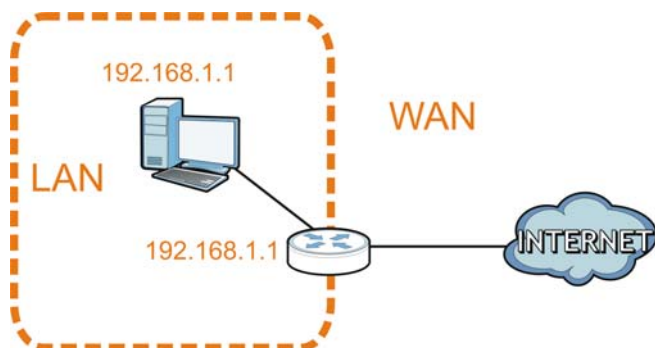
Figure 170 Conflicting Router IP Addresses Example



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 171 Conflicting Computer and Router IP Addresses Example



Setting Up Your Computer's IP Address

Note: Your specific NBG4615 v2 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 251](#)
- [Windows Vista](#) on [page 255](#)
- [Windows 7](#) on [page 259](#)
- [Mac OS X: 10.3 and 10.4](#) on [page 263](#)
- [Mac OS X: 10.5 and 10.6](#) on [page 266](#)
- [Linux: Ubuntu 8 \(GNOME\)](#) on [page 269](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 273](#)

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**.



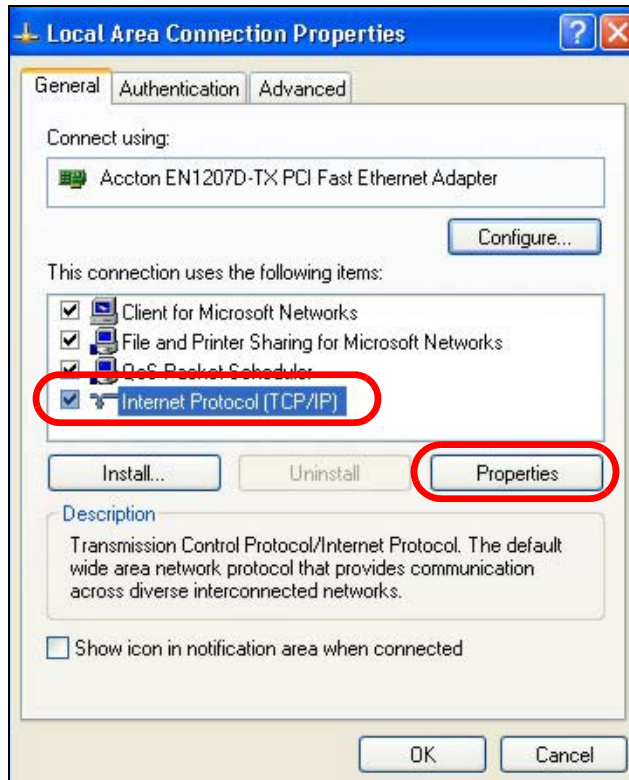
- 2 In the **Control Panel**, click the **Network Connections** icon.



- 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

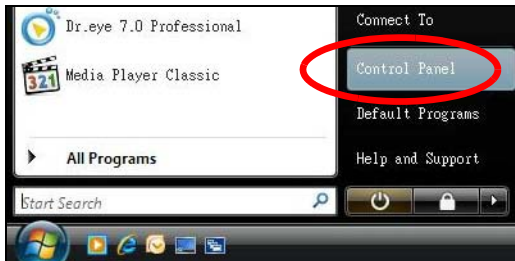
- 1 Click **Start > All Programs > Accessories > Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

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.

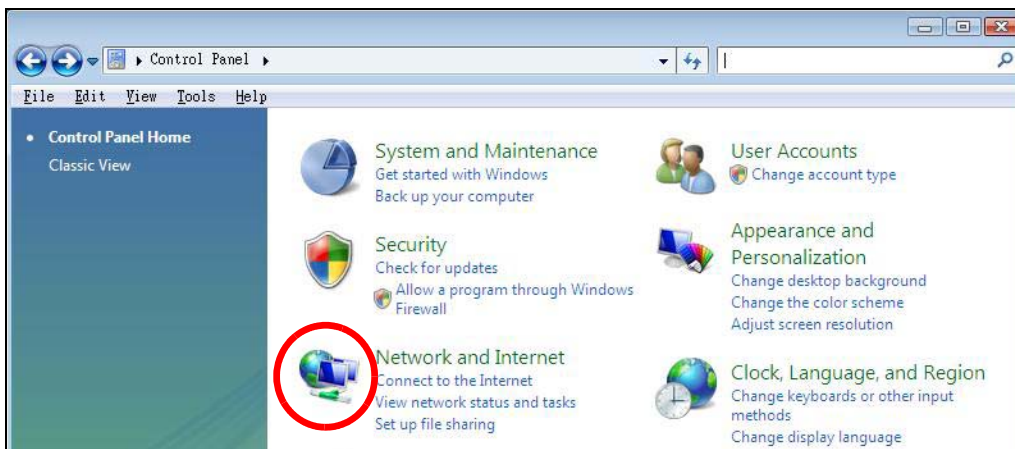
Windows Vista

This section shows screens from Windows Vista Professional.

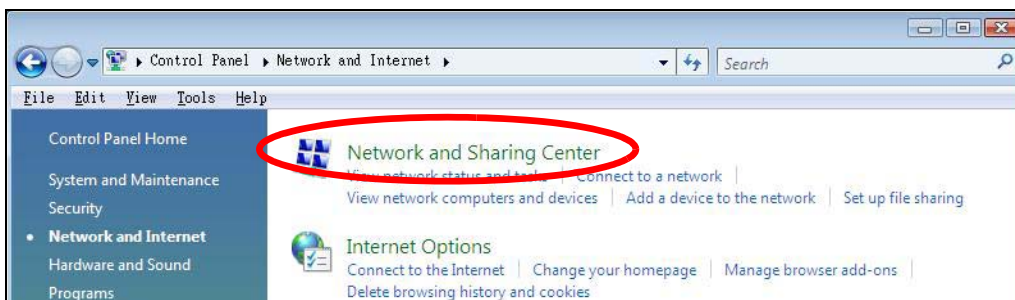
- 1 Click **Start > Control Panel**.



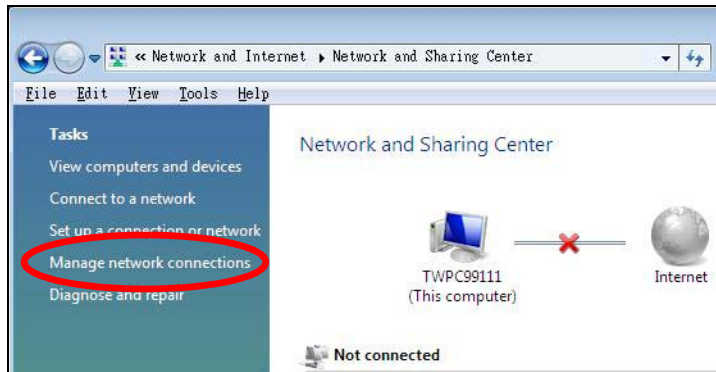
- 2 In the **Control Panel**, click the **Network and Internet** icon.



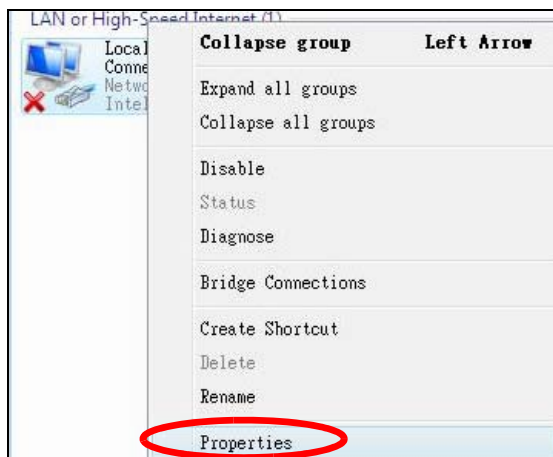
- 3 Click the **Network and Sharing Center** icon.



- 4 Click **Manage network connections**.

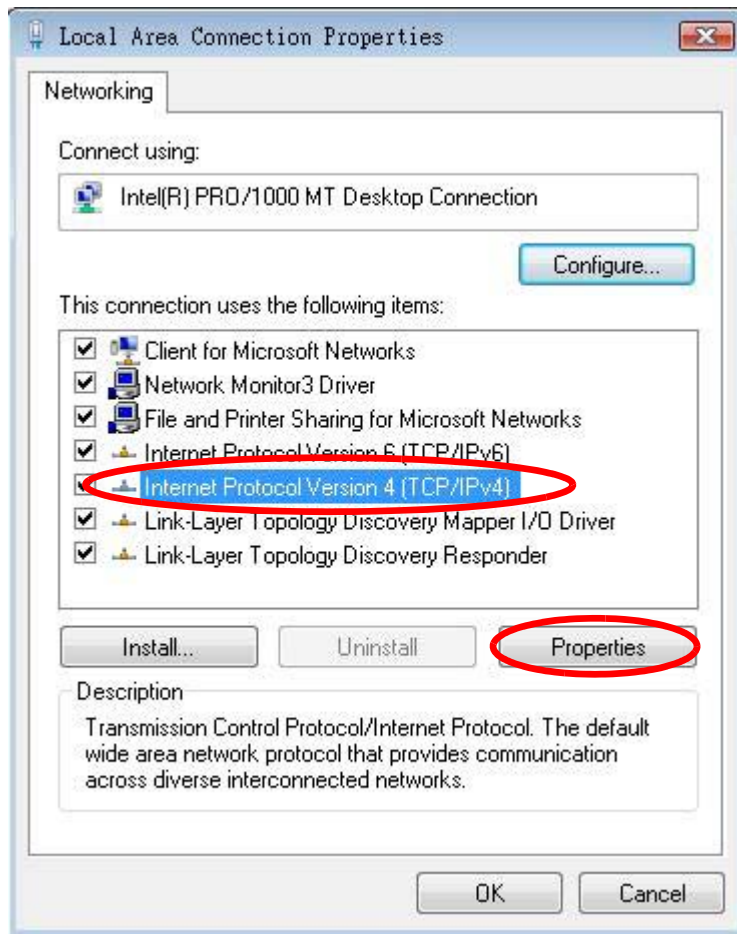


- 5 Right-click **Local Area Connection** and then select **Properties**.

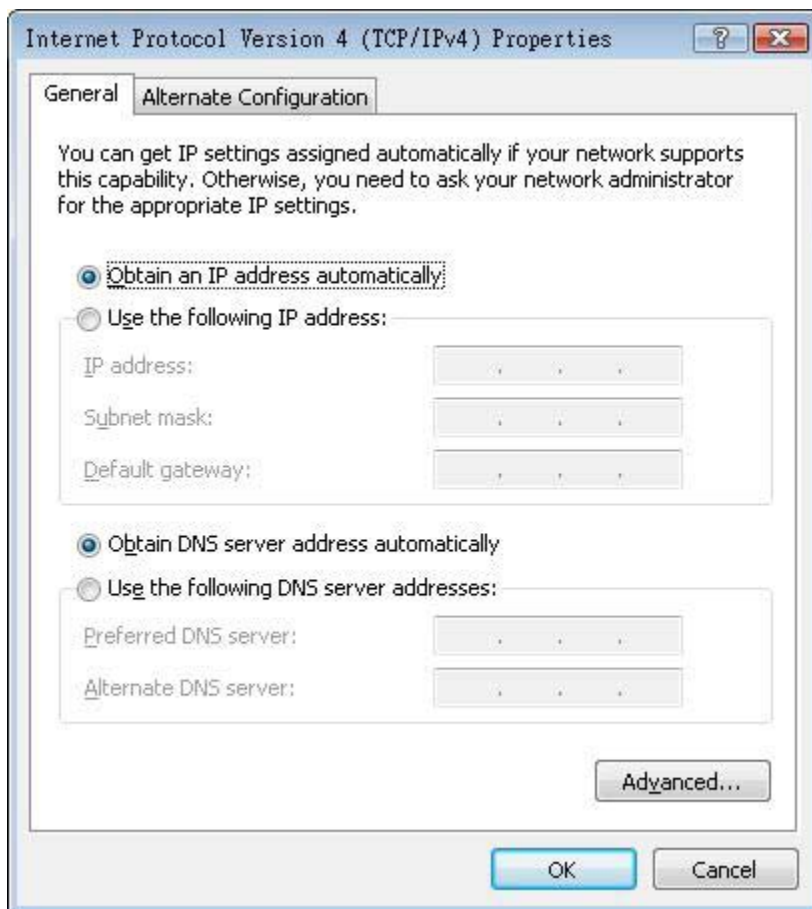


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

- 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.

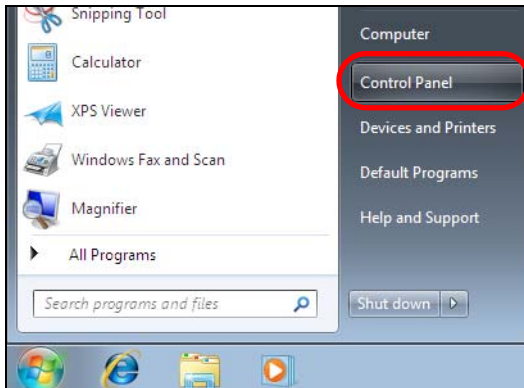
Verifying Settings

- 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.

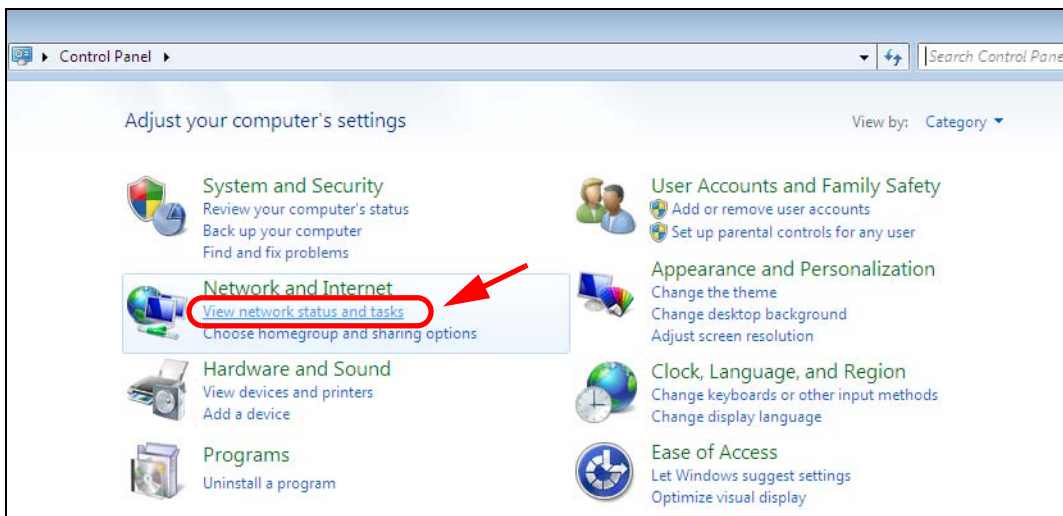
Windows 7

This section shows screens from Windows 7 Enterprise.

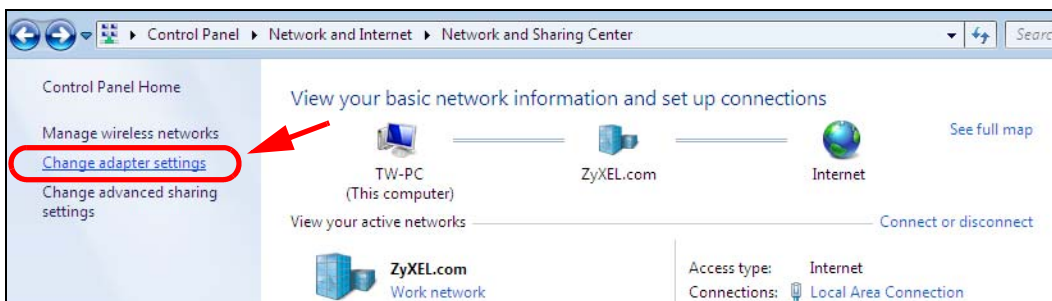
- 1 Click **Start > Control Panel**.



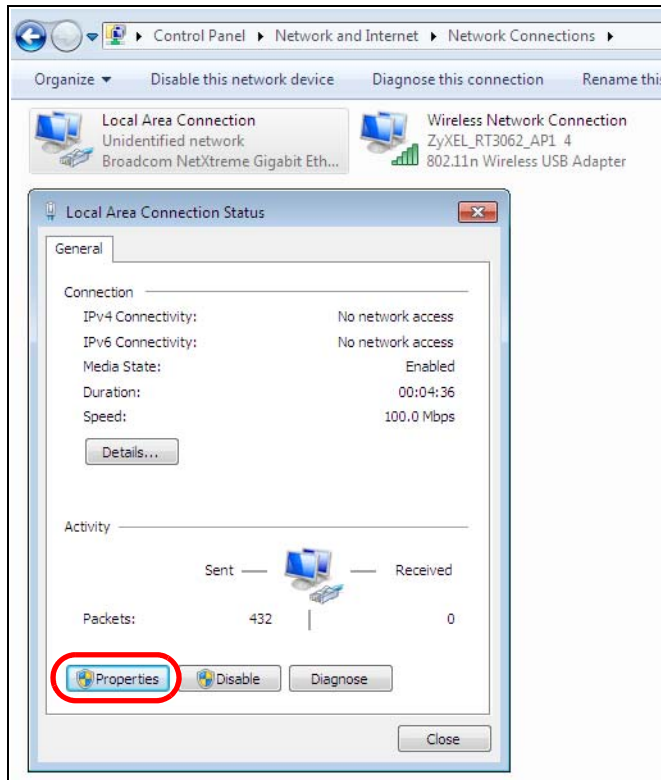
- 2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.



- 3 Click **Change adapter settings**.

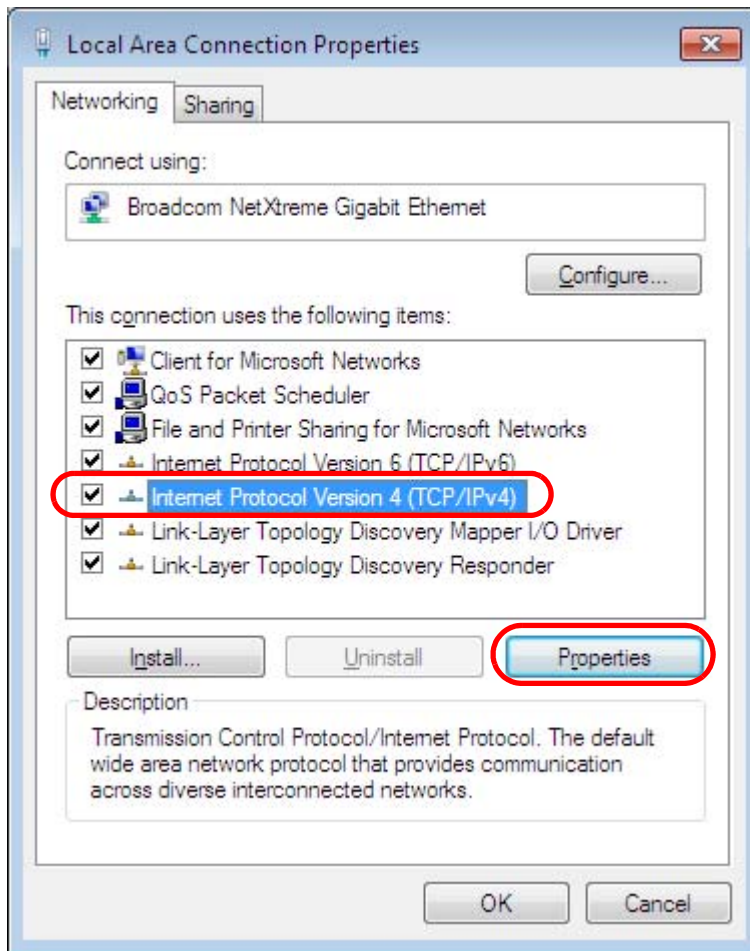


- 4 Double click **Local Area Connection** and then select **Properties**.

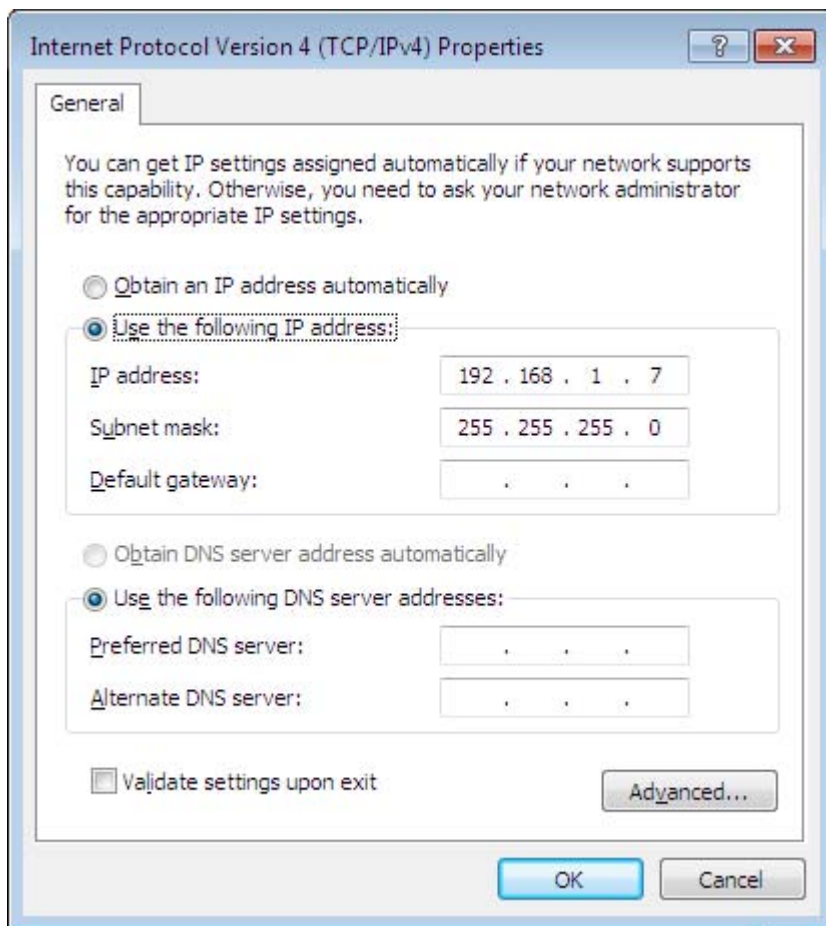


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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



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



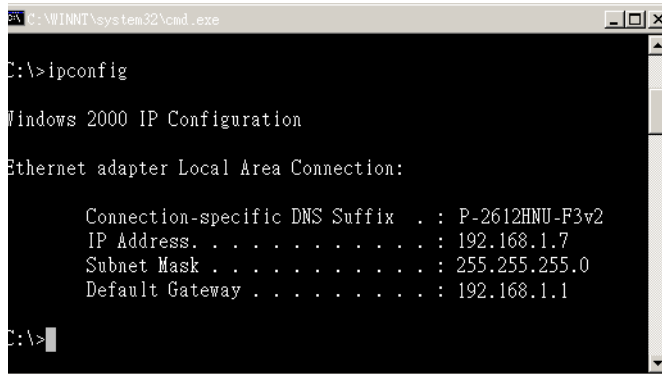
- 7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

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.



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

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

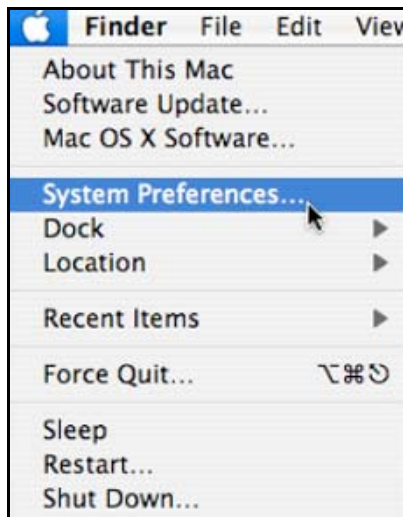
    Connection-specific DNS Suffix  . : P-2612HNU-F3v2
    IP Address. . . . . : 192.168.1.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\>
```

Mac OS X: 10.3 and 10.4

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

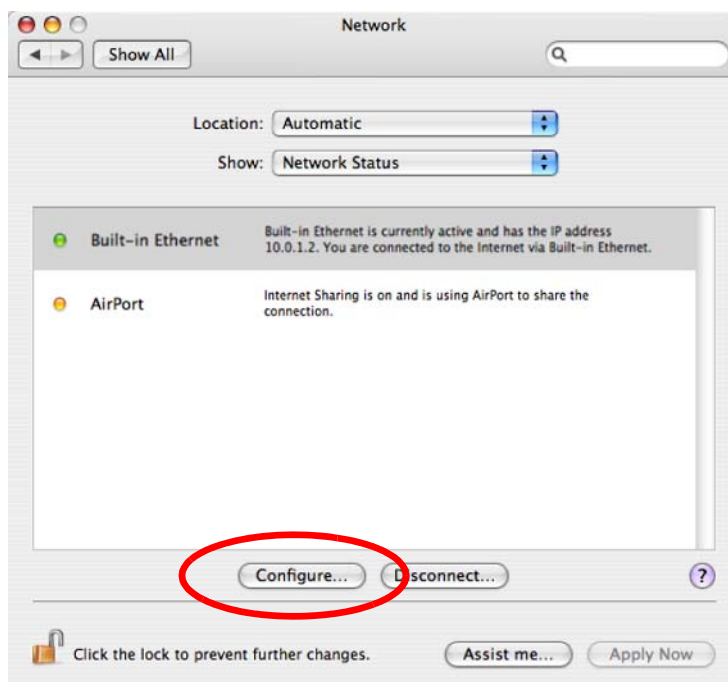
- 1 Click **Apple > System Preferences**.



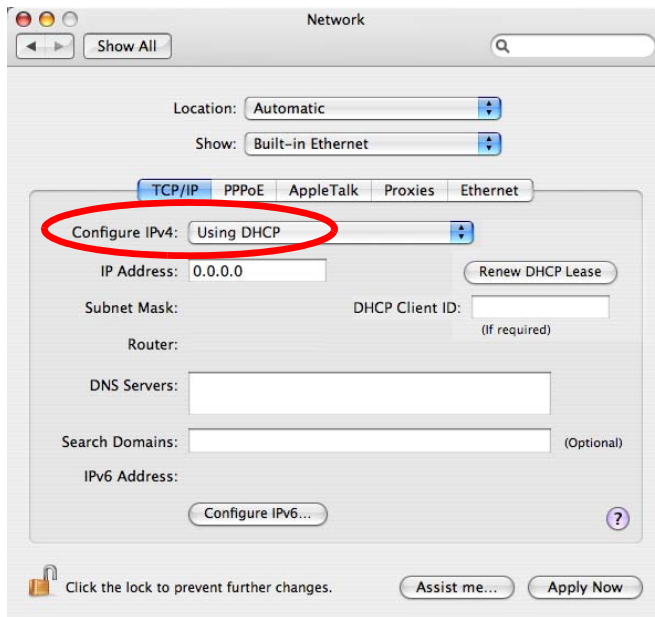
- 2 In the **System Preferences** window, click the **Network** icon.



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

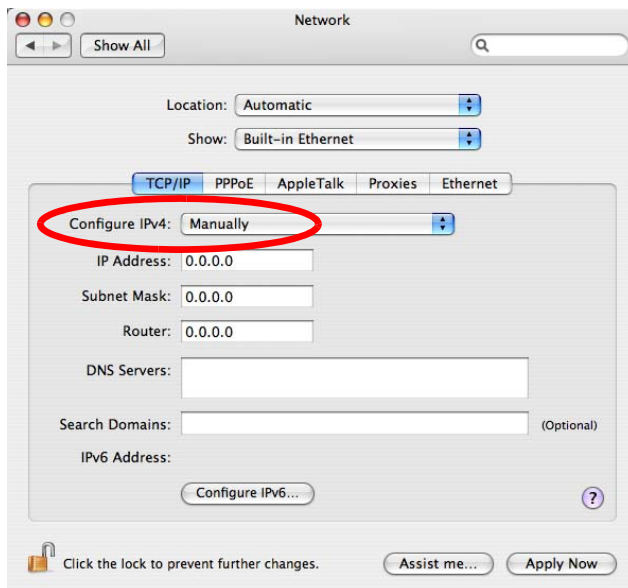


- 4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.



5 For statically assigned settings, do the following:

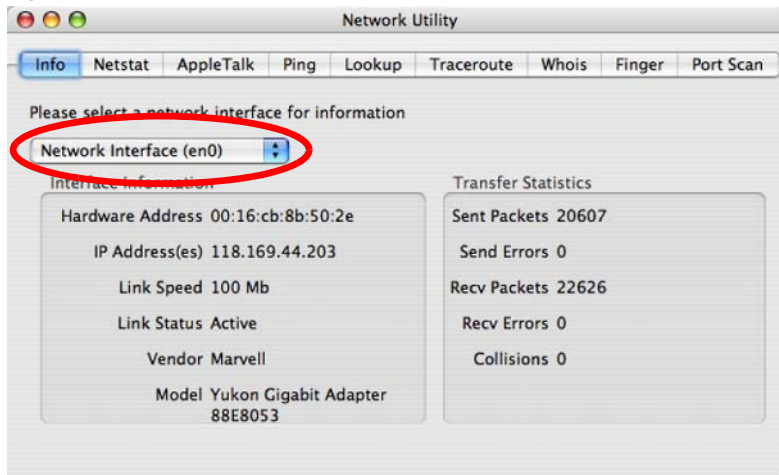
- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.
- In the **Router** field, type the IP address of your device.



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

Verifying Settings

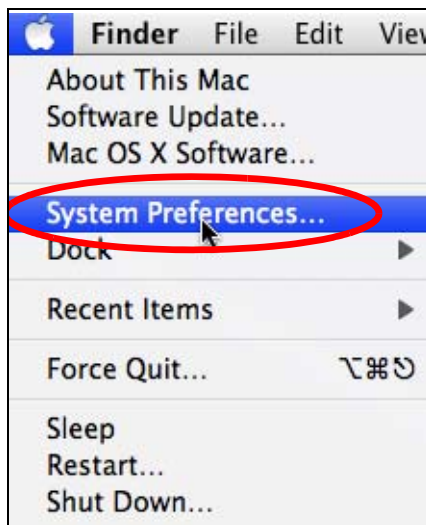
Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 172 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.

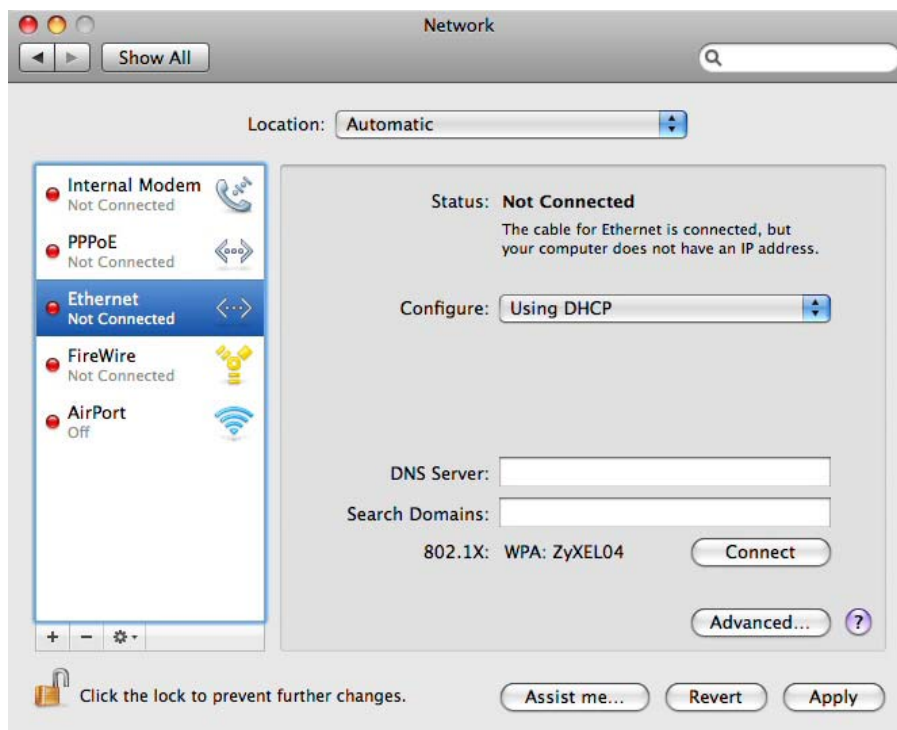
- 1 Click **Apple > System Preferences**.



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

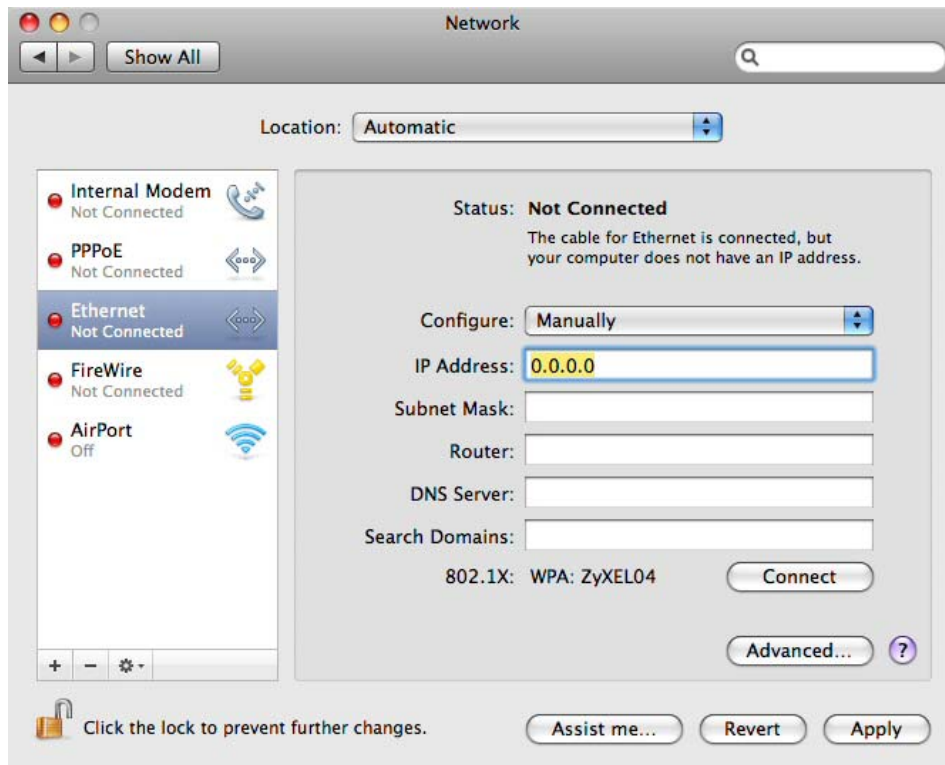


- 3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.



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

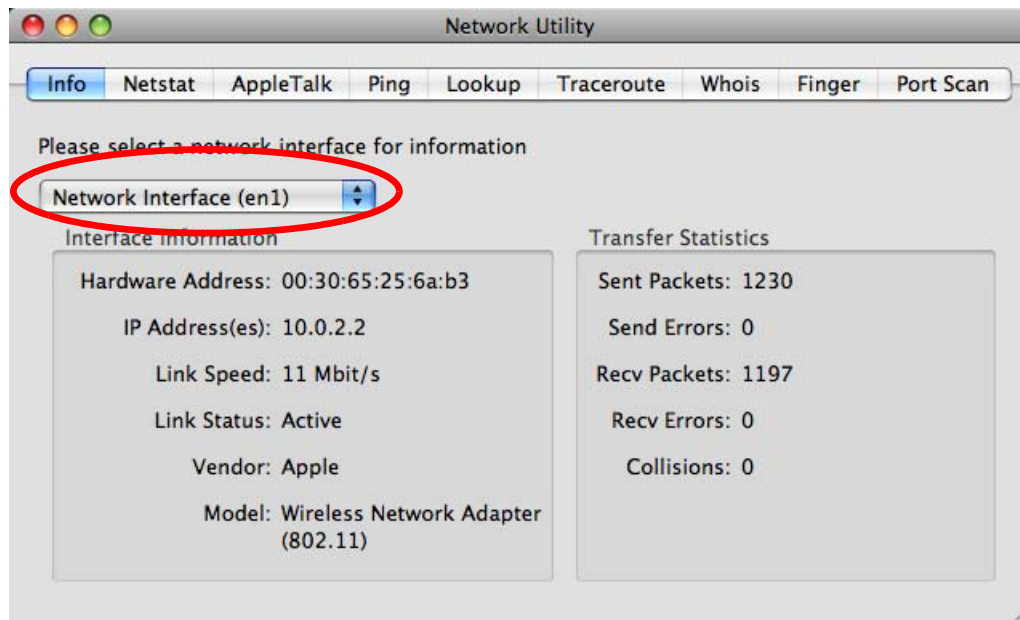
- 5 For statically assigned settings, do the following:
 - From the **Configure** list, select **Manually**.
 - In the **IP Address** field, enter your IP address.
 - In the **Subnet Mask** field, enter your subnet mask.
 - In the **Router** field, enter the IP address of your NBG4615 v2.



- 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 173 Mac OS X 10.5: Network Utility

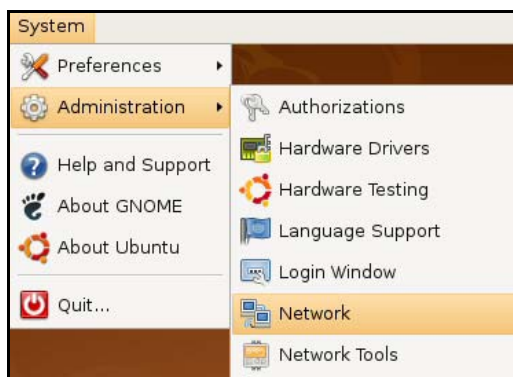
Linux: Ubuntu 8 (GNOME)

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.

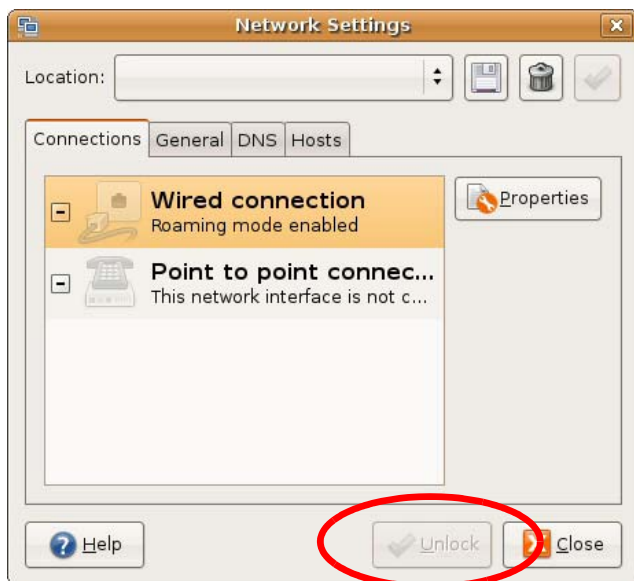
Note: Make sure you are logged in as the root administrator.

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.



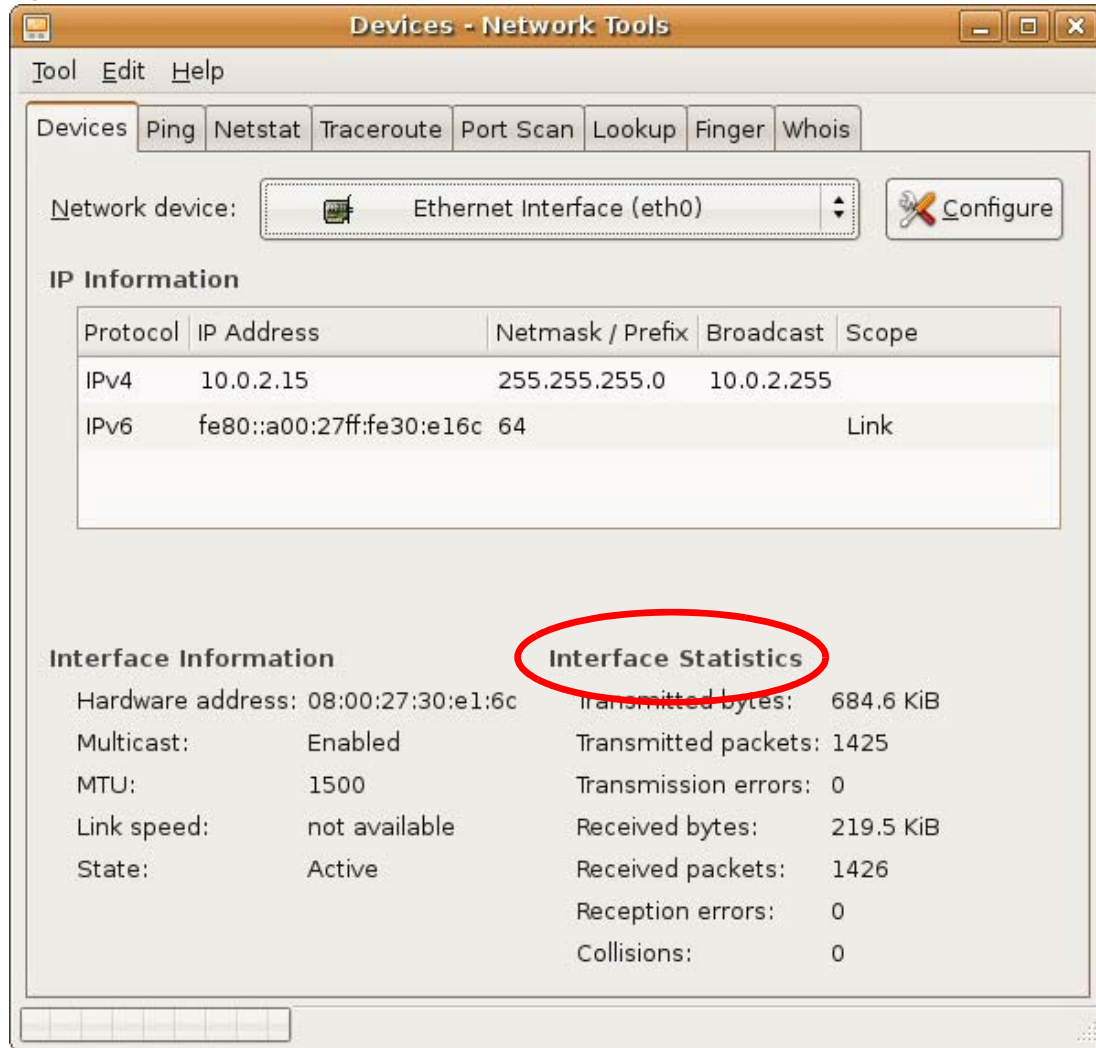
- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
 - In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.
- 6 Click **OK** to 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 174 Ubuntu 8: Network Tools

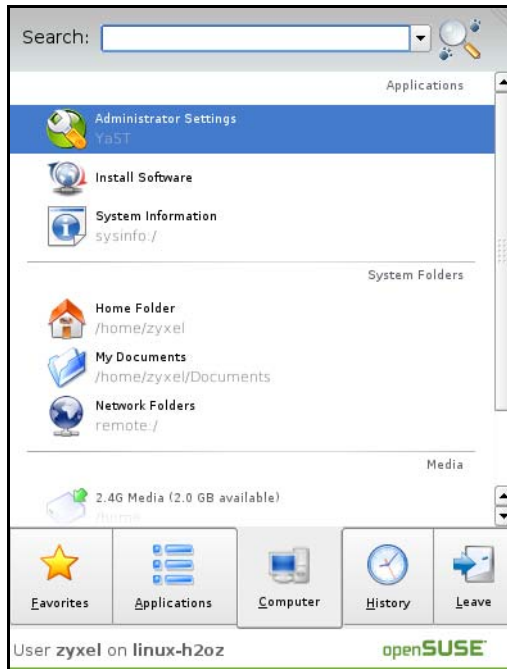
Linux: openSUSE 10.3 (KDE)

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:

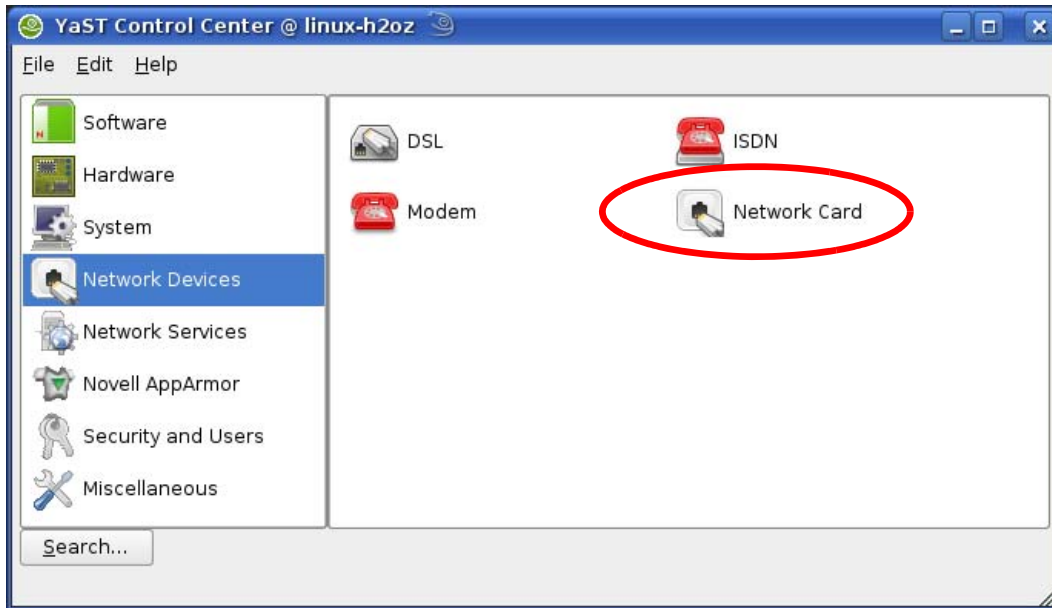
- 1 Click **K Menu > Computer > Administrator Settings (YaST)**.



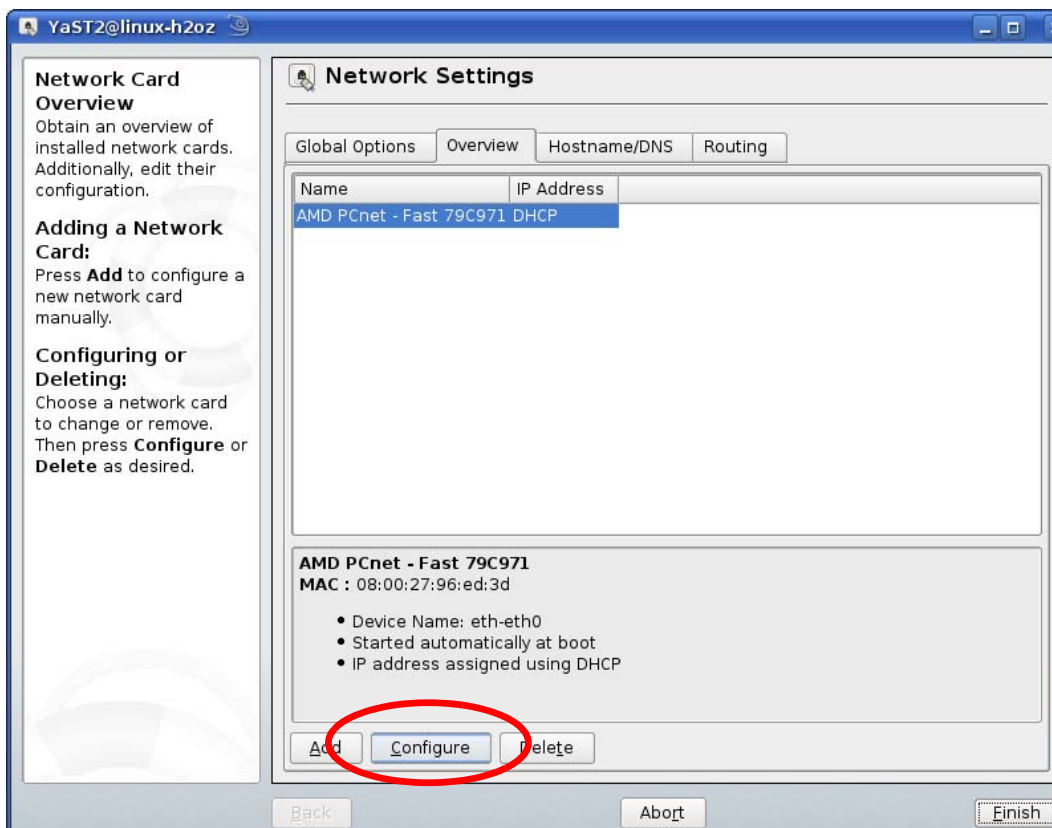
- 2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.



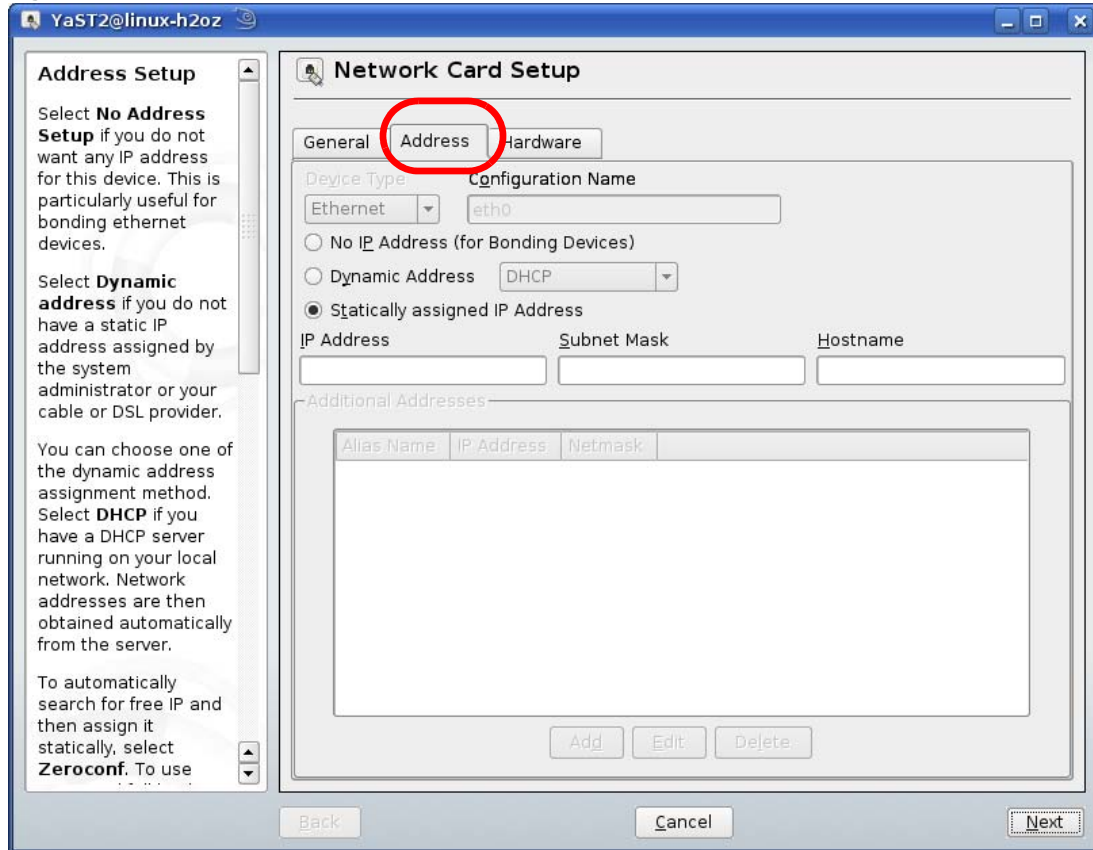
- 3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.



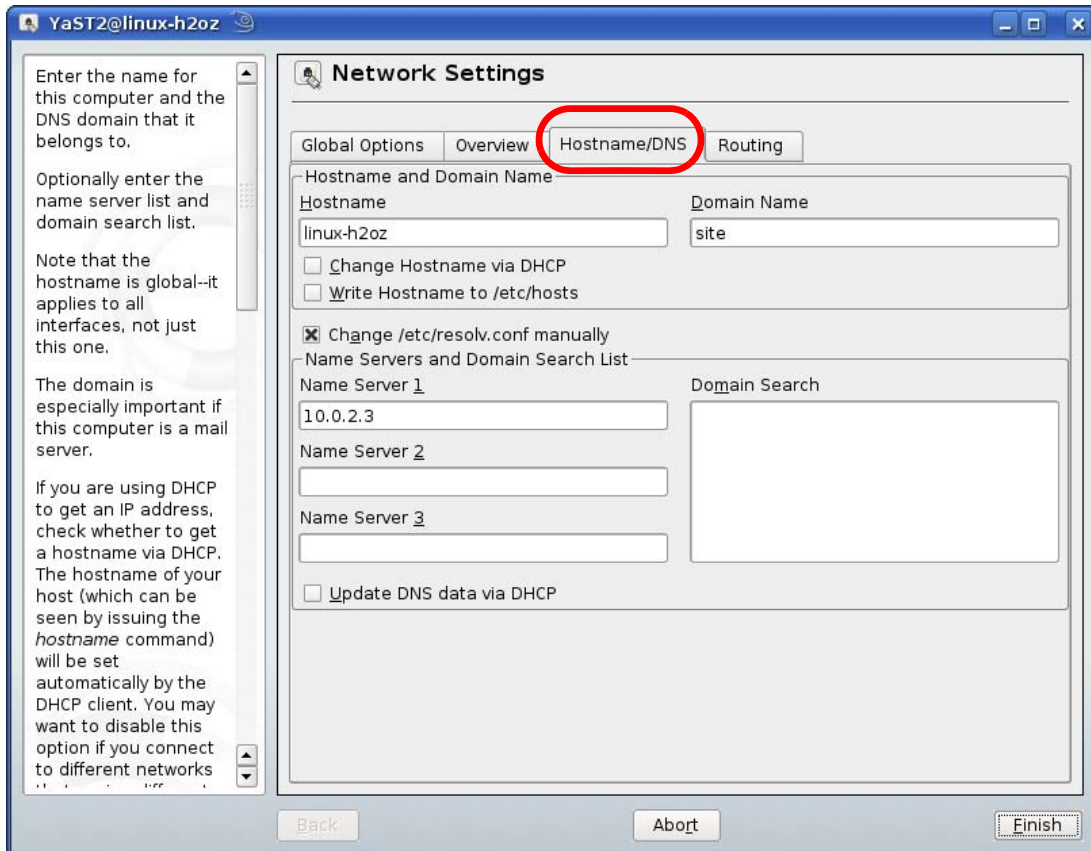
- 4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.



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

Figure 175 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.

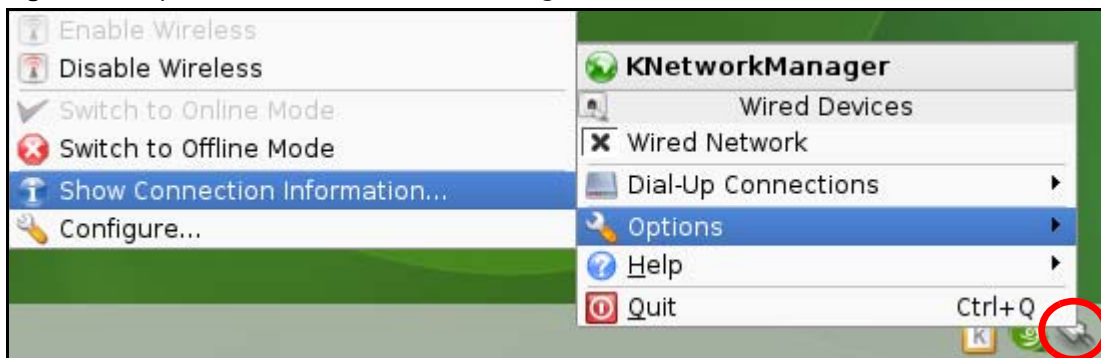


- 9 Click **Finish** to save your settings and close the window.

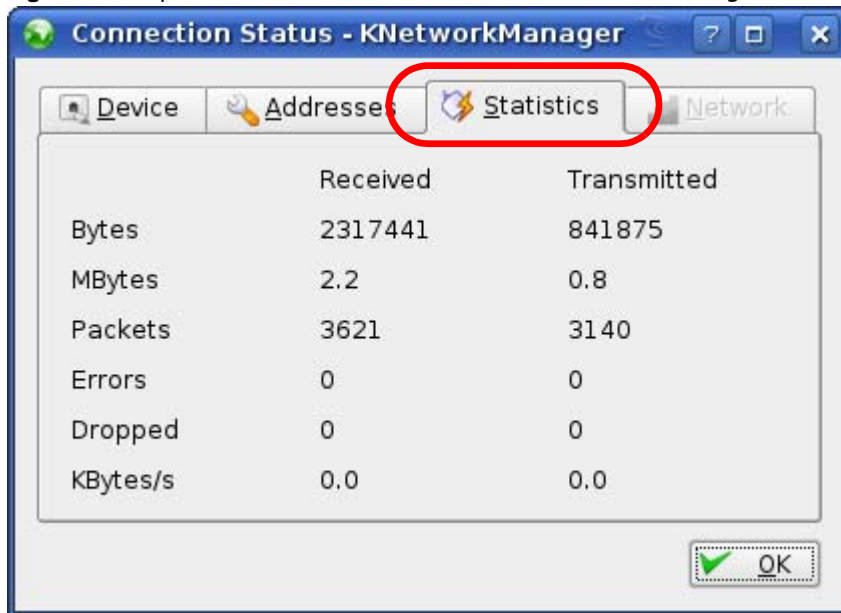
Verifying Settings

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 176 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 177 openSUSE: Connection Status - KNetwork Manager

Wireless LANs

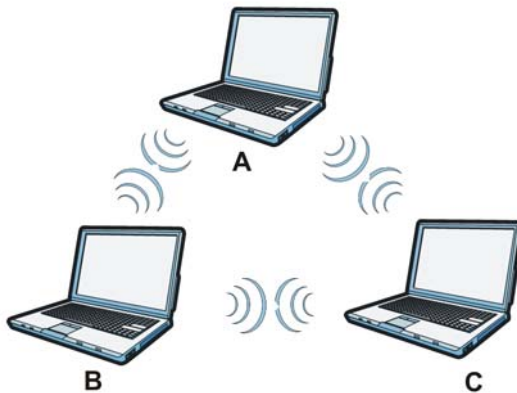
Wireless LAN Topologies

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.

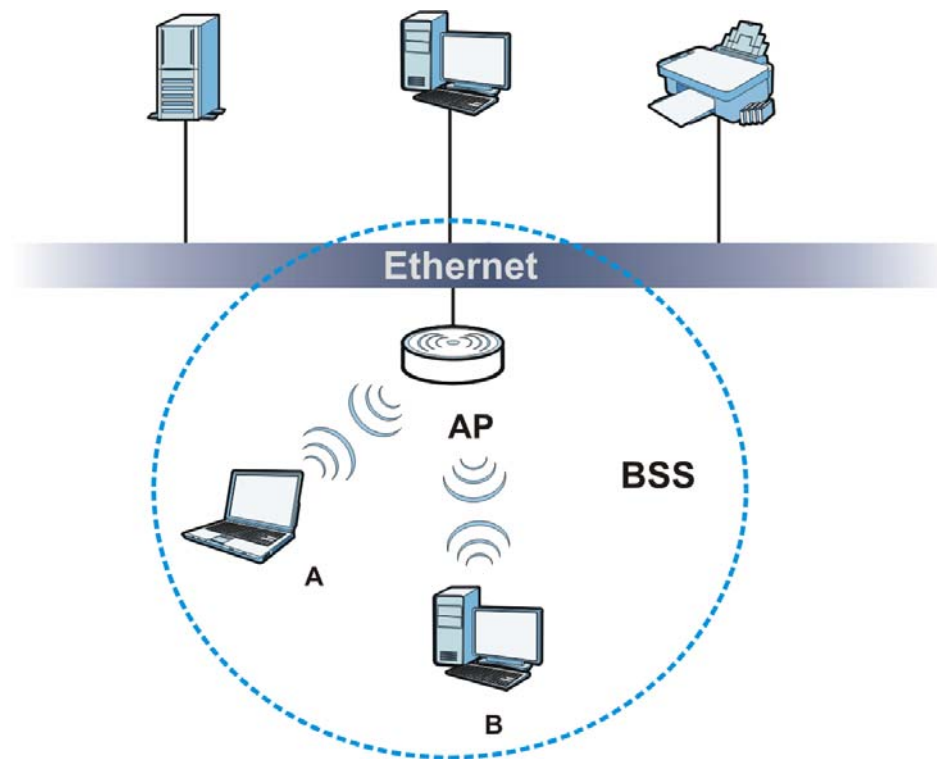
Figure 178 Peer-to-Peer Communication in an Ad-hoc Network



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.

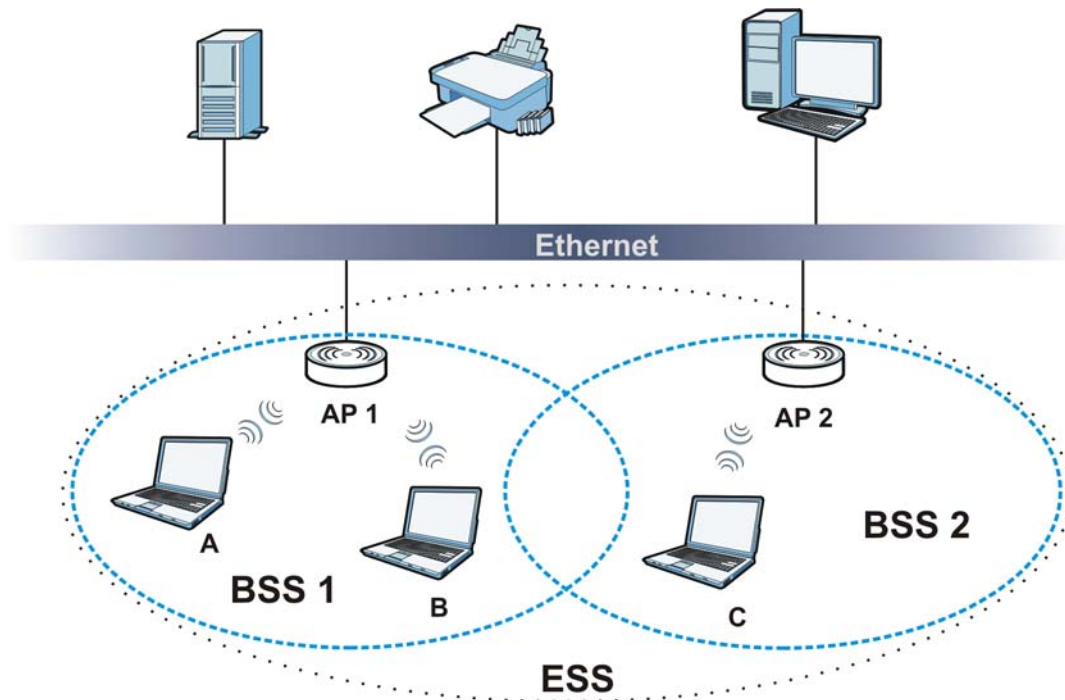
Figure 179 Basic Service Set

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 180 Infrastructure WLAN

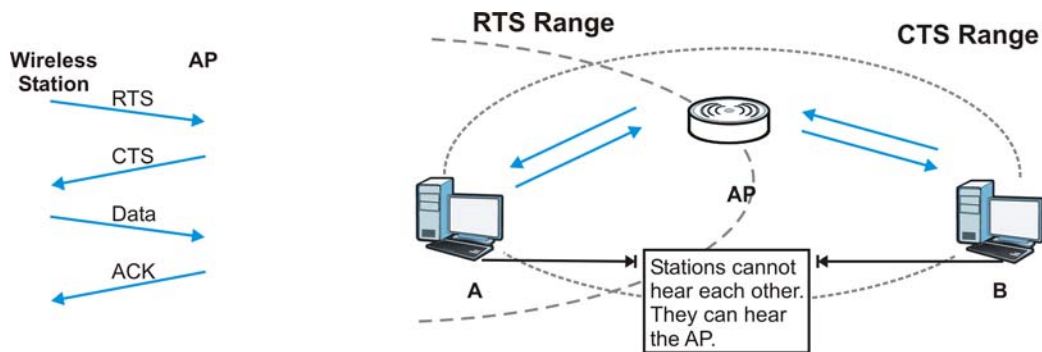
Channel

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 181 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 NBG4615 v2 uses long preamble.

Note: The wireless devices **MUST** use the same preamble mode in order to communicate.

Wireless LAN Standards

The IEEE 802.11b wireless access standard was first published in 1999. IEEE 802.11b has a maximum data rate of 11 Mbps and uses the 2.4 GHz band.

IEEE 802.11g also works in the 2.4 GHz band and 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 (54 Mbps and 1 Mbps respectively).

IEEE 802.11a has a data rate of up to 54 Mbps using the 5 GHz band. IEEE 802.11a is not interoperable with IEEE 802.11b or IEEE 802.11g.

IEEE 802.11n can operate both in the 2.4 GHz and 5 GHz bands and is backward compatible with the IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g standards. It improves network throughput and increases the maximum raw data rate from 54 Mbps to 300 Mbps by using multiple-input multiple-output (MIMO), a channel width of 40 MHz, frame aggregation and short guard interval.

Table 105 Wireless LAN Standards Comparison Table

WIRELESS LAN STANDARD	MAXIMUM NET DATA RATE	FREQUENCY BAND	COMPATIBILITY
IEEE 802.11b	11 Mbps	2.4 GHz	IEEE 802.11g IEEE 802.11n
IEEE 802.11g	54 Mbps	2.4 GHz	IEEE 802.11b IEEE 802.11n
IEEE 802.11a	54 Mbps	5 GHz	IEEE 802.11n
IEEE 802.11n	300 Mbps	2.4 GHz, 5 GHz	IEEE 802.11b IEEE 802.11g IEEE 802.11a

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 NBG4615 v2 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the NBG4615 v2 identity.

The following figure shows the relative effectiveness of these wireless security methods available on your NBG4615 v2.

Table 106 Wireless Security Levels

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

Note: You must enable the same wireless security settings on the NBG4615 v2 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 107 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

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

Encryption

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

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

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

User Authentication

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

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

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

Wireless Client WPA Supplicants

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

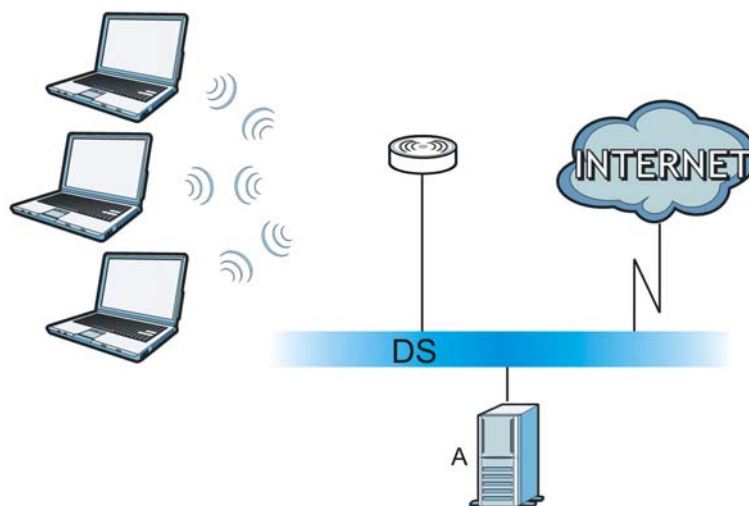
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
- 4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 182 WPA(2) with RADIUS Application Example

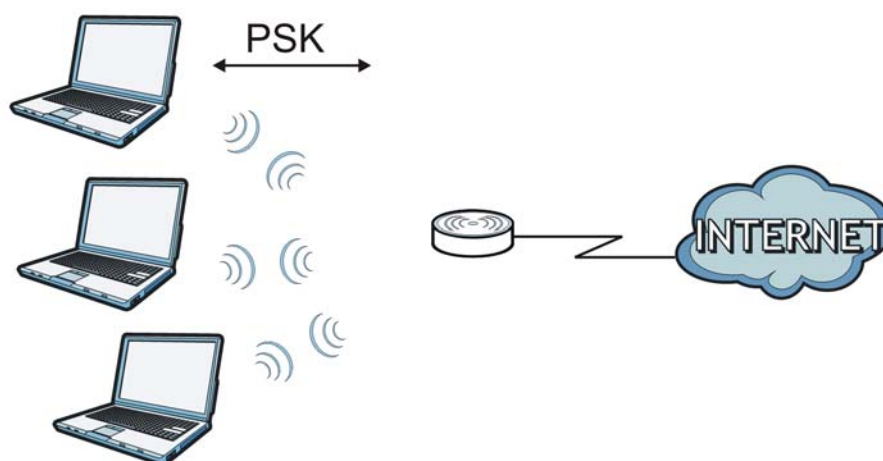


WPA(2)-PSK Application Example

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 183 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 108 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

Table 108 Wireless Security Relational Matrix (continued)

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
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 109 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 109 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 109 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.

Legal Information

Copyright

Copyright © 2012 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

NetUSB is a trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- 1 Reorient or relocate the receiving antenna.
- 2 Increase the separation between the equipment and the receiver.
- 3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4 Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.



FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b, 802.11g or 802.11n (20MHz) operation of this product in the U.S.A. is firmware-limited to channels 1 through 11. IEEE 802.11n (40MHz) operation of this product in the U.S.A. is firmware-limited to channels 3 through 9.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

- 1) this device may not cause interference and
- 2) this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IC Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

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。

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.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. 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.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Regulatory Information

European Union

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

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

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

[Czech]	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
[Danish]	Undertegnede ZyXEL erklærer herved, at følgende udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
[German]	Hiermit erkläre ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
[Estonian]	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

[English]	Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[Spanish]	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
[Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ΖΥΧΕΛ ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΠΛΙΣΜΟΣ ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
[French]	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
[Italian]	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
[Latvian]	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[Lithuanian]	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[Dutch]	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
[Maltese]	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-htigijiet essenzjali u ma provvimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
[Hungarian]	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK irányelv egyéb előírásainak.
[Polish]	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[Portuguese]	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
[Slovenian]	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
[Slovak]	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
[Finnish]	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[Swedish]	Härmed intygar ZyXEL att denna utrustning står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
[Bulgarian]	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/EC.
[Icelandic]	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
[Norwegian]	Erklærer herved ZyXEL at dette utstyret er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 1999/5/EF.
[Romanian]	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 1999/5/EC.



National Restrictions

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

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

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

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1999/5/EC folgen) mit Ausnahme der folgenden aufgeführten Staaten:

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

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

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

Overview of Regulatory Requirements for Wireless LANs			
Frequency Band (MHz)	Max Power Level (EIRP) ¹ (mW)	Indoor ONLY	Indoor and Outdoor
2400-2483.5	100		✓
5150-5350	200	✓	
5470-5725	1000		✓

Belgium

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

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

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

Denmark

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

I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.

France

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

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

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

Italy

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

Questo prodotto è conforme alla specifiche di interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare <http://www.sviluppoeconomico.gov.it/> per maggiori dettagli.

Latvia

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

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

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Malta	MT
Belgium	BE	Netherlands	NL
Cyprus	CY	Poland	PL
Czech Republic	CR	Portugal	PT
Denmark	DK	Slovakia	SK
Estonia	EE	Slovenia	SI
Finland	FI	Spain	ES
France	FR	Sweden	SE
Germany	DE	United Kingdom	GB
Greece	GR	Iceland	IS
Hungary	HU	Liechtenstein	LI
Ireland	IE	Norway	NO
Italy	IT	Switzerland	CH
Latvia	LV	Bulgaria	BG
Lithuania	LT	Romania	RO
Luxembourg	LU	Turkey	TR

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

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



Index

A

ActiveX [190](#)
 Address Assignment [126](#)
 Advanced Encryption Standard
 See AES.
 AES [288](#)
 alternative subnet mask notation [243](#)
 antenna
 directional [292](#)
 gain [291](#)
 omni-directional [291](#)
 AP [15](#)
 AP (access point) [281](#)
 AP Mode
 menu [67, 75, 85, 96](#)
 status screen [65](#)
 AP+Bridge [15](#)

B

Bandwidth management
 overview [193](#)
 priority [195](#)
 services [199](#)
 Basic Service Set, See BSS [279](#)
 BitTorrent [199](#)
 Bridge/Repeater [15](#)
 BSS [279](#)

C

CA [286](#)
 Certificate Authority
 See CA.
 certifications [297](#)
 notices [298](#)
 viewing [298](#)

Channel [59, 66, 74, 84, 95](#)
 channel [136, 281](#)
 interference [281](#)
 Configuration
 restore [216](#)
 content filtering [189](#)
 by keyword (in URL) [189](#)
 Cookies [190](#)
 copyright [297](#)
 CPU usage [59, 66, 74, 85, 95](#)
 CTS (Clear to Send) [282](#)

D

Daylight saving [214](#)
 DDNS [177](#)
 see also Dynamic DNS
 service providers [177](#)
 DHCP [120, 161](#)
 DHCP server
 see also Dynamic Host Configuration Protocol
 DHCP server [158, 161](#)
 disclaimer [297](#)
 DNS [163](#)
 DNS Server [126](#)
 DNS server [163](#)
 documentation
 related [2](#)
 Domain Name System [163](#)
 Domain Name System. See DNS.
 duplex setting [60, 67, 85, 95](#)
 Dynamic DNS [177](#)
 Dynamic Host Configuration Protocol [161](#)
 dynamic WEP key exchange [287](#)
 DynDNS [177](#)
 DynDNS see also DDNS [177](#)

E

EAP Authentication [285](#)
encryption [137, 288](#)
 and local (user) database [138](#)
 key [138](#)
 WPA compatible [138](#)
ESS [280](#)
ESSID [228](#)
Extended Service Set, See ESS [280](#)

F

FCC interference statement [297](#)
File Transfer Program [199](#)
Firewall [184](#)
 Firewall overview
 guidelines [184](#)
 ICMP packets [185](#)
 network security
 Stateful inspection [184](#)
 ZyXEL device firewall [184](#)
firewall
 stateful inspection [183](#)
Firmware upload [214](#)
 file extension
 using HTTP
firmware version [59, 66](#)
fragmentation threshold [282](#)
FTP. see also File Transfer Program [199](#)

G

General wireless LAN screen [140](#)
Guest WLAN [138](#)
Guest WLAN Bandwidth [139](#)
Guide
 Quick Start [2](#)

H

hidden node [281](#)

HTTP [199](#)
Hyper Text Transfer Protocol [199](#)

I

IANA [248](#)
IBSS [279](#)
IEEE 802.11g [283](#)
IGMP [127](#)
 see also Internet Group Multicast Protocol
 version
IGMP version [127](#)
Independent Basic Service Set
 See IBSS [279](#)
initialization vector (IV) [288](#)
Internet Assigned Numbers Authority
 See IANA [248](#)
Internet Group Multicast Protocol [127](#)
IP Address [159, 160, 170](#)
IP alias [158](#)
IP Pool [162](#)

J

Java [190](#)

L

LAN [157](#)
 IP pool setup [158](#)
LAN overview [157](#)
LAN setup [157](#)
LAN TCP/IP [158](#)
Language [217](#)
Link type [60, 66, 74, 85, 95](#)
local (user) database [137](#)
 and encryption [138](#)
Local Area Network [157](#)

M

- MAC [150](#)
- MAC address [126](#), [137](#)
 - cloning [126](#)
- MAC address filter [137](#)
- MAC address filtering [150](#)
- MAC filter [150](#)
- managing the device
 - good habits [16](#)
 - using the web configurator. See web configurator.
 - using the WPS. See WPS.
- MBSSID [15](#)
- Media access control [150](#)
- Memory usage [59](#), [66](#), [74](#), [85](#), [95](#)
- Message Integrity Check (MIC) [288](#)
- mode [15](#)
- Multicast [127](#)
 - IGMP [127](#)

N

- NAT [167](#), [170](#), [248](#)
 - global [168](#)
 - how it works [169](#)
 - inside [168](#)
 - local [168](#)
 - outside [168](#)
 - overview [167](#)
 - port forwarding [174](#)
 - see also Network Address Translation
 - server [168](#)
 - server sets [174](#)
- NAT Traversal [205](#)
- Navigation Panel [60](#), [67](#), [75](#), [85](#), [96](#)
- navigation panel [60](#), [67](#), [75](#), [85](#), [96](#)
- Network Address Translation [167](#), [170](#)

O

- operating mode [15](#)
- other documentation [2](#)

P

- P2P [199](#)
- Pairwise Master Key (PMK) [288](#), [290](#)
- peer-to-peer [199](#)
- Point-to-Point Protocol over Ethernet [129](#)
- Point-to-Point Tunneling Protocol [131](#)
- Pool Size [162](#)
- Port forwarding [170](#), [174](#)
 - default server [170](#), [174](#)
 - example [174](#)
 - local server [170](#)
 - port numbers
 - services
- port speed [60](#), [67](#), [75](#), [85](#), [95](#)
- PPPoE [129](#)
 - dial-up connection
- PPTP [131](#)
- preamble mode [283](#)
- product registration [298](#)
- PSK [288](#)

Q

- Quality of Service (QoS) [152](#)
- Quick Start Guide [2](#)

R

- RADIUS [284](#)
 - message types [285](#)
 - messages [285](#)
 - shared secret key [285](#)
- RADIUS server [137](#)
- registration
 - product [298](#)
- related documentation [2](#)
- Remote management
 - and NAT [202](#)
 - limitations [201](#)
 - system timeout [202](#)
- Reset button [16](#)
- Reset the device [16](#)

Restore configuration [216](#)
Roaming [152](#)
Router Mode
 status screen [57](#)
RTS (Request To Send) [282](#)
 threshold [281, 282](#)
RTS/CTS Threshold [136, 152](#)

S

Scheduling [155](#)
Service and port numbers [187, 198](#)
Service Set [53, 140, 149](#)
Service Set IDentification [53, 140, 149](#)
Service Set IDentity. See SSID.
Session Initiated Protocol [199](#)
SIP [199](#)
SSID [53, 59, 66, 74, 84, 95, 136, 140, 149](#)
stateful inspection firewall [183](#)
Static DHCP [162](#)
Static Route [179](#)
Status [57](#)
subnet [241](#)
Subnet Mask [159, 160](#)
subnet mask [242](#)
subnetting [244](#)
Summary
 DHCP table [120](#)
 Packet statistics [121](#)
 Wireless station status [122](#)
System General Setup [211](#)
System restart [217](#)

T

TCP/IP configuration [161](#)
Temporal Key Integrity Protocol (TKIP) [288](#)
Time setting [213](#)
trademarks [297](#)
trigger port [175](#)
Trigger port forwarding [175](#)
 example [175](#)

process [175](#)

U

Universal [71](#)
Universal Plug and Play [205](#)
 Application [205](#)
 Security issues [205](#)
Universal Repeater [71, 75](#)
Universal Repeater Mode
 status screen [73](#)
UPnP [205](#)
URL Keyword Blocking [190](#)
user authentication [137](#)
 local (user) database [137](#)
 RADIUS server [137](#)
User Name [178](#)

V

VoIP [199](#)
VPN [131](#)

W

Wake On LAN [203](#)
WAN (Wide Area Network) [125](#)
WAN MAC address [126](#)
warranty [298](#)
 note [298](#)
Web Configurator
 how to access [39](#)
 Overview [39](#)
web configurator [15](#)
Web Proxy [190](#)
WEP Encryption [76, 77, 78, 87, 88, 143, 145](#)
WEP encryption [142](#)
WEP key [143](#)
Wi-Fi Protected Access [287](#)
Wireless association list [122](#)
wireless channel [228](#)

wireless client WPA supplicants [289](#)
wireless LAN [228](#)
wireless LAN scheduling [155](#)
Wireless network
 basic guidelines [136](#)
 channel [136](#)
 encryption [137](#)
 example [135](#)
 MAC address filter [137](#)
 overview [135](#)
 security [136](#)
 SSID [136](#)
Wireless security [136](#)
 overview [136](#)
 type [136](#)
wireless security [228](#), [284](#)
Wireless tutorial [97](#)
WISP Mode
 status screen [83](#), [93](#)
Wizard setup [27](#)
WLAN
 interference [281](#)
 security parameters [290](#)
WLAN button [16](#)
WoL [203](#)
World Wide Web [199](#)
WPA [287](#)
 key caching [288](#)
 pre-authentication [288](#)
 user authentication [288](#)
 vs WPA-PSK [288](#)
 wireless client supplicant [289](#)
 with RADIUS application example [289](#)
WPA compatible [138](#)
WPA2 [287](#)
 user authentication [288](#)
 vs WPA2-PSK [288](#)
 wireless client supplicant [289](#)
 with RADIUS application example [289](#)
WPA2-Pre-Shared Key [287](#)
WPA2-PSK [287](#), [288](#)
 application example [289](#)
WPA-PSK [287](#), [288](#)
 application example [289](#)
WPS [15](#)
WWW [199](#)

X

Xbox Live [199](#)

