ZYXEL
Your Networking Ally

DRAFT

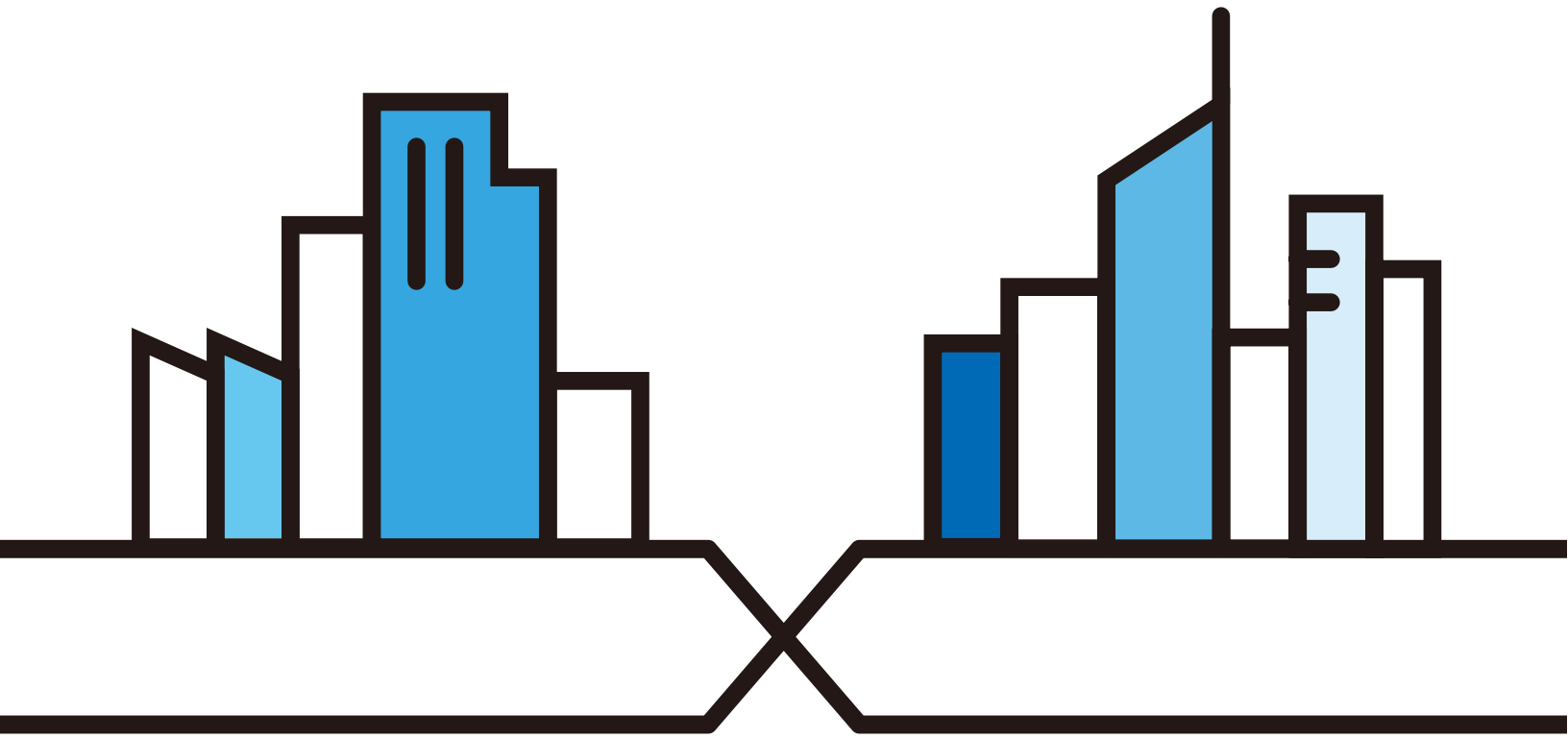
User's Guide

ARMOR G1

AC2600 Multi-Gigabit Security WiFi Router
Model: NBG6818

Default Login Details	
LAN IP Address	http://zyxelwifi.com
Password	12345678

Version 1.00 Edition 1, 12/2019



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 NBG6818 and access the Web Configurator wizards. It contains information on setting up your network and configuring for Internet access.

- More Information

  Go to **support.zyxel.com** to find other information on the NBG6818.

Contents Overview

User's Guide **9**

Introduction 10
eaZy 123 Wizard 16
NBG6818 Modes 25
Easy Mode 26
Router Mode 34
Access Point Mode 40
Tutorials 47

Technical Reference **53**

The Web Configurator 54
Applications 57
WAN 71
Wireless LAN 94
LAN 105
Security 112
System 119
Troubleshooting 128

Table of Contents

Contents Overview 3

Table of Contents 4

Part I: User's Guide 9

Chapter 1
Introduction 10

1.1 Overview 10
1.2 Applications 10
1.3 Ways to Manage the NBG6818 10
1.4 Good Habits for Managing the NBG6818 11
1.5 Resetting the NBG6818 11
1.5.1 How to Use the RESET Button 11
1.6 The WPS Button 11
1.7 LEDs 12
1.8 Wall Mounting 14

Chapter 2
eaZy 123 Wizard 16

2.1 Overview 16
2.2 Accessing the eaZy 123 Wizard 16
2.3 Internet Type 18
2.3.1 WAN Selection Type: Automatic - DHCP 19
2.3.2 WAN Selection Type: PPPoE 19
2.3.3 WAN Selection Type: Static 20
2.4 Wireless Network 21

Chapter 3
NBG6818 Modes 25

3.1 Overview 25
3.1.1 Web Configurator Modes 25
3.1.2 Device Modes 25

Chapter 4
Easy Mode 26

4.1 Overview 26
4.2 What You Can Do 26

4.3 What You Need to Know 27
4.4 Navigation Panel 27
4.5 Network Map 28
4.6 Control Panel 29
4.6.1 Wi-Fi 30
4.6.2 Guest Wi-Fi 31
4.6.3 Parental Control 32
4.6.4 Notification 33
4.6.5 LED 33

Chapter 5
Router Mode 34

5.1 Overview 34
5.2 Router Mode Status Screen 34
5.2.1 Navigation Panel 37

Chapter 6
Access Point Mode 40

6.1 Overview 40
6.2 What You Can Do 40
6.3 What You Need to Know 40
6.3.1 Setting your NBG6818 to AP Mode 40
6.3.2 Accessing the Web Configurator in Access Point Mode 41
6.3.3 Configuring your WLAN and Maintenance Settings 42
6.4 AP Mode Status Screen 42
6.4.1 Navigation Panel 44
6.5 LAN Screen 44

Chapter 7
Tutorials 47

7.1 Overview 47
7.2 Run a Speed Test 47
7.3 Configure the NBG6818's WiFi Networks 48
7.4 Enable or Disable a WiFi Network 50
7.5 Add Clients to a Profile 51

Part II: Technical Reference 53

Chapter 8
The Web Configurator 54

8.1 Overview 54

8.2 Accessing the Web Configurator 54
8.3 Add and Install Your NBG6818 56

Chapter 9
Applications 57

9.1 Overview 57
9.1.1 What You Can Do 57
9.1.2 What You Need To Know 57
9.1.3 Before You Begin 58
9.2 Parental Control Screen 58
9.2.1 Device Screen 58
9.3 OpenVPN Server Screen 62
9.4 OpenVPN Client Screen 62
9.5 USB Application Screen 62
9.5.1 SAMBA Server Screen 62
9.5.2 FTP Server Screen 65
9.5.3 USB Media Sharing Screen 67
9.6 Access Your Shared Files From a Computer 69
9.6.1 Using Windows Explorer 69
9.6.2 Using FTP Program 69

Chapter 10
WAN 71

10.1 Overview 71
10.2 What You Can Do 71
10.3 What You Need To Know 72
10.3.1 Configuring Your Internet Connection 72
10.4 Internet Connection Screen 73
10.4.1 IPoE Encapsulation 73
10.4.2 PPPoE Encapsulation 76
10.4.3 PPTP Encapsulation 79
10.5 NAT & Port Forwarding Screen 81
10.5.1 Add Port Forwarding Rule Screen 82
10.6 Passthrough Screen 83
10.7 Port Trigger Screen 85
10.7.1 Add Port Trigger Rule Screen 86
10.8 Dynamic DNS Screen 87
10.9 UPnP Screen 88
10.9.1 Turning On UPnP in Windows 7 Example 89
10.9.2 Turning on UPnP in Windows 10 Example 91

Chapter 11
Wireless LAN 94

11.1 Overview 94
11.1.1 What You Can Do 94
11.1.2 What You Should Know 95
11.2 Main WiFi Screen 98
11.3 Guest WiFi Screen 99
11.4 MAC Filter Screen 100
11.4.1 Add MAC Address Screen 101
11.5 WPS Screen 102
11.6 Scheduling Screen 104

Chapter 12
LAN 105

12.1 Overview 105
12.2 What You Can Do 105
12.3 What You Need To Know 105
12.4 LAN IP Screen 106
12.4.1 Static DHCP Table-Add/Edit Rule Screen 108
12.5 IPv6 LAN Screen 110

Chapter 13
Security 112

13.1 Overview 112
13.1.1 What You Can Do 112
13.1.2 What You Need To Know 112
13.2 IPv4 Firewall Screen 113
13.2.1 IPv4 Firewall-Add Rule Screen 115
13.3 IPv6 Firewall Screen 116
13.3.1 IPv6 Firewall-Add Rule Screen 117

Chapter 14
System 119

14.1 Overview 119
14.2 What You Can Do 119
14.3 Status Screen 119
14.4 General Setting Screen 121
14.5 Remote Access Screen 122
14.6 Maintenance Screen 124
14.7 Operating Mode Screen 125
14.8 Logs Screen 126

Chapter 15
Troubleshooting 128

15.1 Overview 128

15.2 Power, Hardware Connections, and LEDs 128
15.3 NBG6818 Access and Login 129
15.4 Internet Access 130
15.5 Resetting the NBG6818 to Its Factory Defaults 132
15.6 Wireless Connections 132
15.7 USB Device Problems 134

Appendix A Customer Support 135

Appendix B Setting Up Your Computer's IP Address 141

Appendix C Common Services 161

Appendix D Legal Information 164

Index 171

PART I
User's Guide

CHAPTER 1 Introduction

1.1 Overview

This chapter introduces the main features and applications of the NBG6818.

The NBG6818 extends the range of your existing wired network without additional wiring, providing easy network access to mobile users. You can set up a wireless network with other IEEE 802.11a/b/g/n/ac compatible devices. The NBG6818 is able to function both 2.4GHz and 5GHz networks at the same time.

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

There are two USB ports on the side panel of your NBG6818. One is USB 2.0, and the other is USB 3.0. You can connect USB memory sticks, USB hard drives, or USB devices for file sharing. The NBG6818 automatically detects the USB devices.

1.2 Applications

Your can have the following networks with the NBG6818:

- **Wired**. You can connect network devices via the Ethernet ports of the NBG6818 so that they can communicate with each other and access the Internet.
- **Wireless**. Wireless clients can connect to the NBG6818 to access network resources. You can use WPS (Wi-Fi Protected Setup) to create an instant network connection with another WPS-compatible device.
- **WAN**. Connect to a broadband modem/router for Internet access.

1.3 Ways to Manage the NBG6818

Use any of the following methods to manage the NBG6818.

- 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 NBG6818.
- Web Configurator. This is recommended for everyday management of the NBG6818 using a (supported) web browser.

1.4 Good Habits for Managing the NBG6818

Do the following things regularly to make the NBG6818 more secure and to manage the NBG6818 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 NBG6818 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG6818. You could simply restore your last configuration.

1.5 Resetting the NBG6818

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 NBG6818 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 NBG6818.
3. Press the **RESET** button for longer than five seconds to set the NBG6818 back to its factory-default configurations.

1.6 The WPS Button

Your NBG6818 supports Wi-Fi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the Wi-Fi 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 rear panel of the NBG6818 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).

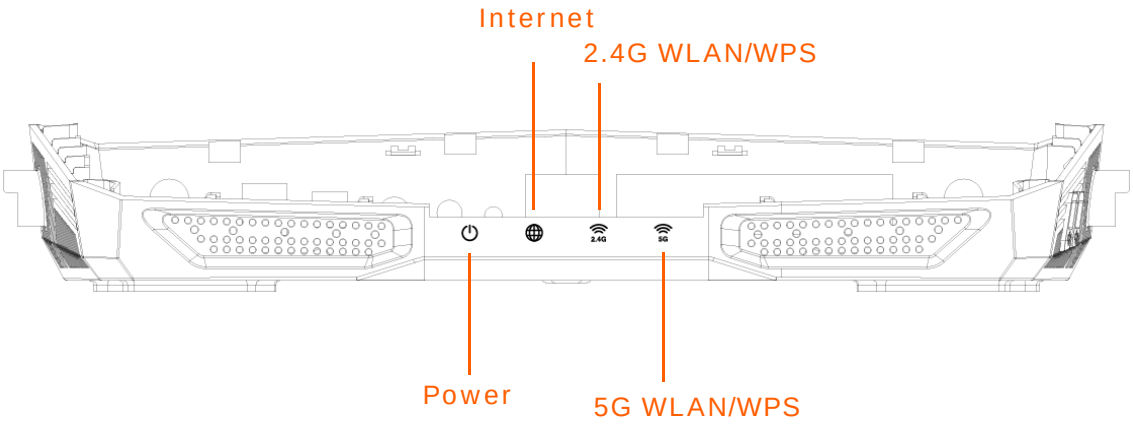
2 Press the WPS button for more than three seconds and release it. Press the WPS button on another WPS-enabled device within range of the NBG6818.

Note: You must activate WPS in the NBG6818 and in another wireless device within two minutes of each other.

For more information on using WPS, see Section 7.2 on page 47.

1.7 LEDs

Figure 1 Front Panel



The following table describes the front panel LEDs.

Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
Power/System	White	On	The NBG6818 is receiving power and functioning properly.
		Blinking	The NBG6818 is in the process of starting up, default restoring, or myZyxelCloud online registration pairing.
		Off	The NBG6818 is not receiving power.
Internet	White	On	The NBG6818 has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the connection is up.
		Blinking	The NBG6818 is sending or receiving IP traffic.
		Off	The NBG6818 does not have an IP connection.

Table 1 Front Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
5G WLAN/WPS	White	On	The NBG6818 is ready and the 5GHz wireless LAN is on, but is not sending/receiving data through the wireless LAN.
		Blinking	The NBG6818 is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
	Amber	On	WPS is enabled. The NBG6818 is in the process of firmware upgrading, configuration restoring, or resetting.
		Blinking	The NBG6818 is negotiating a WPS connection with a wireless client.
		Off	WPS is disabled.
2.4G WLAN/WPS	White	On	The NBG6818 is ready and the 2.4GHz wireless LAN is on, but is not sending/receiving data through the wireless LAN.
		Blinking	The NBG6818 is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
	Amber	On	WPS is enabled. The NBG6818 is in the process of firmware upgrading, configuration restoring, or resetting.
		Blinking	The NBG6818 is negotiating a WPS connection with a wireless client.
		Off	WPS is disabled.

Figure 2 Rear Panel

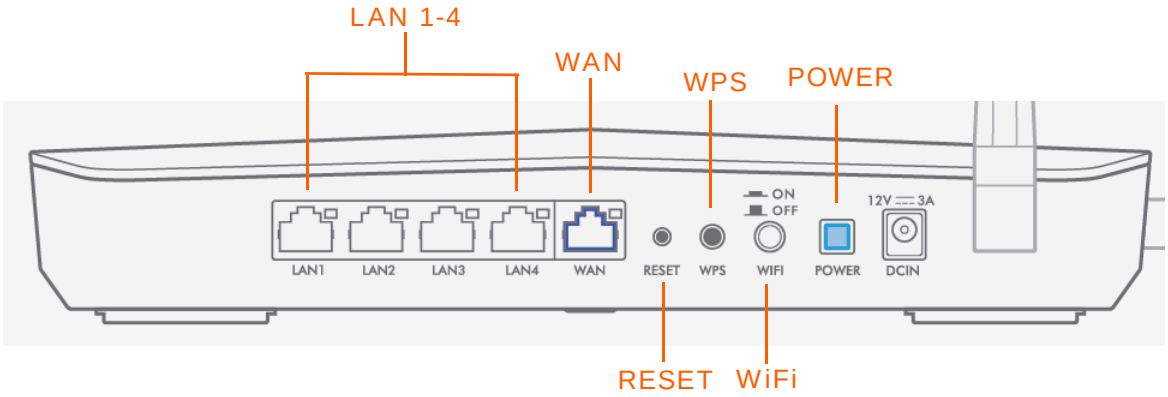
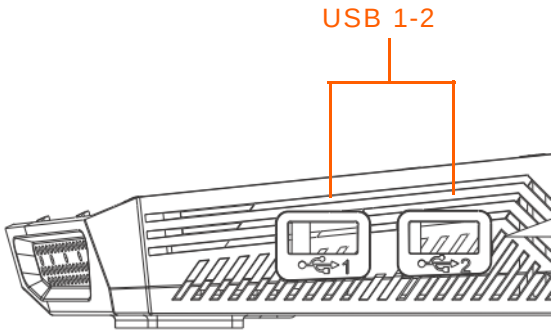


Figure 3 Side Panel\



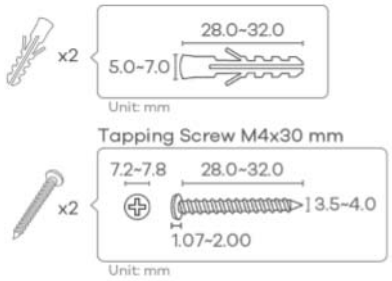
1.8 Wall Mounting

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

Table 2 Wall Mounting Information

Distance between holes	10.50 cm
M4 Screws	Two
Screw anchors (optional)	Two

Figure 4 Screw Specifications



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.

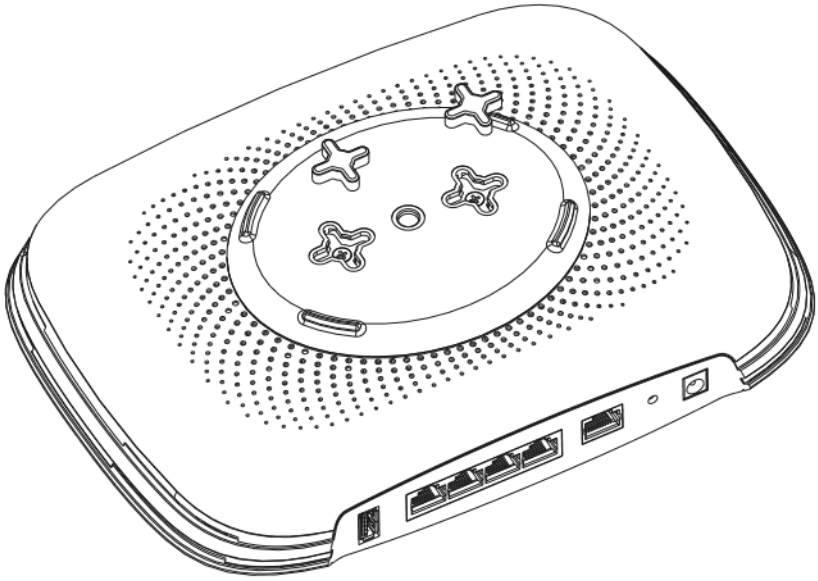
If not using screw anchors, use a screwdriver to insert the screws into the wall. Do not insert the screws all the way in - leave a gap of about 0.5 cm.

4 Make sure the screws are fastened well enough to hold the weight of the NBG6615 with the connection cables.

5 Take out the rubber foots at the back panel.

6 Align the holes on the back of the NBG6818 with the screws on the wall. Hang the NBG6818 on the screws.

Figure 5 Wall Mounting Example



CHAPTER 2
eaZy 123 Wizard

2.1 Overview

This chapter provides information on the eaZy 123 setup screens in the Web Configurator.

The Web Configurator's eaZy 123 setup wizard helps you configure your device to access the Internet. Refer to your ISP for your Internet account information. Leave a field blank if you don't have that information.

2.2 Accessing the eaZy 123 Wizard

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

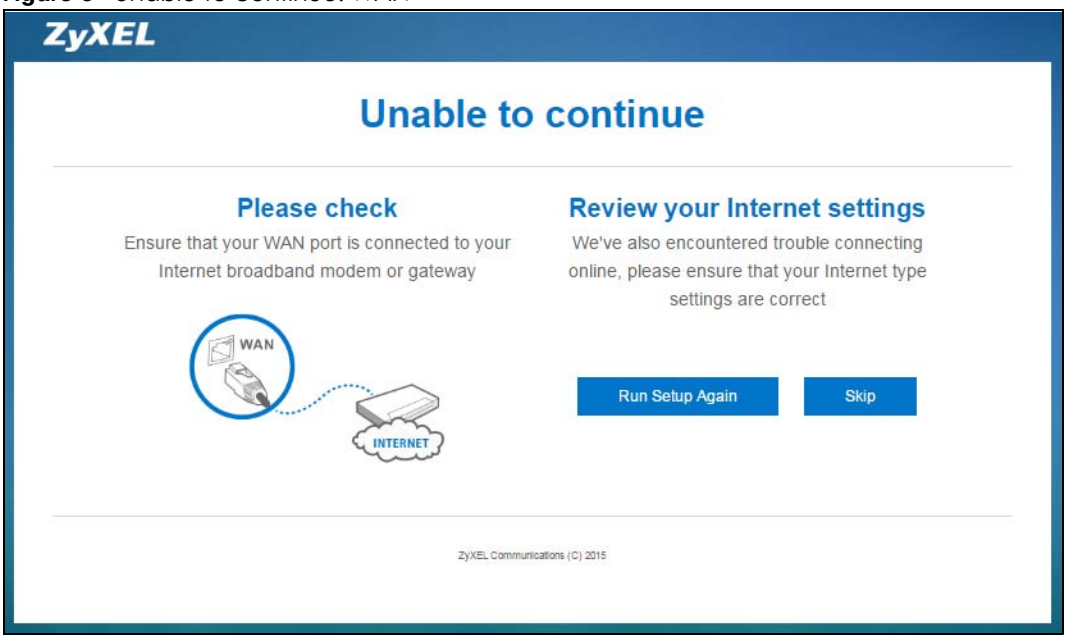
Note: The eaZy 123 wizard appears automatically when the NBG6818 is accessed for the first time or when you reset the NBG6818 to its default factory settings. If you didn't configure the wizard screens, you will be redirected to the login page when you connect to the Internet.

If you have already configured the wizard screens and want to open it again, click  on the upper right corner of any Web Configurator screen. The eaZy 123 wizard attempts to detect which WAN connection type you are using.

If the eaZy 123 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.

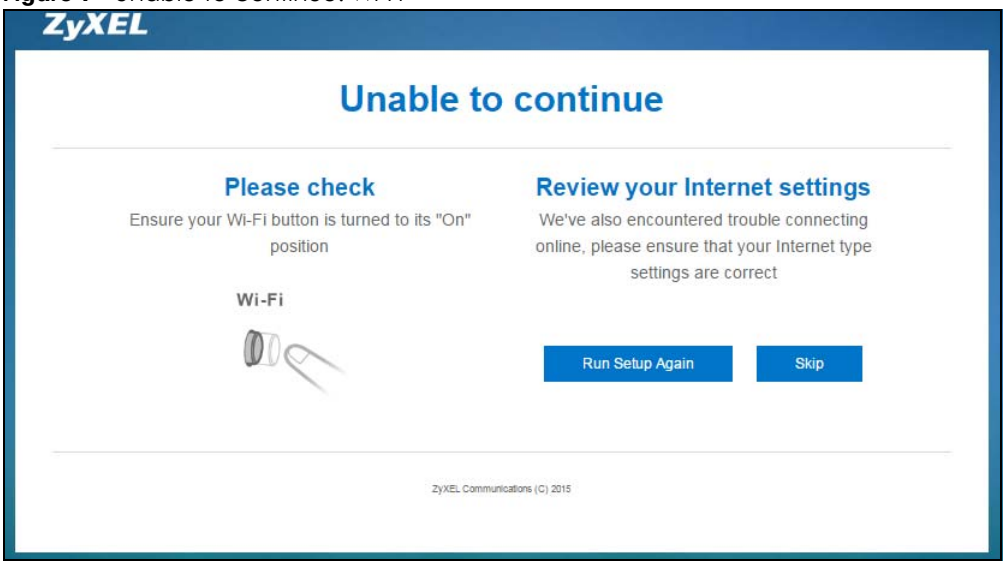
If you do not have the Internet connection, the following screen opens.

Figure 6 Unable to continue: WAN



If you do not press the Wi-Fi button located on the NBG6818's back panel, the following screen opens.

Figure 7 Unable to continue: Wi-Fi



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

The wizard screen opens.

Figure 8 Detecting your Internet Connection Type

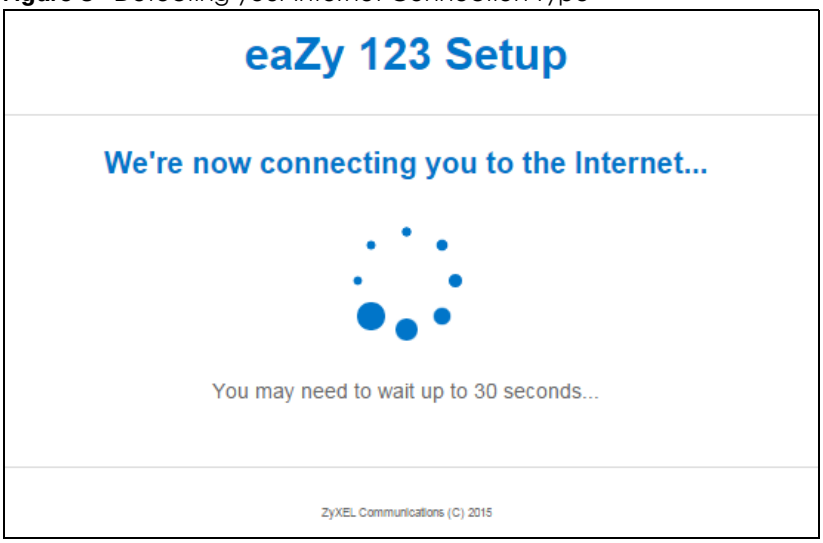
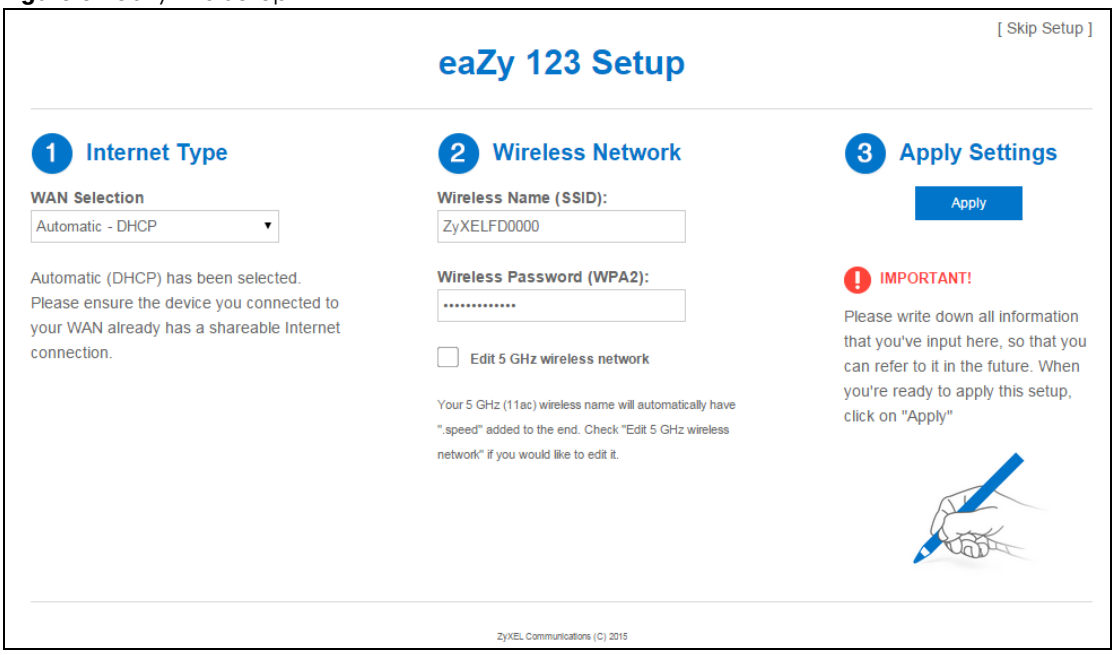


Figure 9 eaZy 123 Setup



2.3 Internet Type

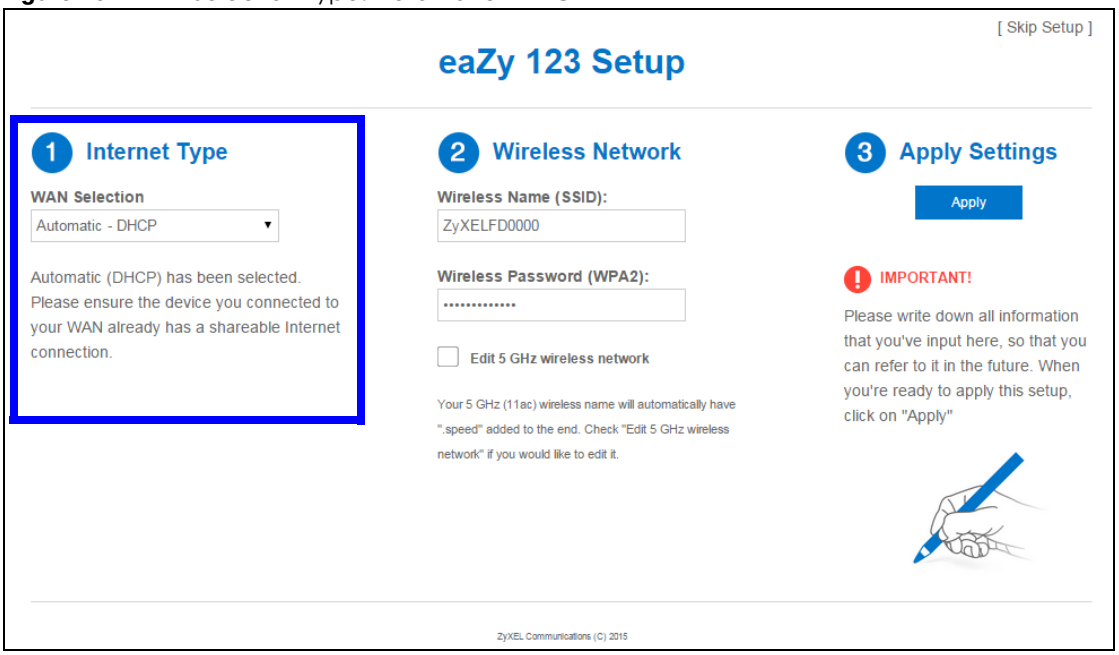
The NBG6818 offers three WAN selection types. They are **Automatic - DHCP**, **PPPoE** or **Static**. Configure the Internet type settings on your NBG6818 in the first part. The following screen depends on your Internet connection type. Enter the details provided by your Internet Service Provider (ISP) in the fields (if any).

Check with your ISP to make sure you use the correct type. This wizard screen varies according to the connection type that you select.

2.3.1 WAN Selection Type: Automatic - DHCP

Select the **Automatic - DHCP** option if your ISP did not assign you a fixed IP address.

Figure 10 WAN Selection Type: Automatic - DHCP



2.3.2 WAN Selection 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.

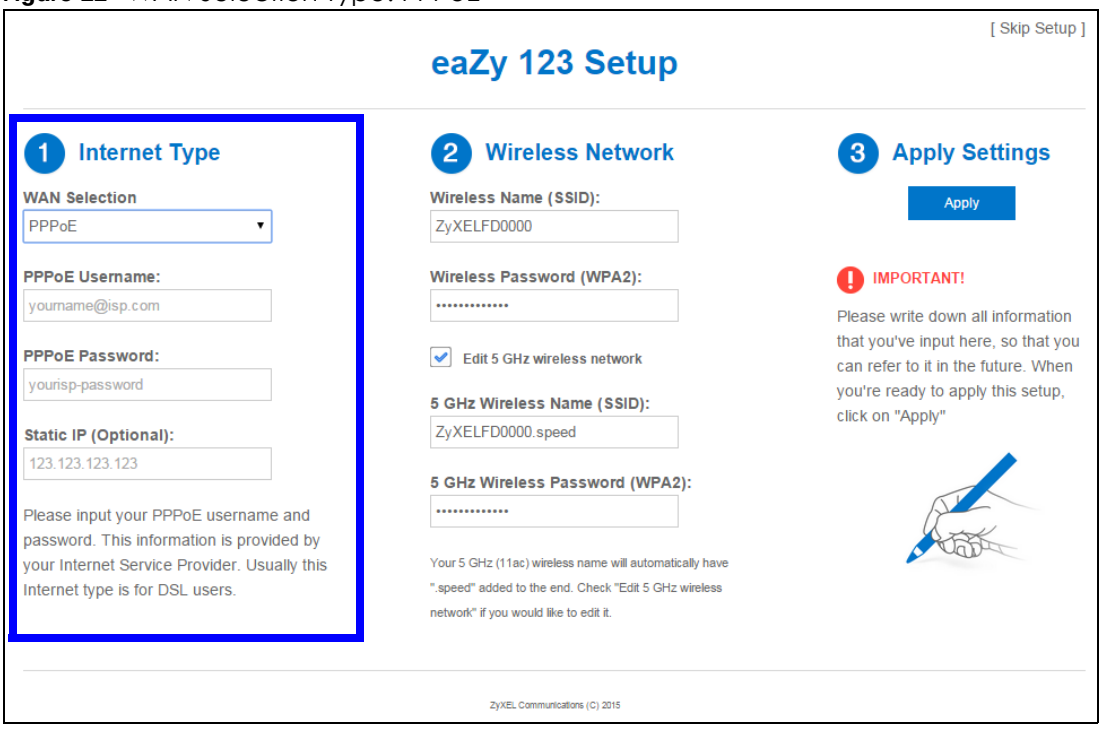
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, RADIUS).

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 NBG6818 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG6818 does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Figure 11 WAN Selection Type: PPPoE



The following table describes the labels in this screen.

Table 3 WAN Selection Type: PPPoE

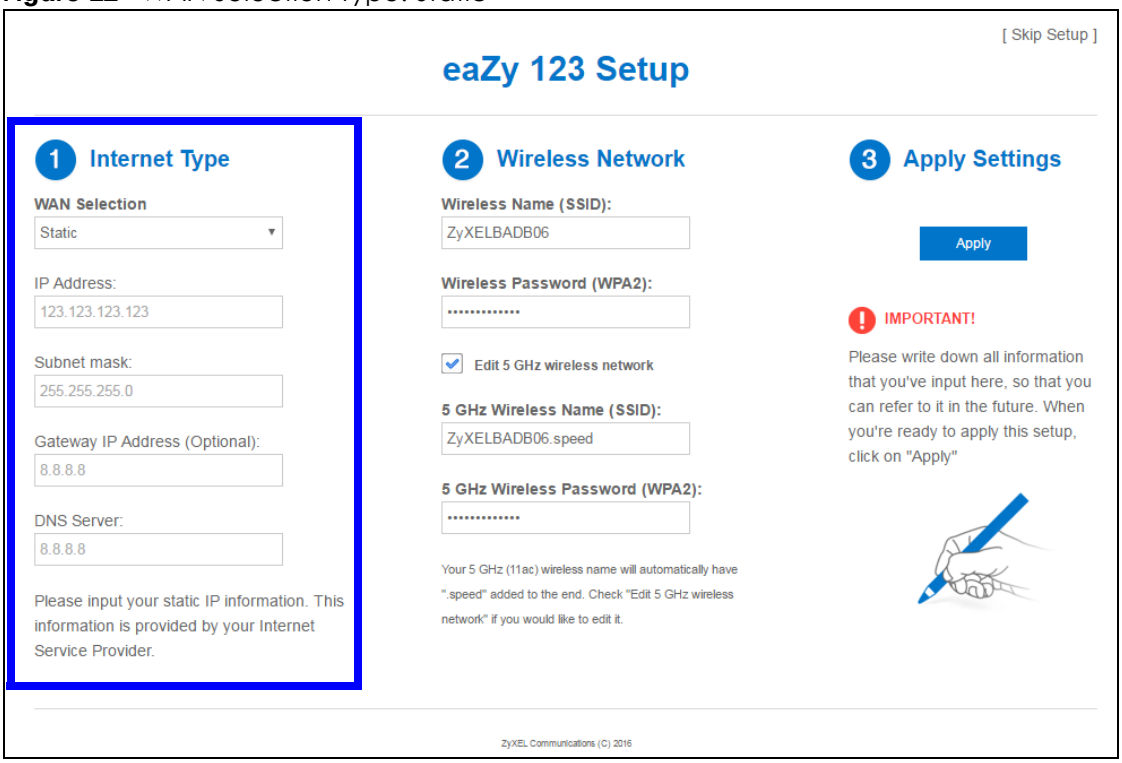
LABEL	DESCRIPTION
WAN Selection	Select the **PPPoE** (Point-to-Point Protocol over Ethernet) option for a dial-up connection.
PPPoE Username	Type the user name given to you by your ISP.
PPPoE Password	Type the password associated with the user name above.
Static IP (Optional)	Enter the WAN IP address assigned by your ISP.

Note: If you get an error message, make sure you have entered the correct information provided by your ISP.

2.3.3 WAN Selection Type: Static

Choose **Static** as the **WAN Selection Type** when the WAN port is used as a regular Ethernet. Click **Next**.

Figure 12 WAN Selection Type: Static



The following table describes the labels in this screen.

Table 4 WAN Selection Type: Static

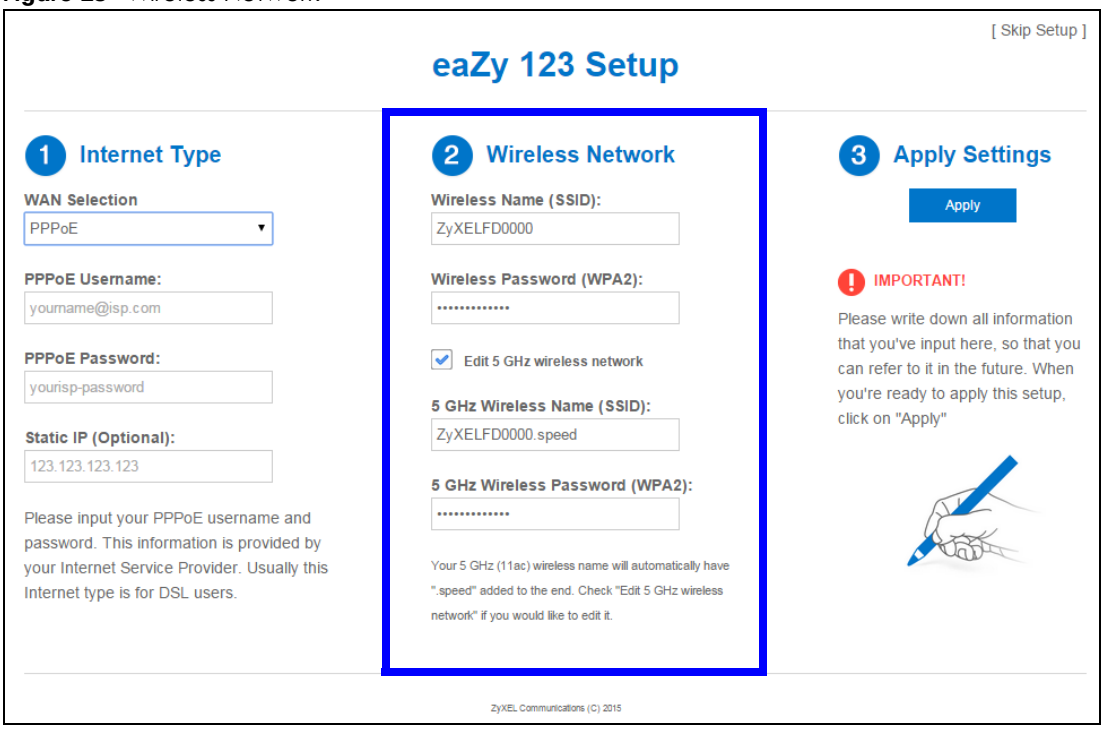
LABEL	DESCRIPTION
WAN Selection	Select the **Static** option when the WAN port is using a fixed IP address.
IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the IP subnet mask in this field.
Gateway IP Address (Optional)	Enter the gateway IP address in this field.
DNS Server	Enter the DNS server IP address in this field.

Note: If you get an error screen, make sure your Internet connection is working and select the right WAN Selection Type. Contact your ISP if you are not sure of your Internet Connection type.

2.4 Wireless Network

Configure the wireless network settings on your NBG6818 in the second part. The default wireless security setting is WPA2-PSK.

Figure 13 Wireless Network



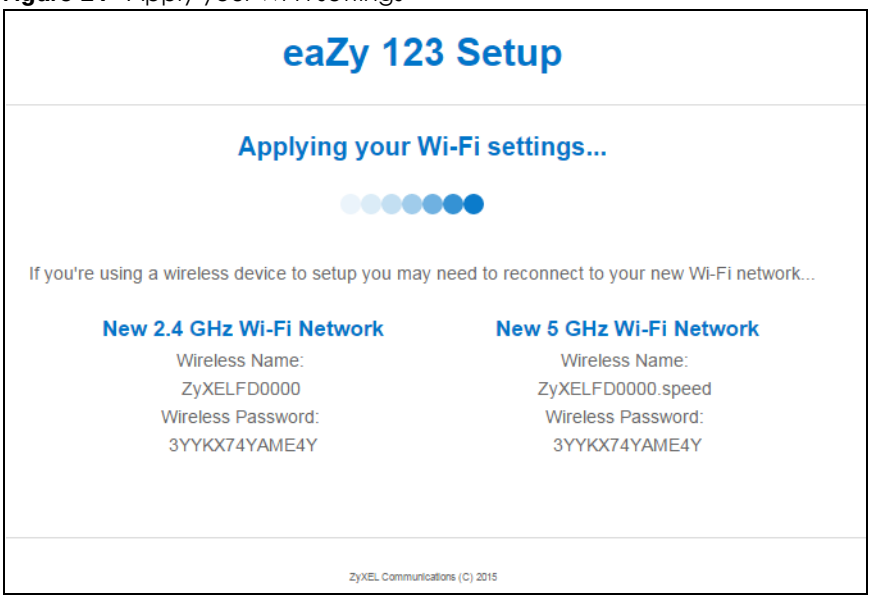
The following table describes the labels in this screen.

Table 5 Wireless Network

LABEL	DESCRIPTION
Wireless Name (SSID)	Enter a descriptive name for the wireless LAN. Note: The setting here applies to 2.4 GHz wireless radios. If you change this field on the NBG6818, make sure all wireless stations use the same SSID in order to access the network.
Wireless Password (WPA2)	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.
Edit 5 GHz wireless network	Select this check box to configure different SSID and wireless security settings for the NBG6818's 5 GHz wireless network. If you do not select this option, the NBG6818 uses the same SSID and Wi-Fi key (you configured above) for the 5 GHZ wireless network.
5GHz Wireless Name (SSID)	Enter a descriptive name for the wireless LAN. If you change this field on the NBG6818, make sure all wireless stations use the same SSID in order to access the network.
5GHz Wireless Password (WPA2)	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.

Click the **Apply** button in the third part to save your settings.

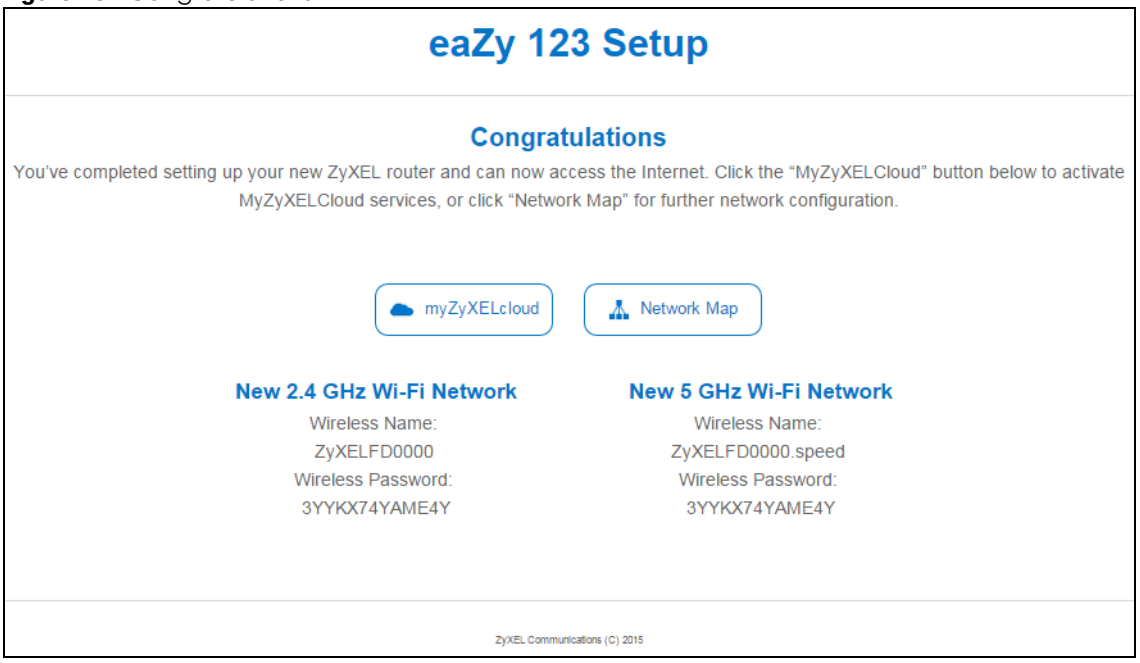
Figure 14 Apply your Wi-Fi settings



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 NBG6818's LAN ports, check your connections. Then turn the NBG6818 off, wait for a few seconds then turn it back on. If that does not work, log in to the web configurator again and check you have typed all information correctly. See the User's Guide for more suggestions.

Figure 15 Congratulations



You can click the **myZyXELcloud** button to go to https://mycloud.zyxel.com, where you can create an account and register your NBG6818. At the time of writing, you can have free DDNS service to get a

domain name mapped to the NBG6818's dynamic IP address. With DDNS, you can use the domain name to remotely access the NBG6818's Web Configurator through the Internet.

You have successfully set up your NBG6818 to operate on your network and access the Internet.

CHAPTER 3
NBG6818 Modes

3.1 Overview

This chapter introduces the different modes available on your NBG6818. 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 NBG6818 features.
- **Device mode**. This is the operating mode of your NBG6818, or simply how the NBG6818 is being used in the network.

3.1.1 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 4 on page 26 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 NBG6818. Click **> Expert Mode** after logging into the Web Configurator. The User's Guide Chapter 10 on page 78 through Chapter 15 on page 155 discusses the screens in this mode.

3.1.2 Device Modes

This refers to the operating mode of the NBG6818, which can act as a:

- **Router**: This is the default device mode of the NBG6818. Use this mode to connect the local network to another network, like the Internet. Go to Section 5.2 on page 34 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 NBG6818 wirelessly. Go to Section 6.4 on page 42 to view the **Status** screen in this mode.

For more information on these modes and to change the mode of your NBG6818, refer to Chapter 15 on page 155.

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 NBG6818 changes. The running applications and services of the network devices connected to the NBG6818 can be interrupted.

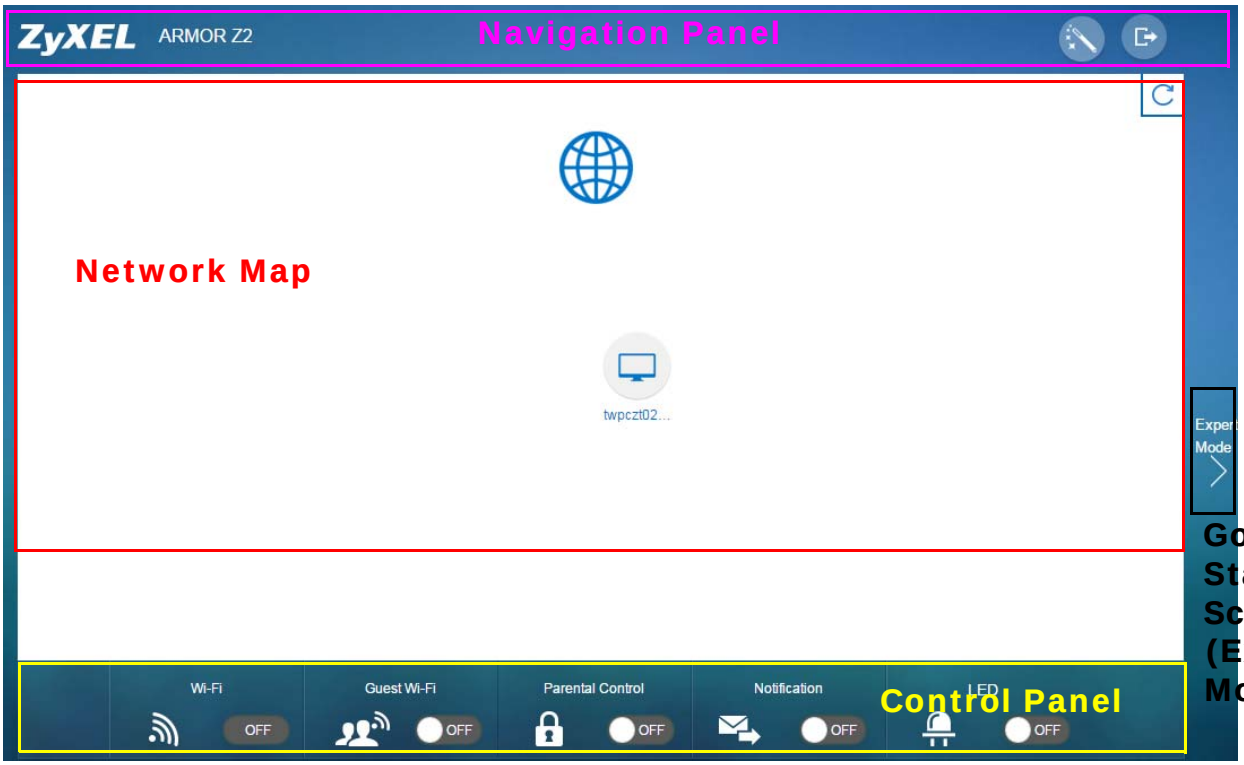
CHAPTER 4
Easy Mode

4.1 Overview

The Web Configurator is set to **Easy Mode** by default. You can configure several key features of the NBG6818 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 16 Easy Mode



4.2 What You Can Do

You can do the following in this mode:

- Use this **Navigation Panel** to open the eaZy123 wizard or log out the NBG6818 (Section 4.4 on page 27).
- Use the **Network Map** screen to check if your NBG6818 is connected to the Internet (Section 4.5 on page 28).

- Use the **Control Panel** to configure and enable NBG6818 features, including guest Wi-Fi, wireless security, parental control and so on (Section 4.6 on page 29).

4.3 What You Need to Know

Between the different device modes, the **Control Panel** (Section 4.6 on page 29) changes depending on which features are applicable to the mode:

- **Router Mode**: All **Control Panel** features are available.
- **Access Point Mode**: **Parental Control** and **Notification** are not available.

4.4 Navigation Panel

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

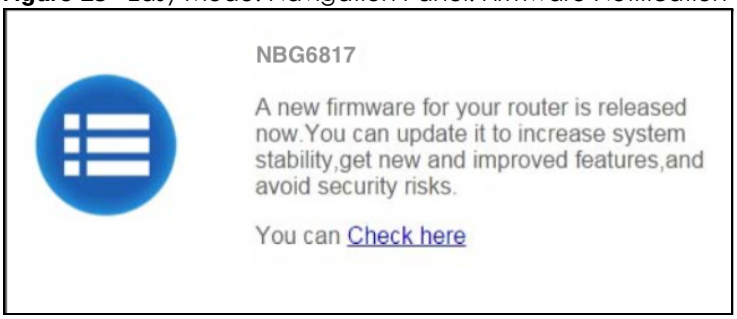
Figure 17 Easy Mode: Navigation Panel

The following table describes the labels in this screen.

Table 6 Easy Mode: Navigation Panel

ITEM	DESCRIPTION
Firmware Notification	Click this icon to open a screen where you can click **Check here** to redirect your screen to the firmware upgrade page. This icon only displays when new firmware is released.
Wizard	Click this icon to open the eaZy123 wizard for the NBG6818.
Logout	Click this to end the Web Configurator session.

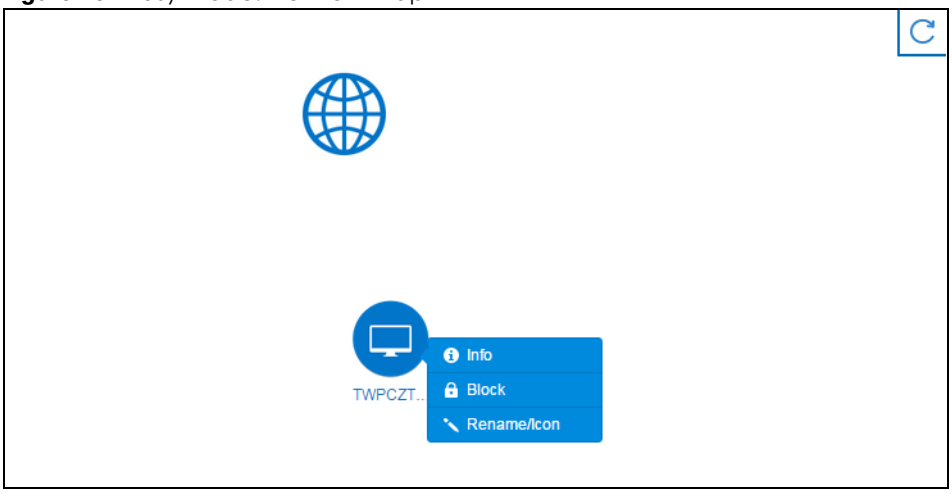
Figure 18 Easy Mode: Navigation Panel: Firmware Notification



4.5 Network Map

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

Figure 19 Easy Mode: Network Map



This screen displays whether the NBG6818 connects to the Internet. It also shows the devices connected to the NBG6818, including those connecting wirelessly. Click the **Refresh** button to refresh the network map.

The following table describes the icons in this screen.

Table 7 Easy Mode: Network Map

ITEM	DESCRIPTION
	This icon shows the NBG6818's connection status. This icon is grayed out if the user is unable to access the Internet.
	Click this button to refresh the NBG6818's connection status and the network map.
Info	Click this to view the device's information that is currently connected to the NBG6818.
Block	Click this to block the device from accessing the Internet through the NBG6818.
Rename / Icon	Click this to rename the device or change the device's icon.

Figure 20 Easy Mode: Network Map: Info

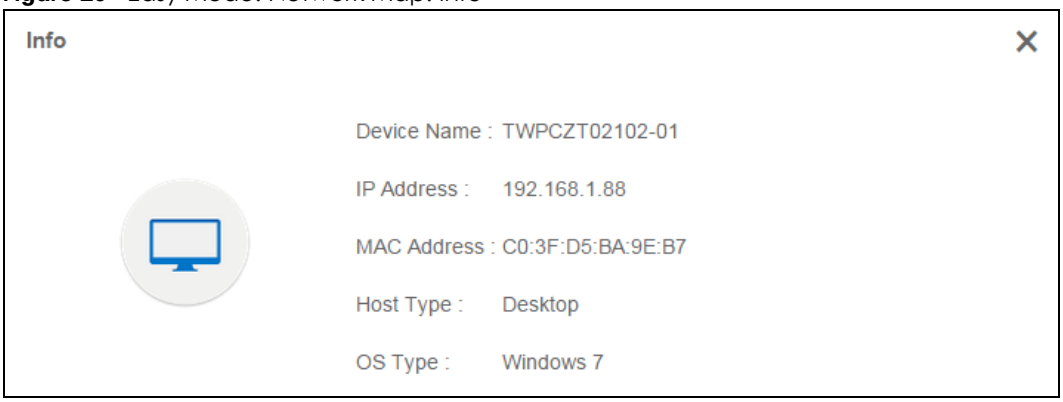
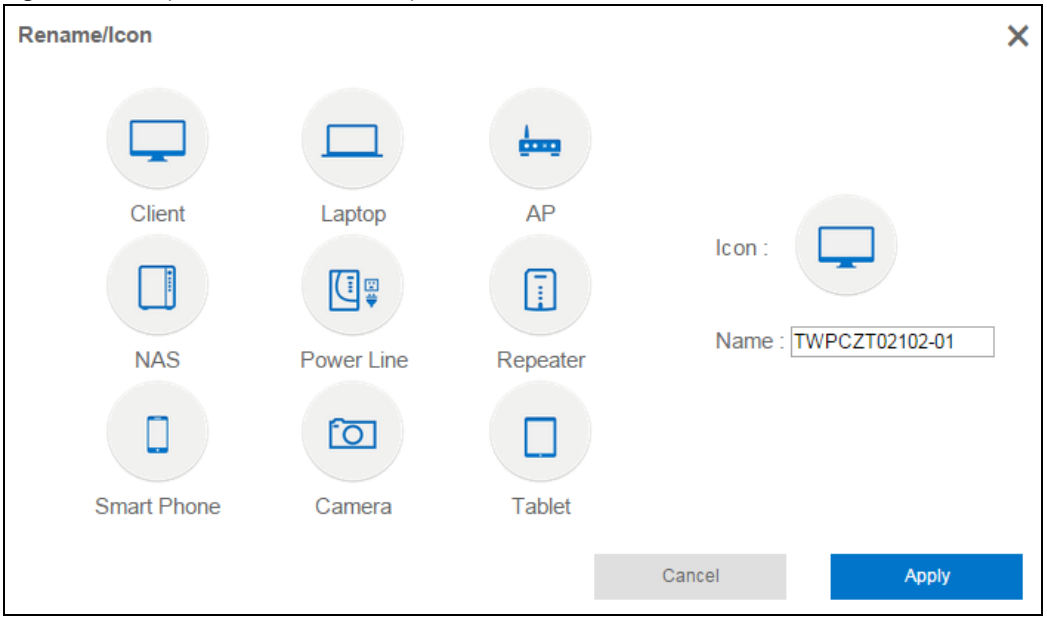


Figure 21 Easy Mode: Network Map: Rename / Icon

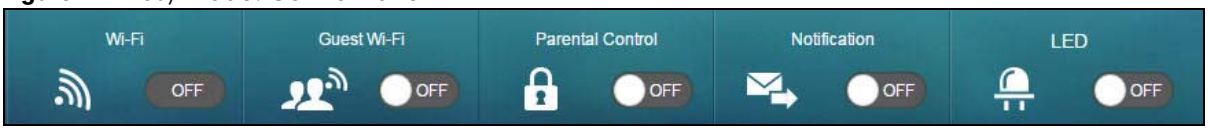


Click **Apply** to save your changes back to the NBG6818. Click **Cancel** to reload the previous configuration for this screen.

4.6 Control Panel

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

Figure 22 Easy Mode: 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 blue 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 8 Easy Mode: Control Panel

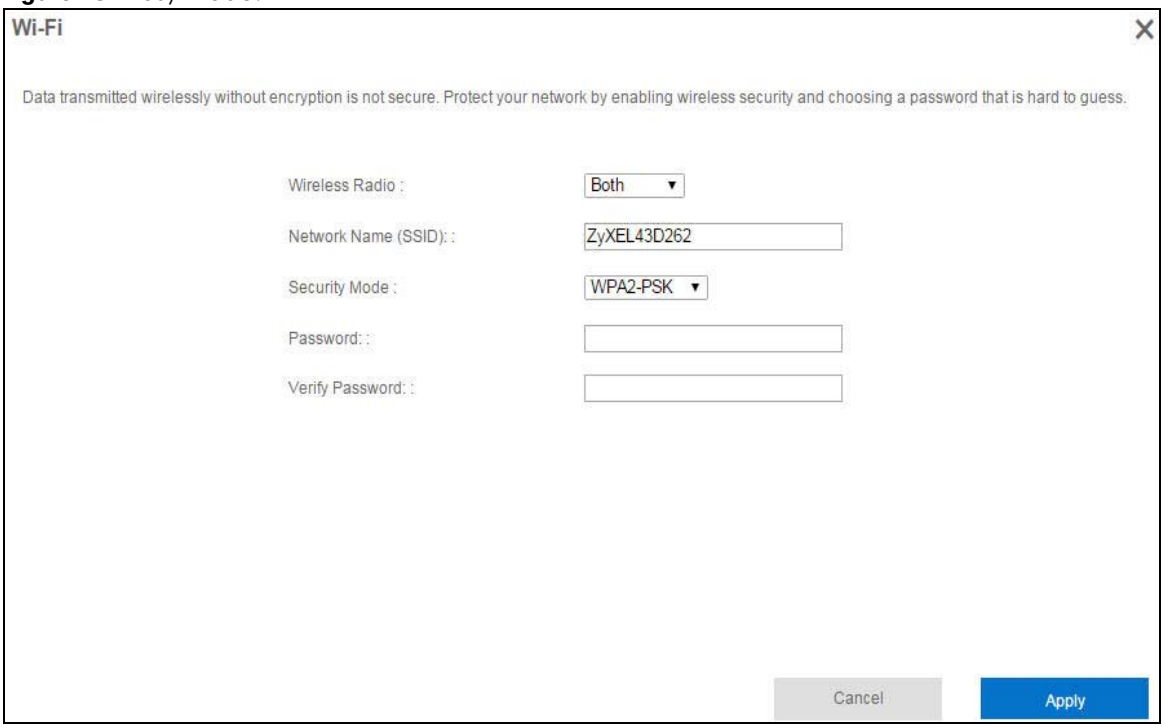
ITEM	DESCRIPTION
Wi-Fi	Click this to configure wireless radio, SSID, security mode and wireless password for the NBG6818's default Wi-Fi network. Refer to Section 4.6.1 on page 30 to see this screen.
Guest Wi-Fi	Click this to configure wireless and wireless security settings for the guest Wi-Fi network.
Parental Control	Switch **ON** to enable parental control, and click this to view the parental control rules. Otherwise, switch **OFF**. Refer to Section 4.6.3 on page 32 to see this screen.
Notification	Switch **ON** to have the NBG6818 send e-mail notifications when the user(s) is connected to the NBG6818 for Internet access during the specified time periods. Otherwise, switch **OFF**. Refer to Section 4.6.4 on page 33 to see this screen.
LED	Switch **ON** to have the NBG6818's LEDs (lights) stay lit/blinking. Otherwise, switch **OFF**.

4.6.1 Wi-Fi

Use this screen to configure security for the NBG6818's default wireless LAN. You can enter the SSID and select the wireless security mode in the following screen. See Chapter 13 on page 112 for how to configure wireless network.

Note: You can enable the wireless function of your NBG6818 by first turning on the **WIFI** switch in the rear panel.

Figure 23 Easy Mode: Wi-Fi



The following table describes the labels in this screen.

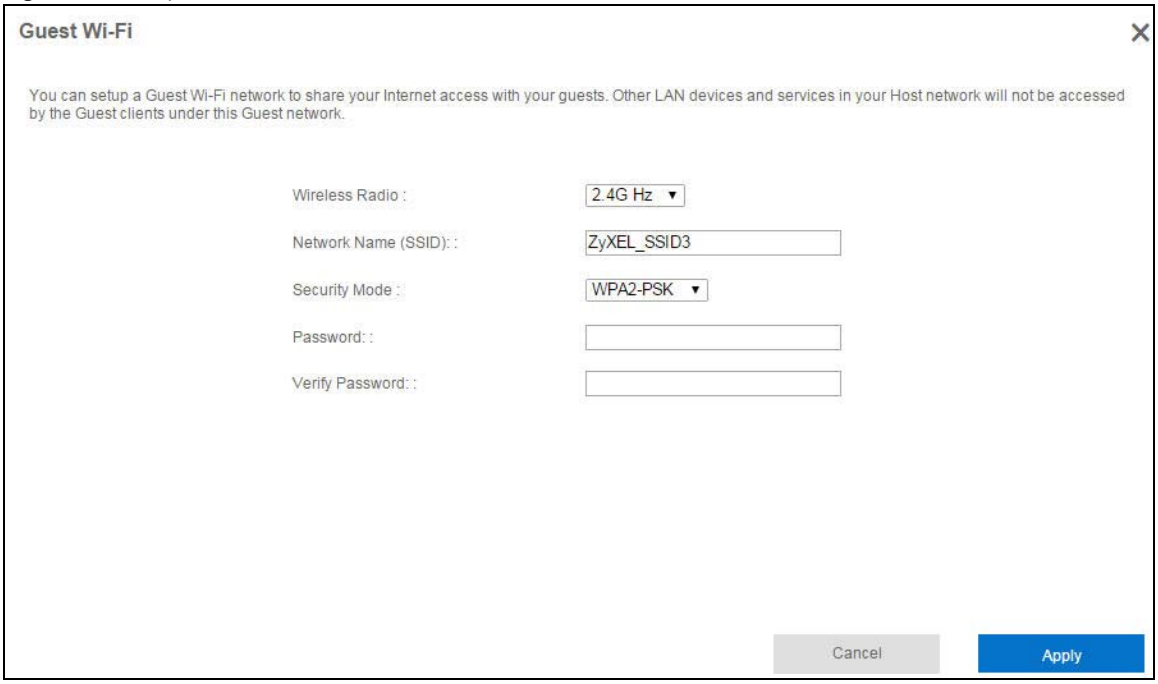
Table 9 Easy Mode: Wi-Fi

LABEL	DESCRIPTION
Wireless Radio	Choose whether you want to apply the wireless security to **2.4G Hz**, **5G Hz** or **Both** wireless radios.
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 enable data encryption. Or Select **No Security** to allow wireless clients to communicate with the access points without any data encryption.
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.
Cancel	Click **Cancel** to reload the previous configuration for this screen.
Apply	Click **Apply** to save your changes back to the NBG6818.

4.6.2 Guest Wi-Fi

This screen allows you to configure guest wireless network settings on the NBG6818. Users connected to the guest wireless network can access the Internet via the NBG6818, but not other networks connected to the NBG6818. See Chapter 11 on page 94 for how to enable and set up the guest wireless network.

Figure 24 Easy Mode: Guest Wi-Fi



The following table describes the labels in this screen.

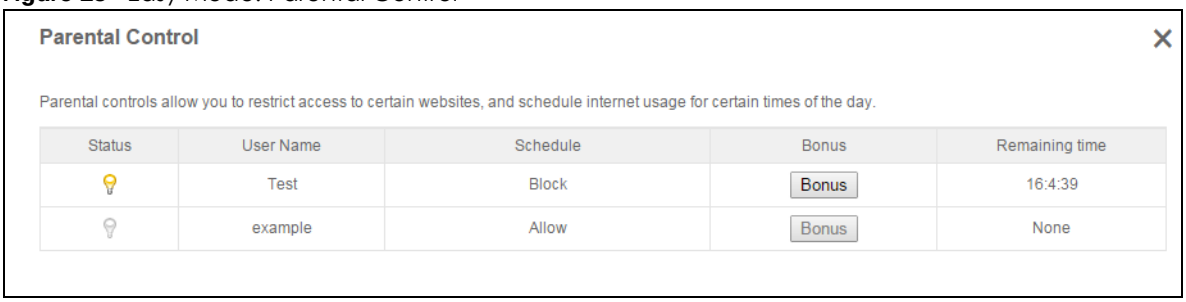
Table 10 Easy Mode: Guest Wi-Fi

LABEL	DESCRIPTION
Wireless Radio	Choose whether you want to apply the wireless settings to the **2.4G Hz** or **5G Hz** wireless radio.
Network Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the guest wireless network.
Security Mode	Select **WPA2-PSK** to enable data encryption. Or select **No Security** to allow wireless clients to communicate with the NBG6818 without any data encryption.
Password	This field appears when you choose **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.
Cancel	Click **Cancel** to reload the previous configuration for this screen.
Apply	Click **Apply** to save your changes back to the NBG6818.

4.6.3 Parental Control

Use this screen to view the parental control rules configured on the NBG6818. See Section 9.2 on page 58 for how to enable and configure parental control rules.

Figure 25 Easy Mode: Parental Control



The following table describes the labels in this screen.

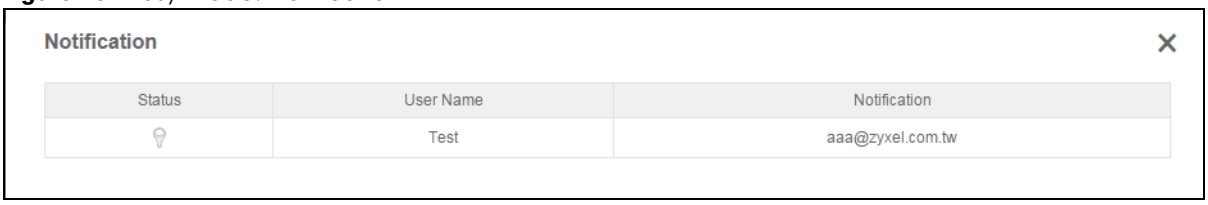
Table 11 Easy Mode: Parental Control

LABEL	DESCRIPTION
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
User Name	This shows the name of the user to which this rule applies.
Schedule	This shows whether the user is allowed to access the Internet (**Allow**) or not (**Block**).
Bonus	If the user is currently not permitted to access the Internet, you can click the **Bonus** to allow access for a specified period of time. A screen then displays allowing you to set how long (in minutes) the user is allowed to access the Internet. This button is grayed out if the user is now able to access the Internet.
Remaining time	This field displays the amount of Internet access time that remains for each user before the NBG6818 blocks the user from accessing the Internet. **None** means there is no extra Internet access time.

4.6.4 Notification

Use this screen to view the e-mail notification rules configured on the NBG6818. See Section 13.2.2 on page 119 for how to configure e-mail notification rules and e-mail settings.

Figure 26 Easy Mode: Notification



The following table describes the labels in this screen.

Table 12 Easy Mode: Notification

LABEL	DESCRIPTION
Notification	
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
User Name	This shows the name of the user to which this rule applies.
Notification	This shows the e-mail address to which the notification is sent.

4.6.5 LED

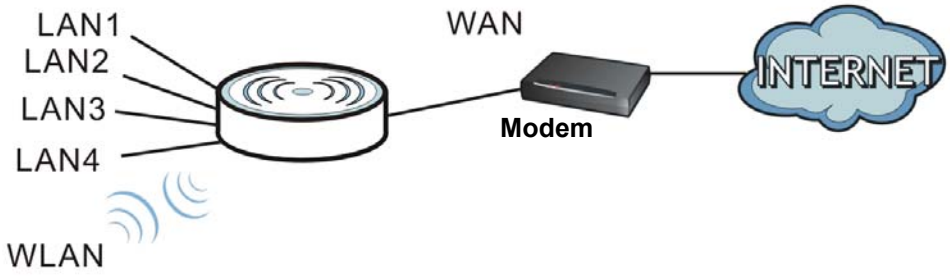
Switch **ON** to turn on the LEDs (lights) on the NBG6818. Otherwise, switch **OFF**.

CHAPTER 5
Router Mode

5.1 Overview

The NBG6818 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 NBG6818 connects the local network (**LAN1** ~ **LAN4**) to the Internet.

Figure 27 NBG6818 Network

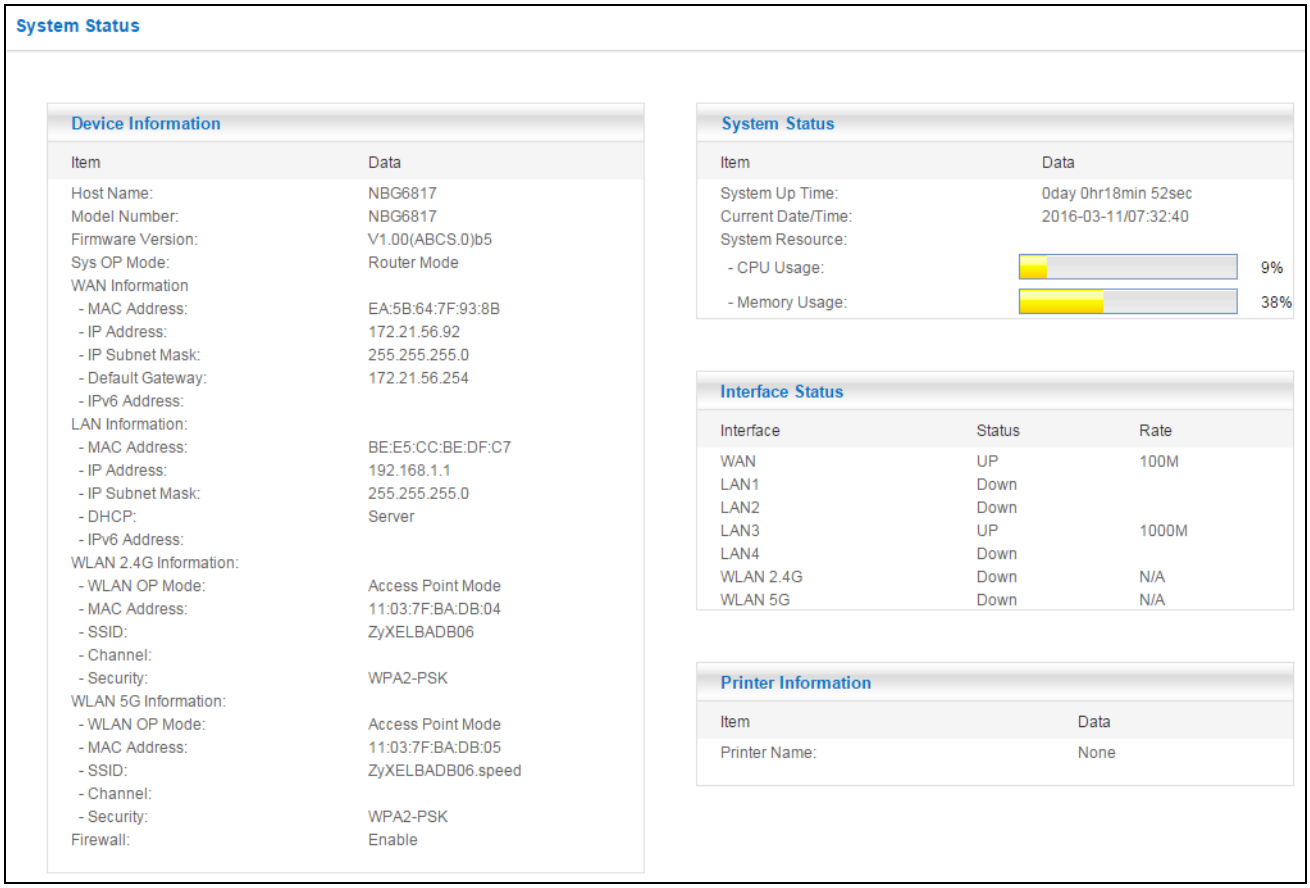


Note: After clicking **Login**, the **Easy Mode** appears. Refer to Chapter 4 on page 26 for the **Easy Mode** screens. Change to **Expert Mode** to see the screens described in the sections following this.

5.2 Router Mode Status Screen

Click **Expert Mode** > **Status** > **System Status** to open the status screen.

Figure 28 Expert Mode: Status > System Status: Router Mode



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

Table 13 Expert Mode: Status > System Status: Router Mode

LABEL	DESCRIPTION
Device Information	
Item	This column shows the type of data the NBG6818 is recording.
Data	This column shows the actual data recorded by the NBG6818.
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.
Sys OP Mode	This is the device mode (Section 3.1.2 on page 25) to which the NBG6818 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.
IPv6 Address	This shows the IPv6 address of the NBG6818 on the WAN.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.

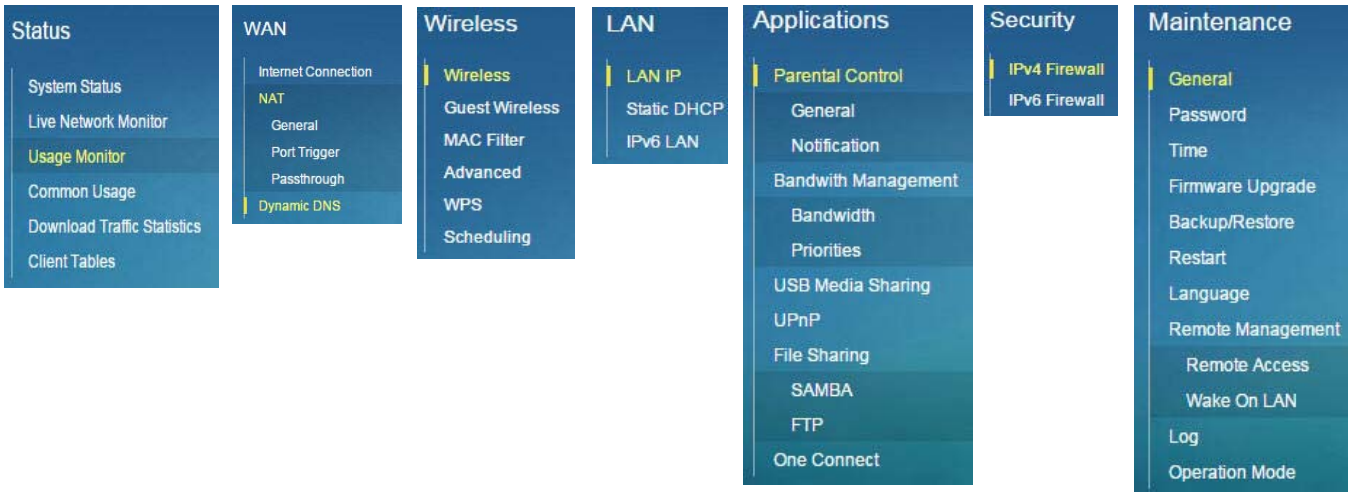
Table 13 Expert Mode: Status > System Status: Router Mode (continued)

LABEL	DESCRIPTION
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**.
IPv6 Address	This shows the IPv6 address of the NBG6818 on the LAN.
WLAN 2.4G Information	
WLAN OP Mode	This is the device mode (Section 3.1.2 on page 25) to which the NBG6818's wireless LAN is set - **Access Point Mode**.
MAC Address	This shows the 2.4GHz wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the NBG6818 in the 2.4GHz wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the NBG6818 is using.
WLAN 5G Information	
WLAN OP Mode	This is the device mode (Section 3.1.2 on page 25) to which the NBG6818's wireless LAN is set - **Access Point Mode**.
MAC Address	This shows the 5GHz wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the NBG6818 in the 5GHz wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the NBG6818 is using.
Firewall	This shows whether the firewall is enabled or not.
System Status	
System Up Time	This is the total time the NBG6818 has been on.
Current Date/Time	This field displays your NBG6818's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG6818's processing ability is currently used. When this percentage is close to 100%, the NBG6818 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 NBG6818 is using.
Interface Status	
Interface	This displays the NBG6818 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 2.4GHz/5GHz WLAN, it displays **Up** when the 2.4GHz/5GHz WLAN is enabled or **Down** when the 2.4G/5G WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or is left blank 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 2.4GHz/5GHz WLAN, it displays the maximum transmission rate when the 2.4GHz/5GHz WLAN is enabled and **N/A** when the WLAN is disabled.
Printer Information	
Printer Name	The NBG6818 can act as a print server and allows you to share a USB printer on your LAN. This displays the name of the printer connected to the NBG6818's USB port. Note: You need to manually install the printer driver in your computer and add the printer to your printer list.

5.2.1 Navigation Panel

Use the sub-menus on the navigation panel to configure NBG6818 features.

Figure 29 Expert Mode: Navigation Panel: Router Mode



The following table describes the sub-menus.

Table 14 Expert Mode: Navigation Panel: Router Mode

LINK	TAB	FUNCTION
Status		
System Status		This screen shows the NBG6818's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Live Network Monitor		This screen shows transmission data rates between the NBG6818 and the Internet or connected devices.
Usage Monitor		This screen shows transmission data and bandwidth usage between the NBG6818 and the Internet or connected devices.
Common Usage		This screen shows the top five traffic flows transmitting from/to the selected LAN device(s).
Download Traffic Statistics		This screen shows the type and percentage of most download traffic.
Client Tables		Use this screen to view online clients information.
WAN		
Internet Connection		This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address.
NAT	General	Use this screen to enable NAT. Use this screen to configure servers behind the NBG6818 and forward incoming service requests to the server(s) on your local network.
	Port Trigger	Use this screen to change your NBG6818's port triggering settings.
	Passthrough	Use this screen to enable ALGs (Application Layer Gateway) and VPN pass-through settings.
Dynamic DNS		Use this screen to set up dynamic DNS.
Wireless		

Table 14 Expert Mode: Navigation Panel: Router Mode (continued)

LINK	TAB	FUNCTION
Wireless		Use this screen to enable the wireless LAN and configure wireless LAN and wireless security settings.
Guest Wireless		Use this screen to configure multiple BSSs on the NBG6818.
MAC Filter		Use the MAC filter screen to configure the NBG6818 to block access to devices or block the devices from accessing the NBG6818.
Advanced		This screen allows you to configure advanced wireless settings.
WPS		Use this screen to configure WPS.
Scheduling		Use this screen to schedule the times the Wireless LAN is enabled.
LAN		
LAN IP		Use this screen to configure LAN IP address and subnet mask. Use this screen to configure the IPv6 address for the NBG6818 on the LAN. Use this screen to enable the NBG6818's DHCP server.
Static DHCP		This screen allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses.
IPv6 LAN		Use this screen to configure the IPv6 address for your NBG6818 on the LAN.
Applications		
Parental Control	General	Use this screen to enable parental control, set parental controls rules/ schedules and block web sites containing certain keywords in the URL.
	Notification	Use this screen to send e-mail notifications, configure e-mail notification rules and e-mail settings.
Bandwidth Management	Bandwidth	Use this screen to enable StreamBoost. Use this screen to configure the maximum allowable bandwidth and enable automatic update.
	Priorities	Use this screen to change the priority of the connected devices.
USB Media Sharing		Use this screen to have the NBG6818 function as a DLNA-compliant media server, that lets DLNA-compliant media clients play video, audio, and photo content files stored on the connected USB storage device.
UPnP		Use this screen to enable UPnP on the NBG6818.
File Sharing	SAMBA	Use this screen to enable file sharing through the NBG6818.
	FTP	Use this screen to have the NBG6818 act as a FTP server.
One Connect		Use this screen to enable or disable Wi-Fi auto-configuration.
Security		
IPv4 Firewall		Use this screen to configure IPv4 firewall rules.
IPv6 Firewall		Use this screen to configure IPv6 firewall rules.
Maintenance		
General		Use this screen to view and change administrative settings such as system and domain names.
Password		Use this screen to change the password of your NBG6818.
Time		Use this screen to change your NBG6818's time and date.
Firmware Upgrade		Use this screen to upload firmware to your NBG6818.
Backup/Restore		Use this screen to backup and restore the configuration or reset the factory defaults to your NBG6818.
Restart		This screen allows you to reboot the NBG6818 without turning the power off.
Language		This screen allows you to select the language you prefer.

Table 14 Expert Mode: Navigation Panel: Router Mode (continued)

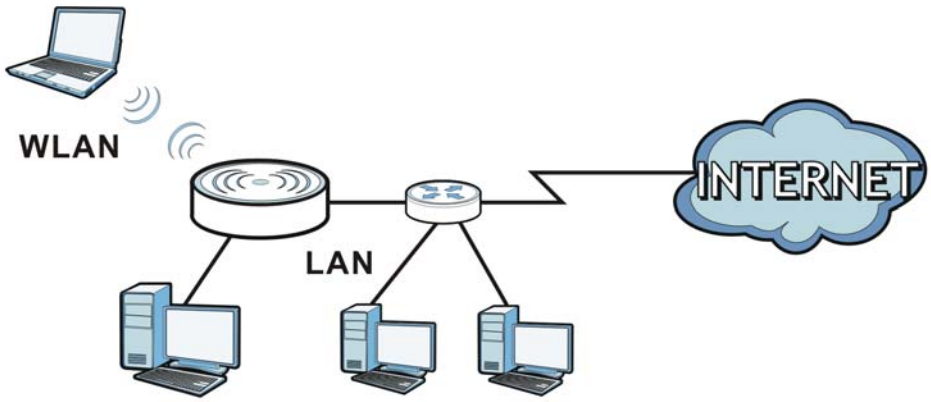
LINK	TAB	FUNCTION
Remote Management	Remote Access	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet and HTTP/HTTPS to manage the NBG6818.
	Wake On LAN	Use this screen to enable Wake on LAN to remotely turn on a device on the local network.
Log		Use this screen to view the list of activities recorded by your NBG6818.
Operation Mode		This screen allows you to select whether your device acts as a router, or an access point.

CHAPTER 6
Access Point Mode

6.1 Overview

Use your NBG6818 as an access point (AP) if you already have a router or gateway on your network. In this mode your NBG6818 bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

Figure 30 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.

6.2 What You Can Do

- Use the **Status** screen to view read-only information about your NBG6818 (Section 6.4 on page 42).
- Use the **LAN** screen to set the IP address for your NBG6818 acting as an access point (Section 6.5 on page 44).

6.3 What You Need to Know

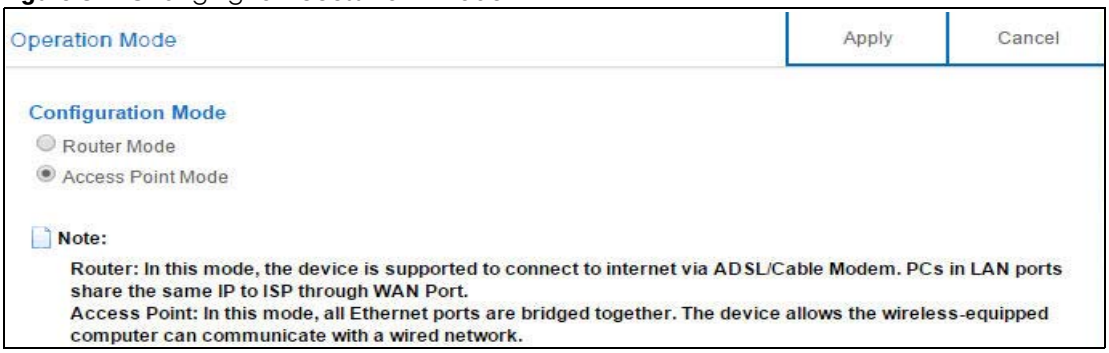
See Chapter 7 on page 47 for a tutorial on setting up a network with the NBG6818 as an access point.

6.3.1 Setting your NBG6818 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 NBG6818 as an access point, go to **Expert Mode > Maintenance > Operation Mode** and select **Access Point Mode**.

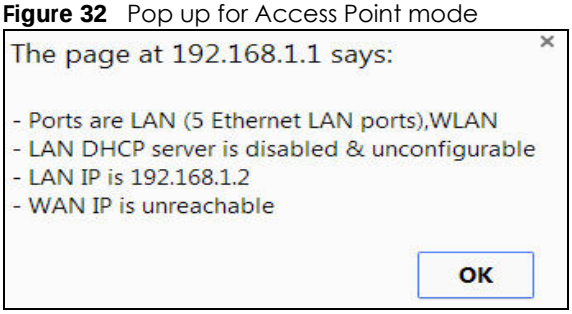
Figure 31 Changing to Access Point mode



Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your NBG6818 is already in Access Point mode.

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

Figure 32 Pop up for Access Point mode



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

6.3.2 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 NBG6818.

2 The default IP address of the NBG6818 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 B on page 141 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 26 for the **Easy Mode** screens. Change to **Expert Mode** to see the screens described in the sections following this.

6.3.3 Configuring your WLAN and Maintenance Settings

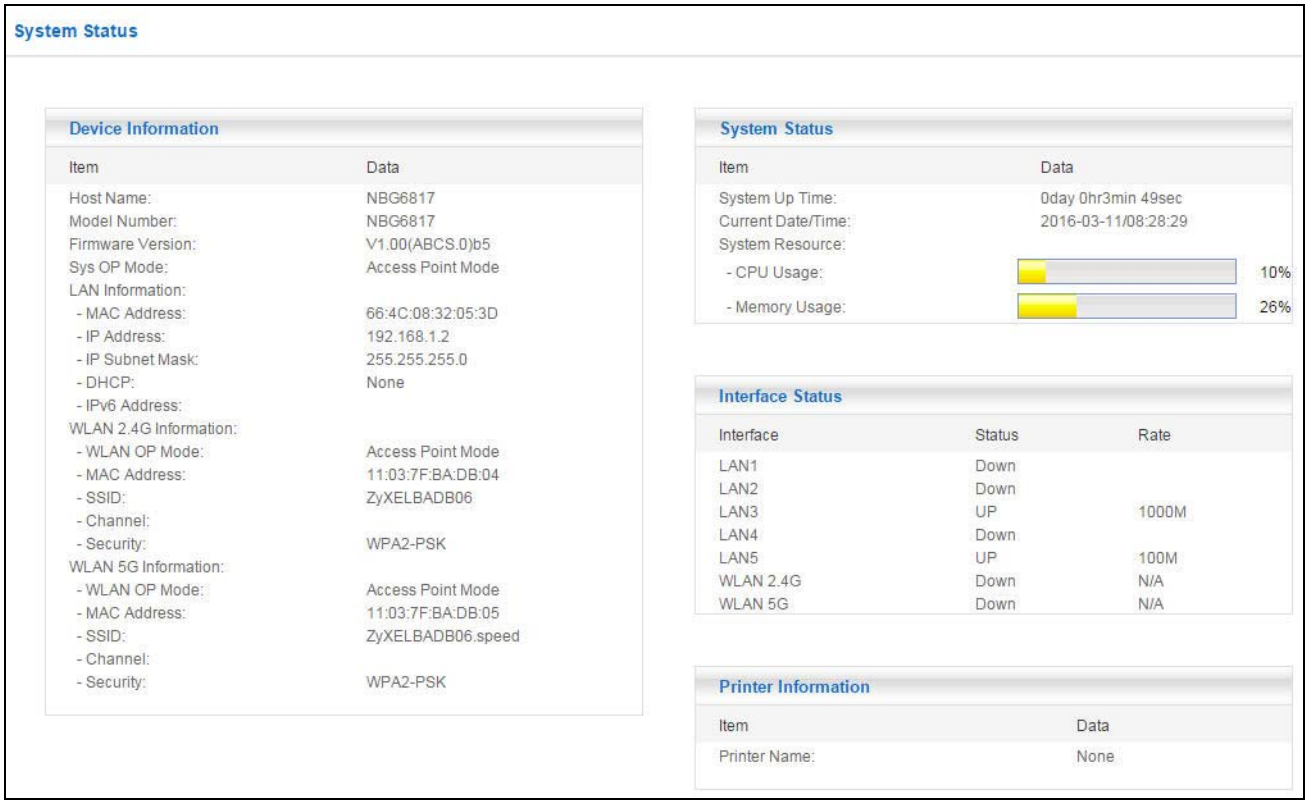
The configuration of wireless and maintenance settings in **Access Point Mode** is the same as for **Router Mode**.

- See Chapter 11 on page 94 for information on the configuring your wireless network.
- See Chapter 14 on page 119 for information on configuring your maintenance settings.

6.4 AP Mode Status Screen

Click **Expert Mode > Status** to open the **Status** screen.

Figure 33 Expert Mode: Status > System Status: Access Point Mode



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

Table 15 Expert Mode: Status > System Status: 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.
Sys OP Mode	This is the device mode (Section 3.1.2 on page 25) to which the NBG6818 is set - **AP Mode**.

Table 15 Expert Mode: Status > System Status: Access Point Mode (continued)

LABEL	DESCRIPTION
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**.
IPv6 Address	This shows the IPv6 address of the NBG6818 on the LAN.
WLAN 2.4G Information	
WLAN OP Mode	This is the device mode (Section 3.1.2 on page 25) to which the NBG6818's wireless LAN is set - **Access Point Mode**.
MAC Address	This shows the 2.4GHz wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the NBG6818 in the 2.4GHz wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the NBG6818 is using.
WLAN 5G Information	
WLAN OP Mode	This is the device mode (Section 3.1.2 on page 25) to which the NBG6818's wireless LAN is set - **Access Point Mode**.
MAC Address	This shows the 5GHz wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the NBG6818 in the 5GHz wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the NBG6818 is using.
System Status	
Item	This column shows the type of data the NBG6818 is recording.
Data	This column shows the actual data recorded by the NBG6818.
System Up Time	This is the total time the NBG6818 has been on.
Current Date/Time	This field displays your NBG6818's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG6818's processing ability is currently used. When this percentage is close to 100%, the NBG6818 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.
- Memory Usage	This shows what percentage of the heap memory the NBG6818 is using.
Interface Status	
Interface	This displays the NBG6818 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 2.4GHz/5GHz WLAN, it displays **Up** when the 2.4GHz/5GHz WLAN is enabled or **Down** when the 2.4G/5G WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or is left blank when the line is disconnected. For the 2.4GHz/5GHz WLAN, it displays the maximum transmission rate when the 2.4GHz/5GHz WLAN is enabled and **N/A** when the WLAN is disabled.

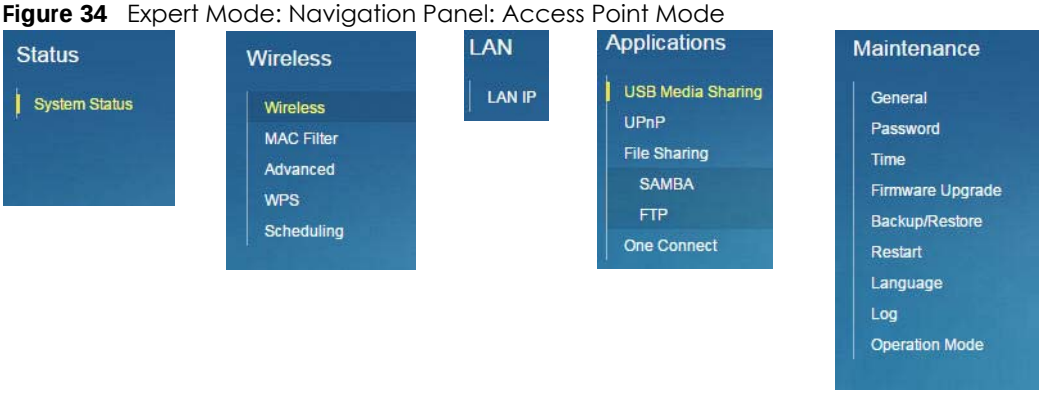
Table 15 Expert Mode: Status > System Status: Access Point Mode (continued)

LABEL	DESCRIPTION
Printer Information	
Printer Name	The NBG6818 can act as a print server and allows you to share a USB printer on your LAN. This displays the name of the printer connected to the NBG6818's USB port. Note: You need to manually install the printer driver in your computer and add the printer to your printer list.

6.4.1 Navigation Panel

Use the menu in the navigation panel to configure NBG6818 features in **Access Point Mode**.

Figure 34 Expert Mode: Navigation Panel: Access Point Mode



Refer to Table 14 on page 37 for descriptions of the labels shown in the navigation panel.

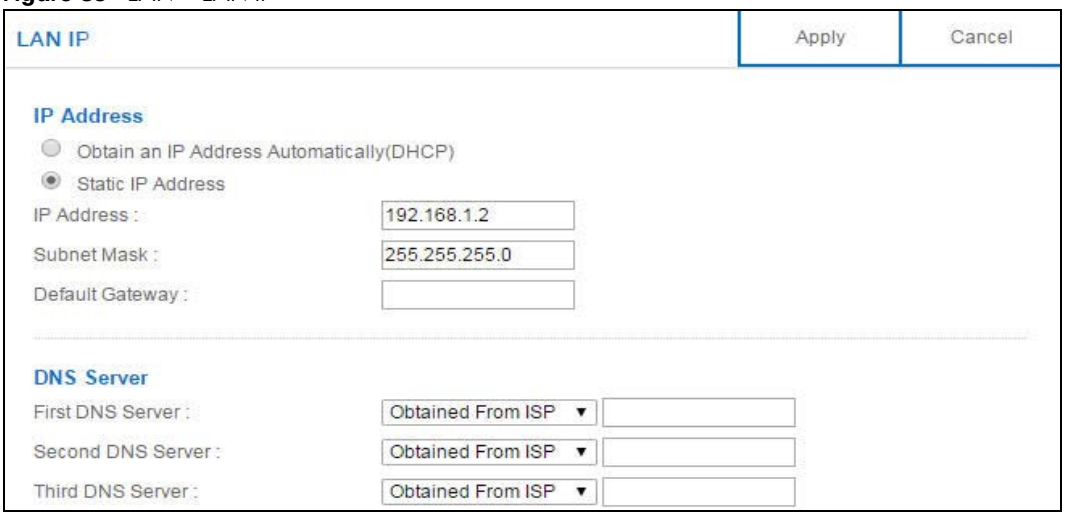
6.5 LAN Screen

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

Click **Expert Mode > LAN** to see the screen below.

Note: If you change the IP address of the NBG6818 in the screen below, you will need to log into the NBG6818 again using the new IP address.

Figure 35 LAN > LAN IP



The table below describes the labels in the screen.

Table 16 LAN > LAN IP

LABEL	DESCRIPTION
IP Address	
Obtain an IP Address Automatically	When you enable this, the NBG6818 gets its IP address from the network's DHCP server (for example, your ISP). Users connected to the NBG6818 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 NBG6818. You need to reset the NBG6818 to be able to access the Web Configurator again (see Section 15.6 on page 148 for details on how to reset the NBG6818). Also when you select this, you cannot enter an IP address for your NBG6818 in the field below.
Static IP Address	Click this if you want to specify the IP address of your NBG6818. 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 NBG6818 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 NBG6818.
Default Gateway	Enter a gateway IP address (if your ISP or network administrator gave you one) in this field.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the NBG6818'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 16 LAN > LAN IP (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the NBG6818.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

CHAPTER 7
Tutorials

7.1 Overview

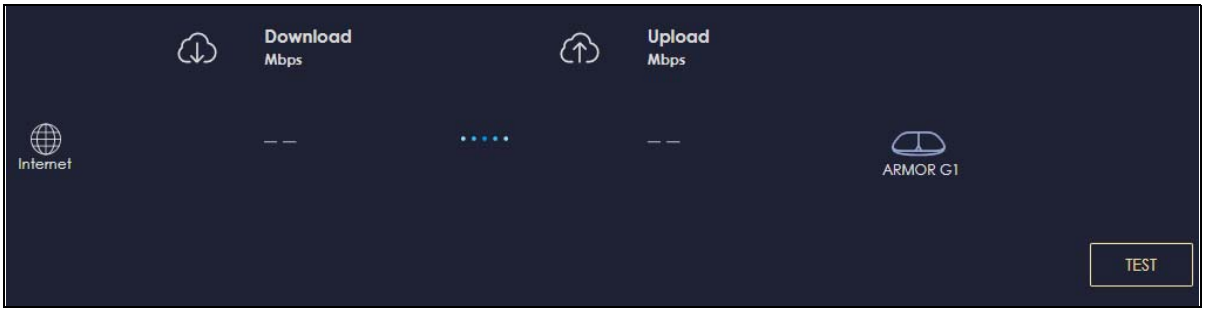
This chapter provides tutorials for setting up your NBG6818.

- Run a Speed Test
- Connect to NBG6818 Wireless Network without WPS
- Using Guest SSIDs on the NBG6818

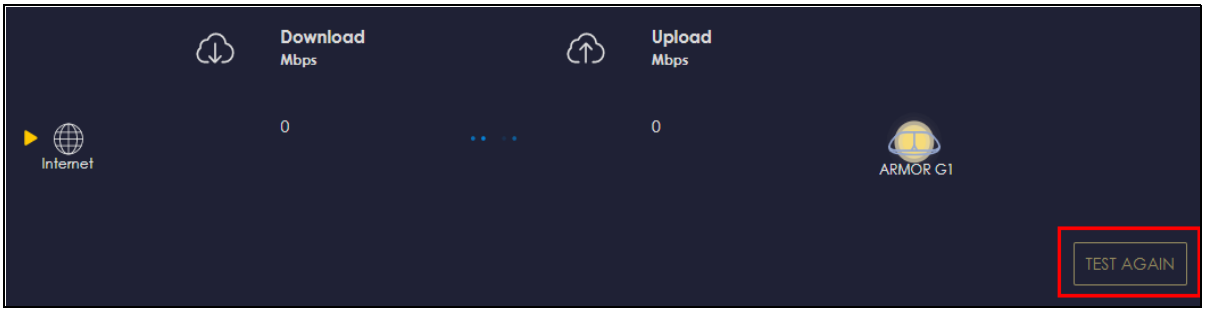
7.2 Run a Speed Test

With the NBG6818 Web Configurator, you can check the speed of the connection between your NBG6818 and the broadband modem/router.

1 Click the **Navigation Panel** icon on the top-left corner ( ), and click **Diagnose** to open the **Advanced Speed Test** screen. Use this screen to view all the available connections in your NBG6818 System.



2 Click **TEST** to perform a speed test. This shows data rates for both upstream and downstream traffic. Click **TEST AGAIN** to update the information in this screen.



3 Click the **Speed Test History** tab to view a summary of the tests made. Click **Clear** to delete all records.

7.3 Configure the NBG6818's WiFi Networks

In the NBG6818 you can configure independent wireless networks with different privileges. Clients can associate only with the network for which they have security settings (SSID and password). The following table describes the different NBG6818's profile networks and their privileges.

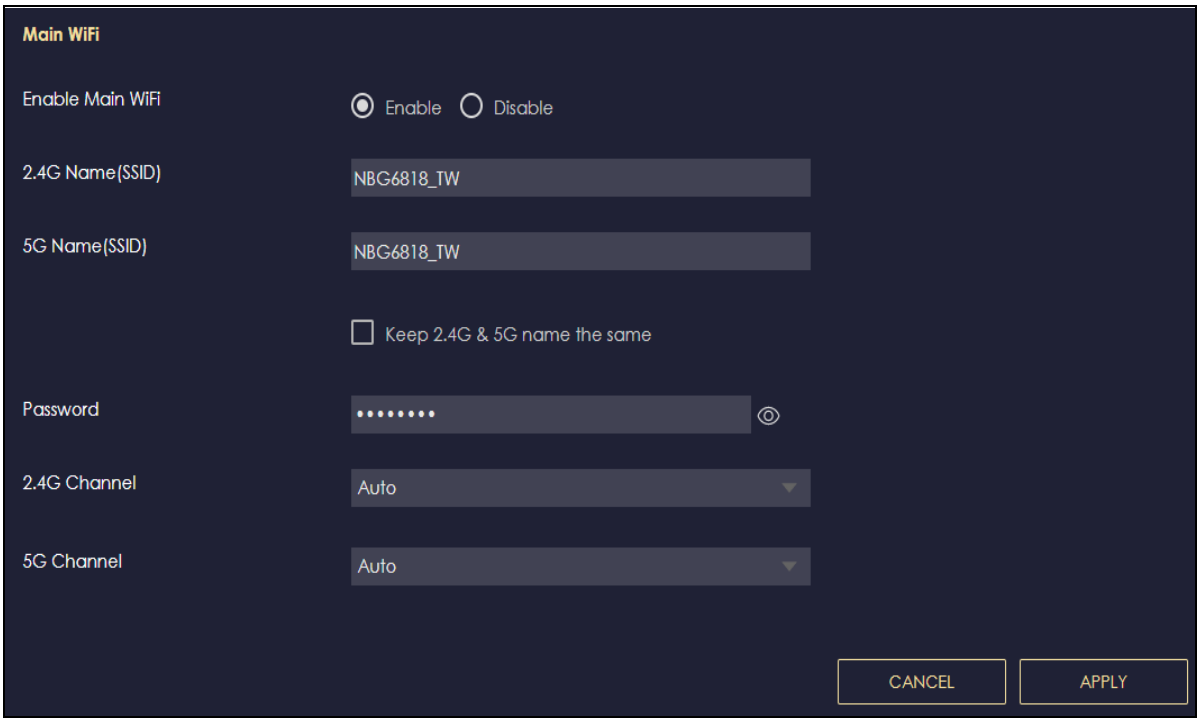
Table 17 WiFi Network Privileges

WIFI NETWORK	INTERNET ACCESS	2.4G / 5G WIFI NETWORK	ACCESS TO WEB CONFIGURATOR	ACCESS TO WIRED LAN
Main WiFi	Yes	2.4G and 5G	Yes	Yes
Guest WiFi	Yes	2.4G and 5G	No	No
Visitor WiFi	Yes, after captive portal log in.	2.4G and 5G	No	No

Note: A user can only configure the WiFi networks' security settings if they are connected to the **Main WiFi** network.

1 Click the **Navigation Panel** icon on the top-left corner ( ), and click **Settings** to open the **WiFi** screen. Use each tab in the **WiFi** menu to configure each of the WiFi networks' security settings.

2 Select **Enable** to activate a WiFi Network. Enter the **2.4G/5G Name** and **Password** clients use to connect to the WiFi network. You can configure two different WiFi Names for the **Main WiFi** 2.4G and 5G networks. Select **Keep 2.4G & 5G name the same,** so they both use the same WiFi Name. Click **Apply** to save your changes.

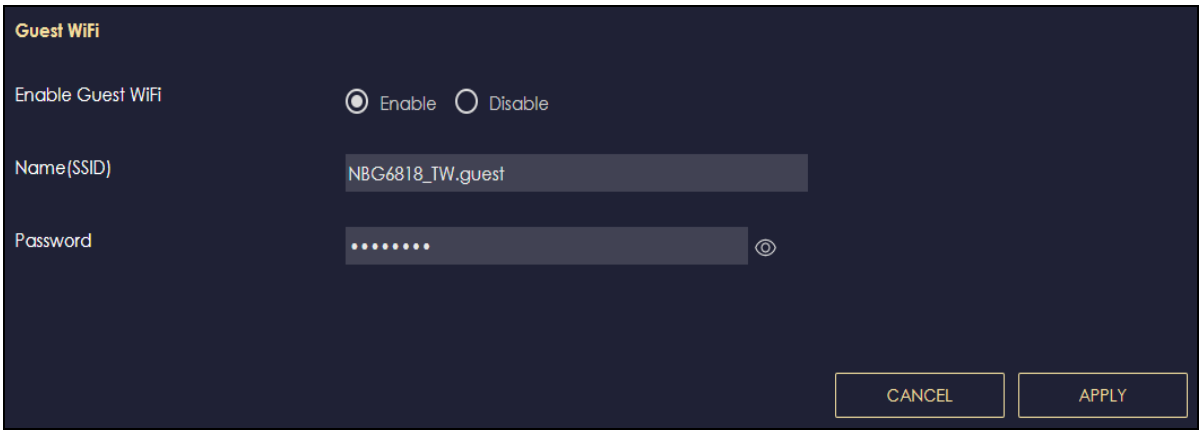


7.4 Enable or Disable a WiFi Network

After the NBG6818 is set up, you can use separate WiFi networks for your clients. The WiFi settings will be applied to all clients in the same network.

1 Click the **Navigation Panel** icon on the top-left corner ( ), and click **Settings** to open the **WiFi** screen.

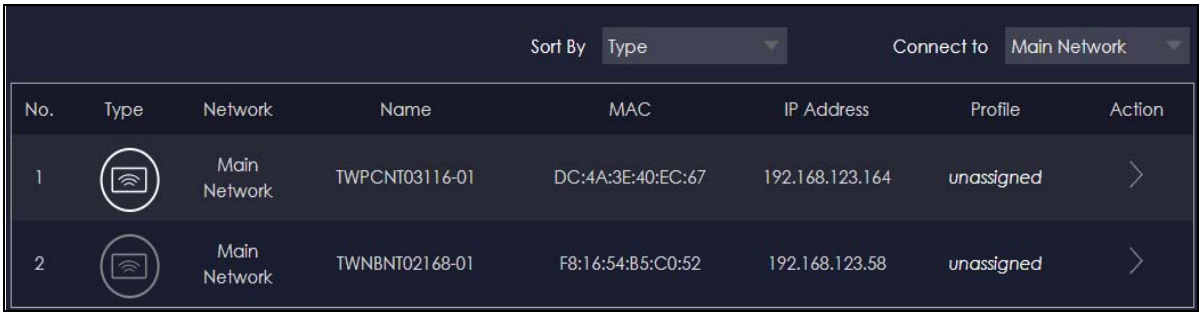
2 Enable guest WiFi and enter the **WiFi Name (SSID)** and **WiFi Password**. Click **APPLY** to save your changes.



7.5 Add Clients to a Profile

Profiling clients allows you to easily block/allow Internet access or set a schedule for all client devices in the same profile.

1 Click the **Navigation Panel** icon on the top-left corner ( ), and click **Parental Control** to open the **Device** screen. Use the **Device** screen to view all the clients in your NBG6818.



PART II
Technical Reference

CHAPTER 8
The Web Configurator

8.1 Overview

This chapter describes how to access the NBG6818 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 NBG6818 via Internet browser. Use Internet Explorer 11 and later versions or Mozilla Firefox 67.0.2 and later versions or Safari 5.0 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 10.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter (Chapter 15 on page 128) to see how to make sure these functions are allowed in Internet Explorer.

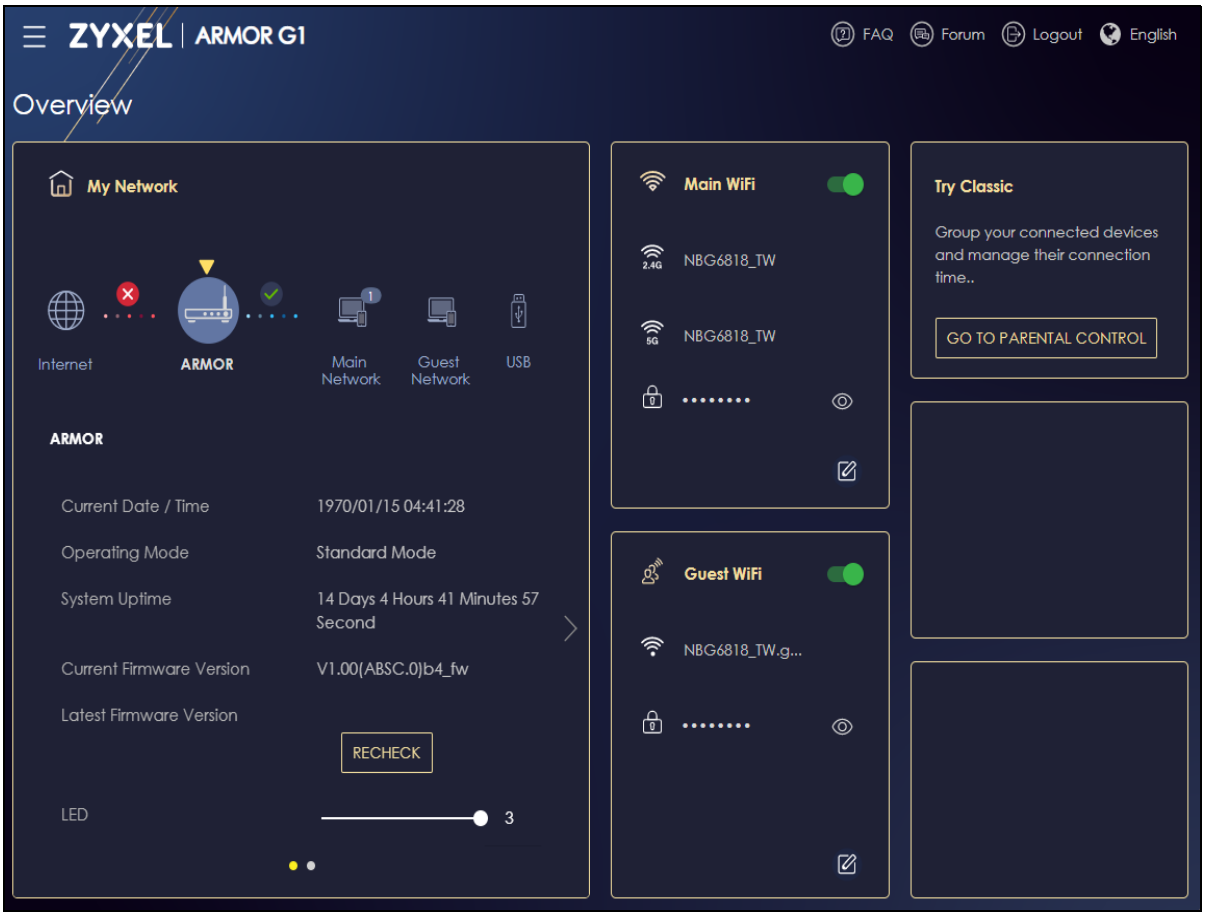
8.2 Accessing the Web Configurator

1. Make sure your NBG6818 hardware is properly connected and prepare your computer or computer network to connect to the NBG6818 (refer to the Quick Start Guide).
2. Launch your web browser.
3. The NBG6818 is in router mode by default. Type "http://zyxelwifi.com" as the website address.
4. A login screen displays. To access the web configurator and manage the NBG6818 you need to be connected to your myZyxelCloud account. Click **Log In** and you will be redirected to the myZyxelCloud website to log into your myZyxelCloud account.


ZYXEL | ARMOR G1
Welcome to the web configurator
Login with myZyxelCloud account
Login with local password
myZyxelCloud
LOG IN

8.3 Add and Install Your NBG6818

The NBG6818 **Overview** screen displays allowing you to monitor your NBG6818. It shows if the NBG6818 is online, and how many wireless clients are currently connected to your device, as well as their upstream/ downstream data rates.



CHAPTER 9 Applications

9.1 Overview

This chapter shows you how to configure parental control, OpenVPN, USB media sharing and file sharing.

9.1.1 What You Can Do

- Use the **Parental Control** screens to enable parental control, configure the parental control rules and schedules, and send e-mail notifications. (Section 9.2 on page 58).
- Use the **OpenVPN Server** screen to (Section 9.3 on page 62).
- Use the **OpenVPN Client** screen (Section 9.4 on page 62).
- Use the **USB Application** screen to allow file sharing or to set up your NBG6818 to act as a media server (Section 9.5 on page 62).

9.1.2 What You Need To Know

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

DLNA

The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network. DLNA clients play files stored on DLNA servers. The NBG6818 can function as a DLNA-compliant media server and stream files to DLNA-compliant media clients without any configuration.

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file-sharing feature on your NBG6818 supports New Technology File System (NTFS), File Allocation Table (FAT) and FAT32 file systems.

The NBG6818 uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the NBG6818. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

Samba

SMB is a client-server protocol used by Microsoft Windows systems for sharing files, printers, and so on.

Samba is a free SMB server that runs on most Unix and Unix-like systems. It provides an implementation of an SMB client and server for use with non-Microsoft operating systems.

File Transfer Protocol

This is a method of transferring data from one computer to another over a network such as the Internet.

9.1.3 Before You Begin

Make sure the NBG6818 is connected to your network and turned on.

1. Connect the USB device to one of the NBG6818's USB ports.
2. The NBG6818 detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by the NBG6818, see the troubleshooting for suggestions.

9.2 Parental Control Screen

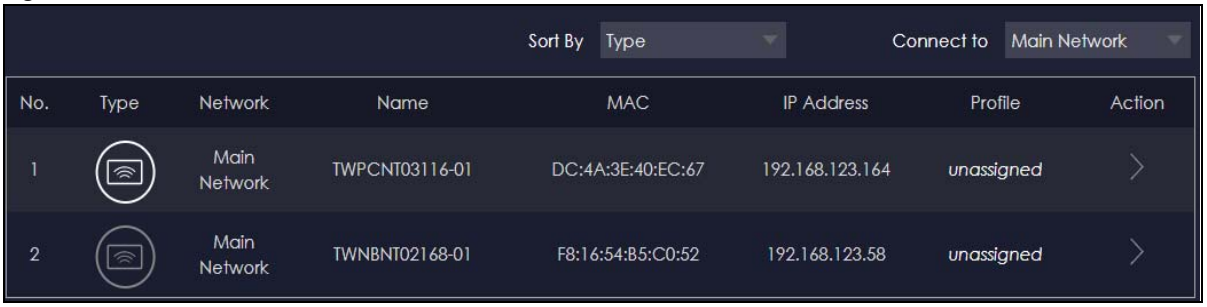
Parental Control allows you to block specific URLs. You can also define time periods and days during which the NBG6818 performs parental control on a specific user.

9.2.1 Device Screen

Use this screen to enable parental control, view the parental control rules and schedules.

Click **Parental Control** > **Device** to show the following screen.

Figure 36 Parental Control > Device



The following table describes the fields in this screen.

Table 18 Parental Control

LABEL	DESCRIPTION
Sort By	
Connect to	
No.	This shows the index number of the rule.
Type	The shows the type of device to which this rule applies.
Network	
Name	This shows the name of the user to which this rule applies.
MAC	This field shows the MAC address of the device with the name in the **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.
IP Address	This field displays the IP address relative to the **No.** field listed above.
Profile	This shows the name of the rule that is applied to the device. If no rule exists, **unassigned** is showed in this field.
Action	Click the **Action** icon ( ) to configure a rule for the device.

9.2.1.1 Device Detail Screen

Use this screen to configure basic settings for the device. Click the **Action** icon ( ), and then the **Edit** icon ( ) to show the following screen.

Figure 37 Device Detail

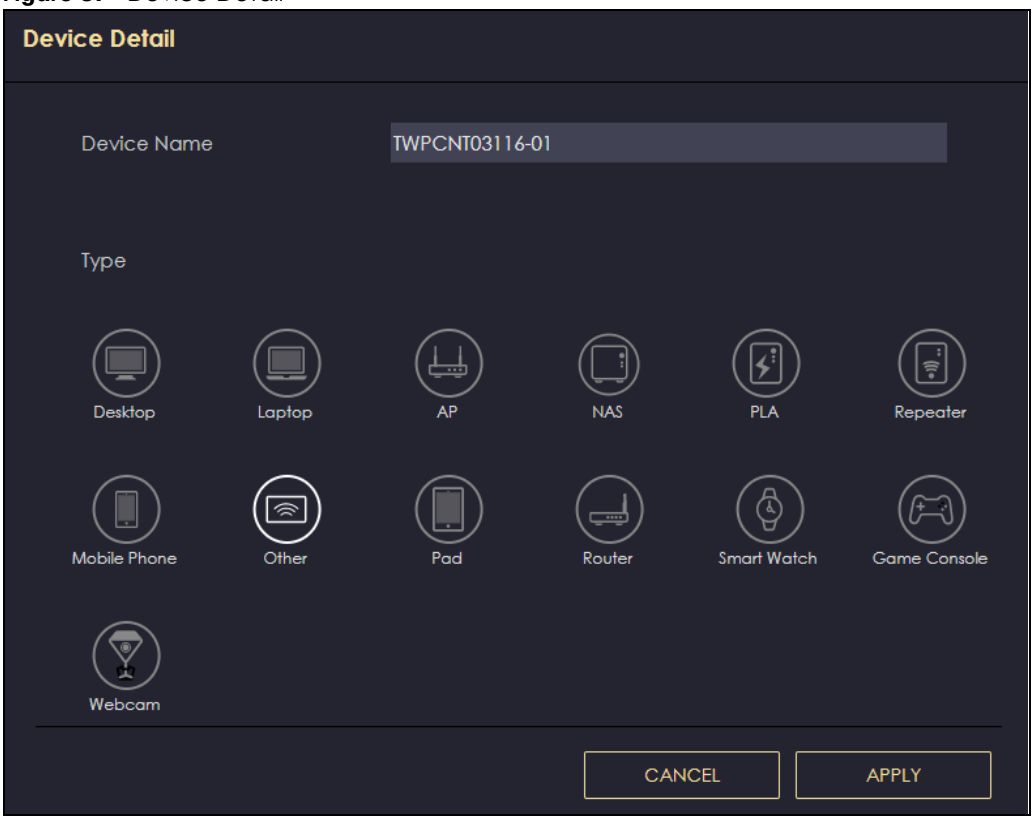


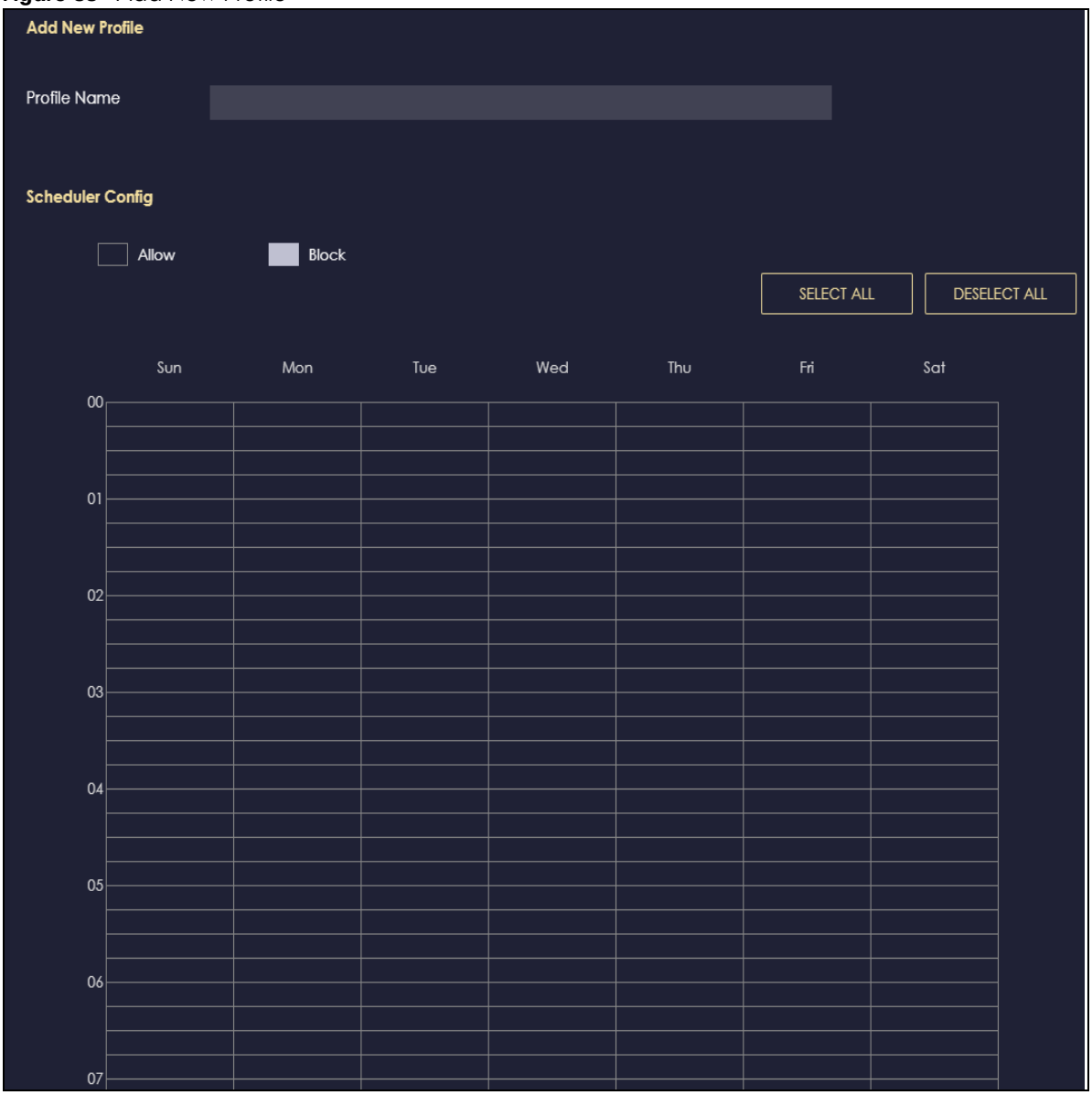
Table 19 Device Detail

LABEL	DESCRIPTION
Device Name	Enter a name for the device to which this rule applies.
Type	Choose the type of device to which this rule applies.
Apply	Click **Apply** to save your settings back to the NBG6818.
Cancel	Click **Cancel** to exist the screen without saving.

9.2.1.2 Add New Profile Screen

Use this screen to configure a restricted access schedule. Click the **Action** icon ( ), then **Add New Profile** to show the following screen.

Figure 38 Add New Profile



The following table describes the fields in this screen.

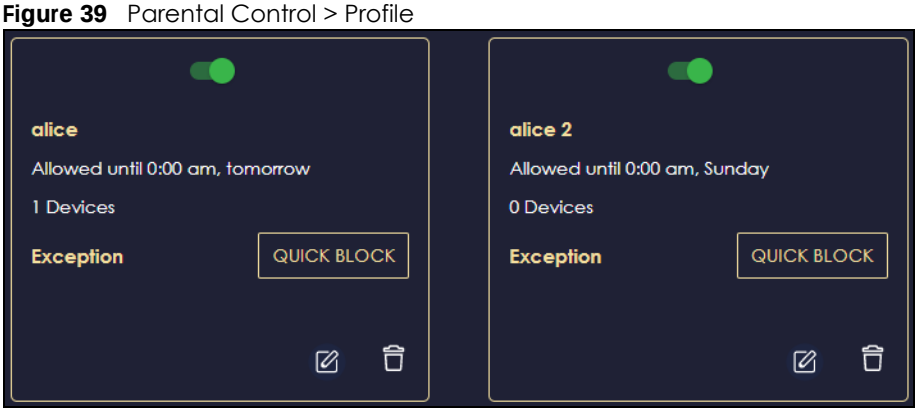
Table 20 Add New Profile

LABEL	DESCRIPTION
Profile Name	Enter a name for this rule.
Select All	Click **Select All** or click gray blocks to specify days and times to turn the Wireless LAN on or off. If you click **Select All** you can not select any specific days and times.
Deselect All	Click **Deselect All** to remove all the wireless LAN scheduling.
Apply	Click **Apply** to save your changes back to the NBG6818.
Back	Click **Back** to exist the screen without saving.

9.2.1.3 Profile Screen

Use this screen to edit or delete an existing rule. Click **Parental Control** > **Profile** to show the following screen.

Figure 39 Parental Control > Profile



The following table describes the fields in this screen.

Table 21 Parental Control > Profile

LABEL	DESCRIPTION
Enable/Disable	Set the switch to the right ( ) to enable an existing rule. Otherwise, set the switch to the left ( ).
Quick Block	
Edit	Click on the **Edit** icon to edit an existing rule.
Delete	Click on the **Delete** icon to delete an existing rule.

9.3 OpenVPN Server Screen

9.4 OpenVPN Client Screen

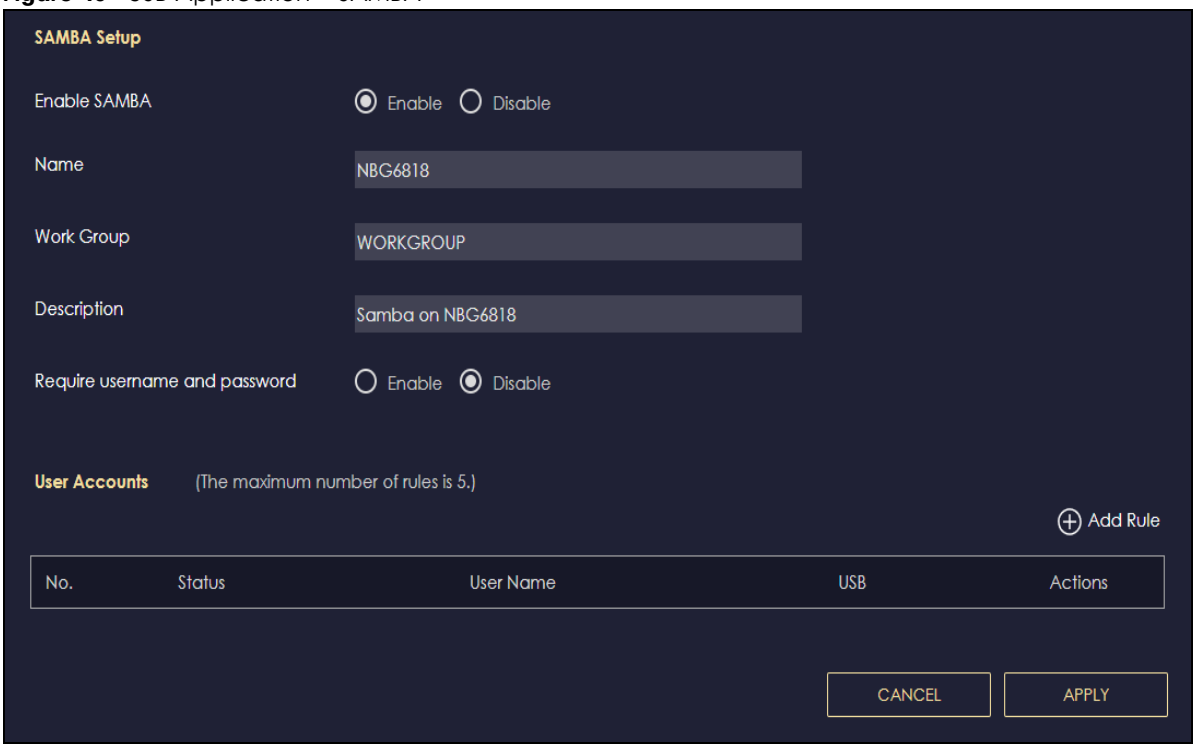
9.5 USB Application Screen

9.5.1 SAMBA Server Screen

Use this screen to set up file-sharing via the NBG6818 using Windows Explorer or the workgroup name. You can also configure the workgroup name and create file-sharing user accounts.

Click **USB Application > SAMBA** to show the following screen.

Figure 40 USB Application > SAMBA



The following table describes the labels in this screen.

Table 22 USB Application > SAMBA

LABEL	DESCRIPTION
SAMBA Setup	
Enable SAMBA	Select this to enable file sharing through the NBG6818 using Windows Explorer or by browsing to your work group.
Name	Specify the name to identify the NBG6818 in a work group.
Work Group	You can add the NBG6818 to an existing or a new workgroup on your network. Enter the name of the workgroup which your NBG6818 automatically joins. You can set the NBG6818's workgroup name to be exactly the same as the workgroup name to which your computer belongs to. Note: The NBG6818 will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.
Description	Enter the description of the NBG6818 in a work group.
Require username and password	Select **Yes** to need a user account for access to the connected USB stick from any computer. Otherwise, select **No**.
User Accounts	Before you can share files you need a user account. Configure the following fields to set up a file-sharing account.
No.	This is the index number of the user account.
Status	This field displays whether a user account is activated or not.
User Name	This field displays the user name that will be allowed to access the shared files.
USB	This field displays the user's access rights to the USB storage device which is connected to the NBG6818's USB port.

Table 22 USB Application > SAMBA (continued)

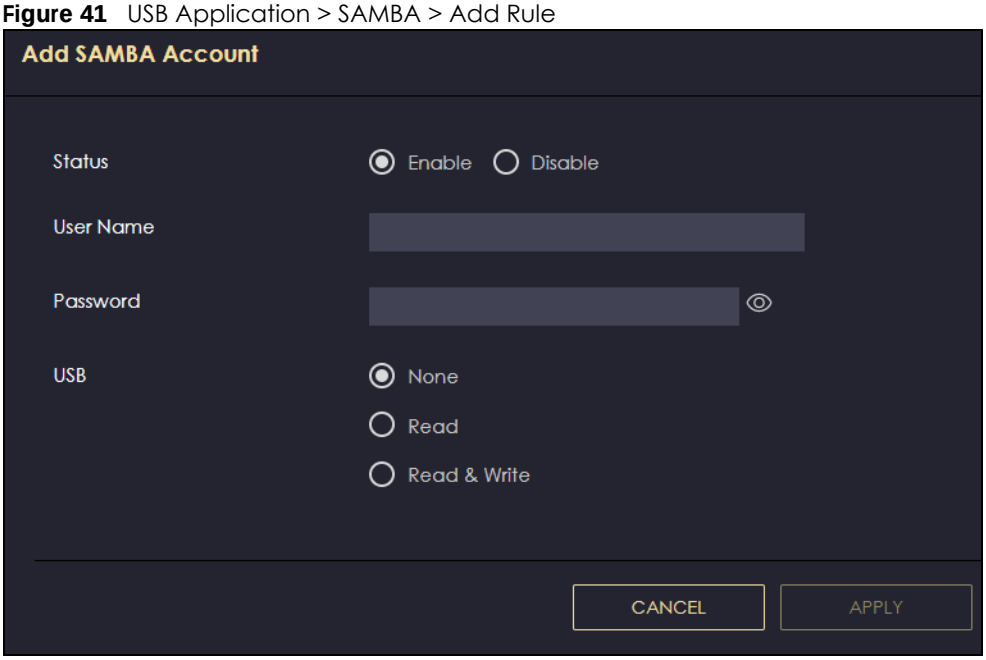
LABEL	DESCRIPTION
Actions	Click the icons under **Actions** to delete or edit a port forwarding rule. Click to delete an existing trigger port settings. Click to edit an existing trigger port settings.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.5.1.1 Add SAMBA Account Screen

Use this screen to configure settings for a SAMBA account.

Click **USB Application** > **SAMBA** > **Add Rule** to show the following screen.

Figure 41 USB Application > SAMBA > Add Rule



The following table describes the labels in this screen.

Table 23 USB Application > SAMBA > Add Rule

LABEL	DESCRIPTION
Status	Select **Enable** to enable the account. Select **Disable** to disable the account.
User Name	Enter a user name that will be allowed to access the shared files. You can enter up to 20 characters. Only letters and numbers allowed.
Password	Enter the password used to access the shared files. You can enter up to 20 characters. Only letters and numbers are allowed. The password is case sensitive.

Table 23 USB Application > SAMBA > Add Rule

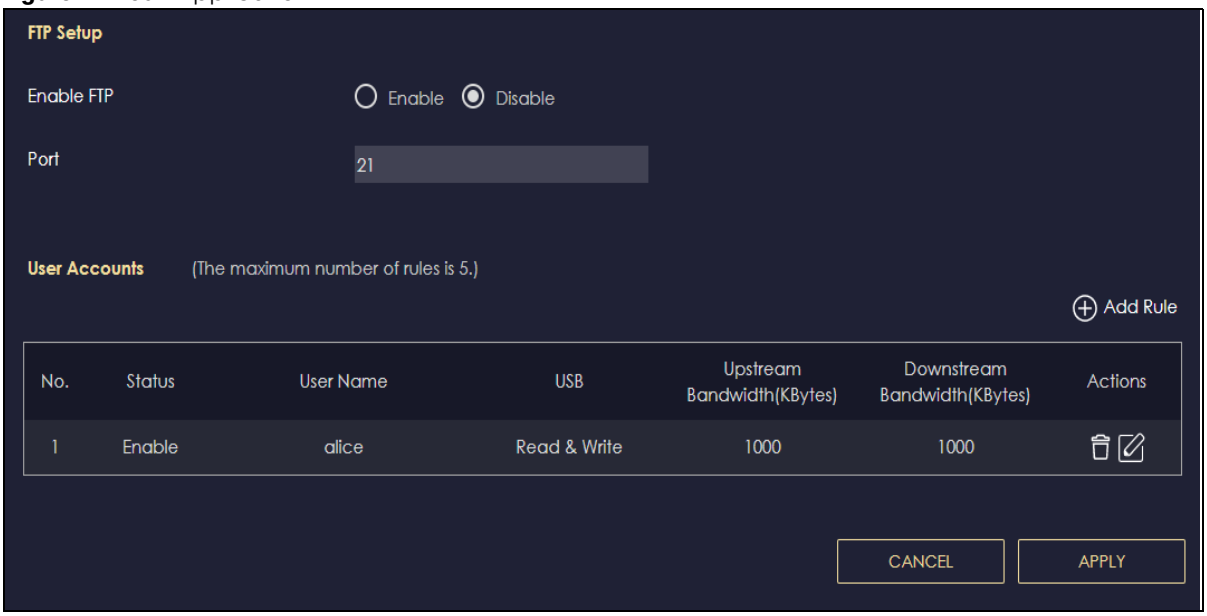
LABEL	DESCRIPTION
USB	Specify the user's access rights to the USB storage device which is connected to the NBG6818's USB port. **Read & Write** - The user has read and write rights, meaning that the user can create and edit the files on the connected USB device. **Read** - The user has read rights only and can not create or edit the files on the connected USB device. **None** - The user cannot access the files on the USB device(s) connected to the USB port.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to exist the screen without saving.

9.5.2 FTP Server Screen

Use this screen to set up file sharing via the NBG6818 using FTP and create user accounts.

Click **USB Application** > **FTP** to show the following screen.

Figure 42 USB Application > FTP



The following table describes the labels in this screen.

Table 24 Expert Mode > Applications > File Sharing > FTP

LABEL	DESCRIPTION
Enable FTP	Select this to enable the FTP server on the NBG6818 for file sharing using FTP.
Port	You may change the server port number for FTP if needed, however you must use the same port number in order to use that service for file sharing.
User Accounts	Before you can share files you need a user account. Configure the following fields to set up a file-sharing account.
No.	This is the index number of the user account.

Table 24 Expert Mode > Applications > File Sharing > FTP (continued)

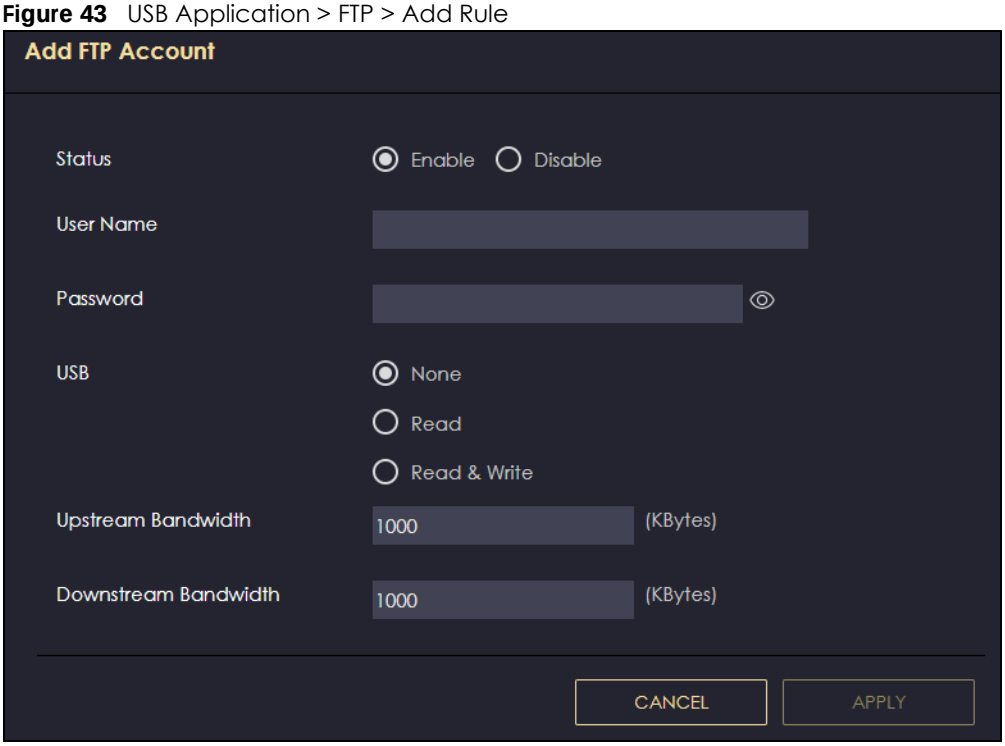
LABEL	DESCRIPTION
Status	This field displays whether a user account is activated or not. Select the check box to enable the account. Clear the check box to disable the account.
User Name	This field displays the user name that will be allowed to access the shared files.
USB	This field displays the user's access rights to the USB storage device which is connected to the NBG6818's USB port.
Upstream Bandwidth	This field shows the maximum bandwidth (in Kbps) allowed for incoming FTP traffic.
Downstream Bandwidth	This field shows the maximum bandwidth (in Kbps) allowed for outgoing FTP traffic.
Actions	Click the icons under **Actions** to delete or edit a port forwarding rule. Click to delete an existing trigger port settings. Click to edit an existing trigger port settings.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.5.2.1 Add FTP Account Screen

Use this screen to configure settings for a FTP account.

Click **USB Application** > **FTP** > **Add Rule** to show the following screen.

Figure 43 USB Application > FTP > Add Rule



The following table describes the labels in this screen.

Table 25 USB Application > FTP > Add Rule

LABEL	DESCRIPTION
Status	Select **Enable** to enable the account. Select **Disable** to disable the account.
User Name	Enter a user name that will be allowed to access the shared files. You can enter up to 20 characters. Only letters and numbers allowed.
Password	Enter the password used to access the shared files. You can enter up to 20 characters. Only letters and numbers are allowed. The password is case sensitive.
USB	Specify the user's access rights to the USB storage device which is connected to the NBG6818's USB port. **Read & Write** - The user has read and write rights, meaning that the user can create and edit the files on the connected USB device. **Read** - The user has read rights only and can not create or edit the files on the connected USB device. **None** - The user cannot access the files on the USB device(s) connected to the USB port.
Upstream Bandwidth	Enter the maximum bandwidth (in Kbps) allowed for incoming FTP traffic.
Downstream Bandwidth	Enter the maximum bandwidth (in Kbps) allowed for outgoing FTP traffic.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to exist the screen without saving.

9.5.3 USB Media Sharing Screen

You can set up your NBG6818 to act as a media server to provide media (like video) to DLNA-compliant players, such as Windows Media Player, Zyxel DMAs (Digital Media Adapters), Xboxes or PS3s. The media server and clients must have IP addresses in the same subnet.

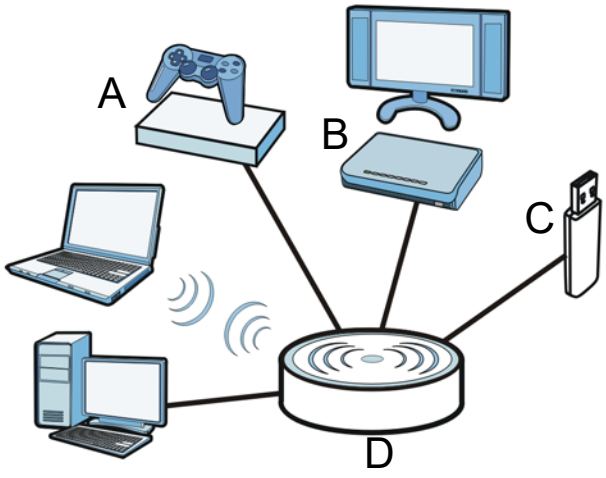
The NBG6818 media server enables you to:

- Publish all folders for everyone to play media files in the USB storage device connected to the NBG6818.
- Use hardware-based media clients like the DMA-2500 to play the files.

Note: Anyone on your network can play the media files in the published folders. No user name and password nor other form of security is required.

The following figure is an overview of the NBG6818's media server feature. DLNA devices **A** and **B** can access and play files on a USB device (**C**) which is connected to the NBG6818 (**D**).

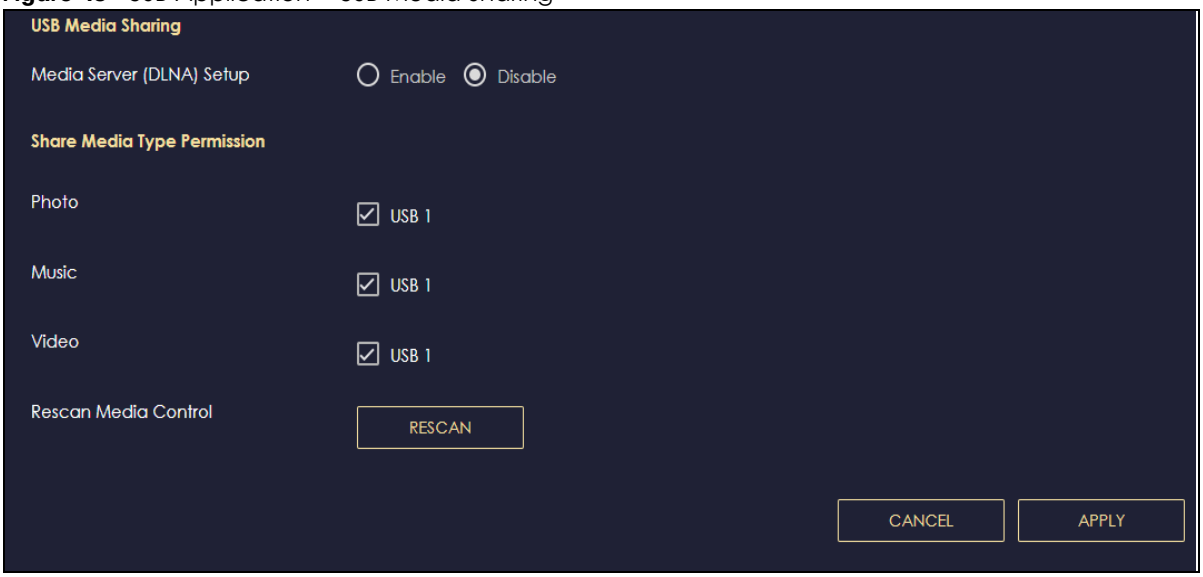
Figure 44 Media Server Overview



Use this screen to have the NBG6818 act as a DLNA-compliant media server that lets DLNA-compliant media clients on your network play video, music, and photos from the NBG6818 (without having to copy them to another computer).

Click **USB Application** > **USB Media Sharing** to show the following screen.

Figure 45 USB Application > USB Media Sharing



The following table describes the labels in this screen.

Table 26 USB Application > USB Media Sharing

LABEL	DESCRIPTION
USB Media Sharing	
Media Server (DLNA) Setup	Choose **Enable** to have the NBG6818 function as a DLNA-compliant media server. Otherwise, choose **Disable**.
Share Media Type Permission	
Photo/Music/Video	Select the media type that you want to share on the USB device connected to the NBG6818's USB port.

Table 26 USB Application > USB Media Sharing (continued)

LABEL	DESCRIPTION
Rescan Media Control	
Rescan	Click this button to have the NBG6818 scan the media files on the connected USB device and do indexing of the file list again so that DLNA clients can find the new files if any.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.6 Access Your Shared Files From a Computer

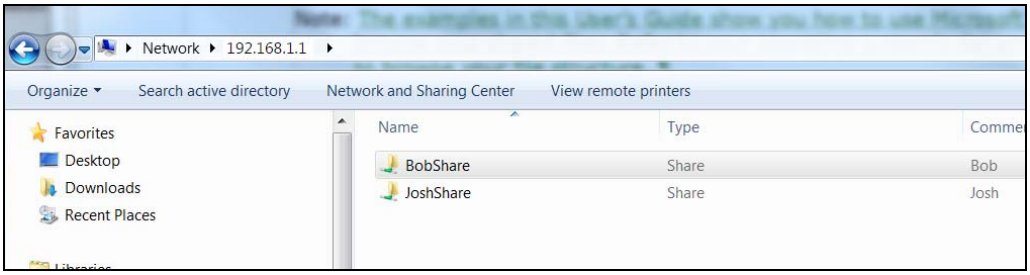
9.6.1 Using Windows Explorer

You can use Windows Explorer to access the file storage devices connected to the NBG6818.

Note: The examples in this User's Guide show you how to use Microsoft's Windows 7 to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

Open Windows Explorer to access **BobShare** using the Windows Explorer browser.

In the Windows Explorer's address bar type a double backslash "\\" followed by the IP address of the NBG6818 (the default IP address of the NBG6818 is 192.168.1.1) and press [ENTER]. The share folder **BobShare** is available.



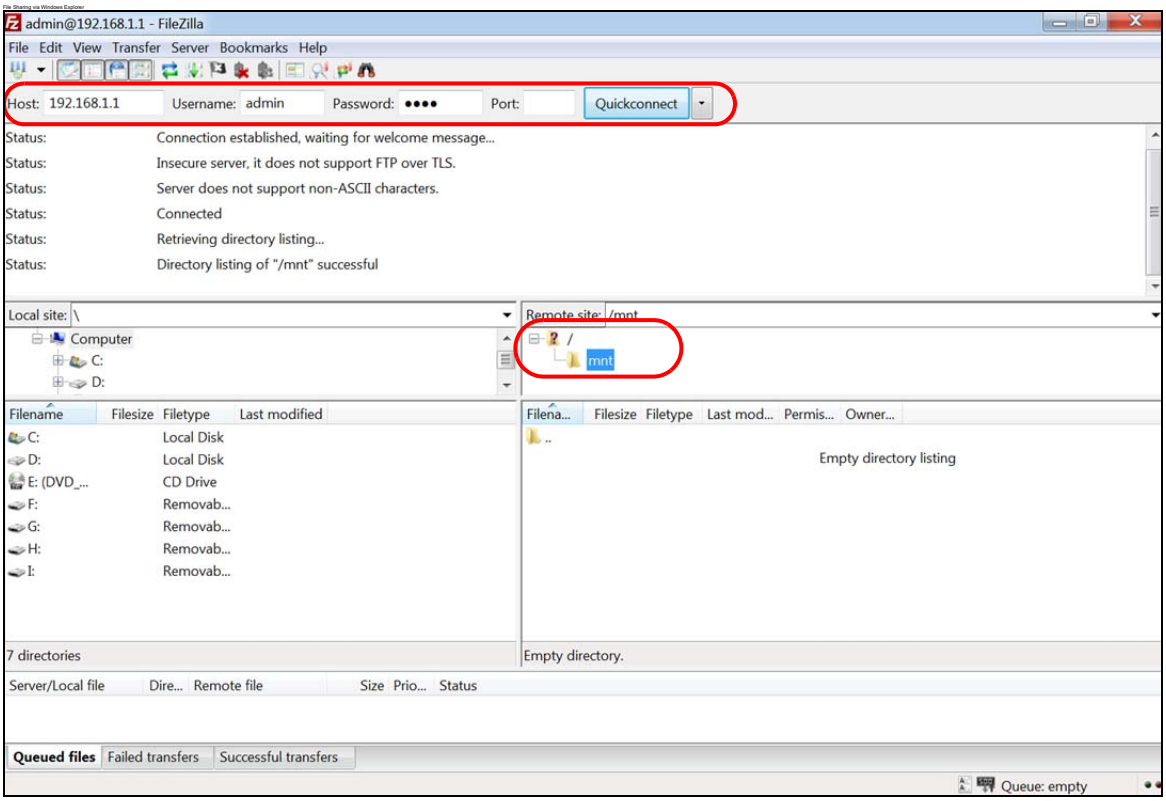
Once you access **BobShare** via your NBG6818, you do not have to relogin unless you restart your computer.

9.6.2 Using FTP Program

Here is how to use an FTP program to access a file storage device connected to the NBG6818's USB port.

Note: This example uses the FileZilla FTP program to browse your shared files.

1 In FileZilla enter the IP address of the NBG6818 (the default is 192.168.1.1), your account's user name and password and port 21 and click **Quickconnect**. A screen asking for password authentication appears.



2 Once you log in the USB device displays in the **mnt** folder.

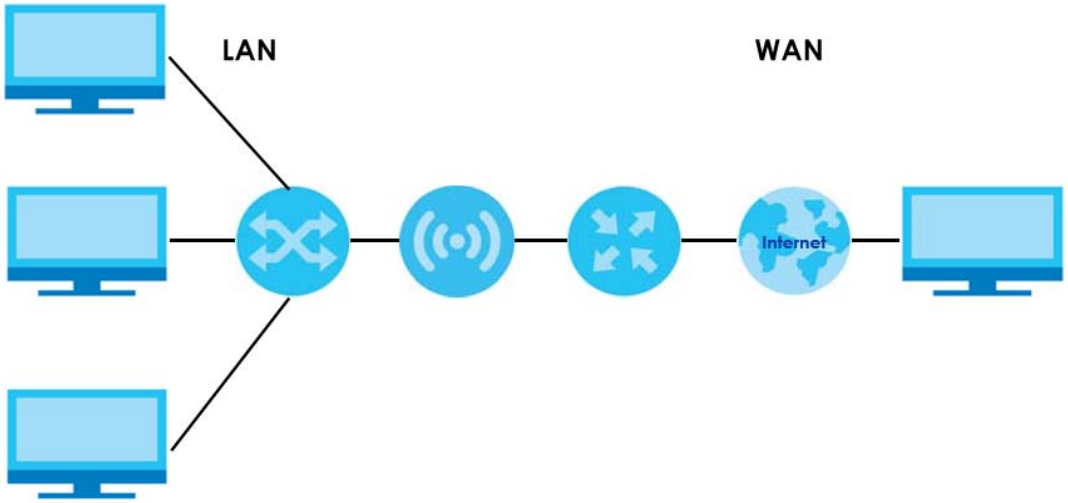
CHAPTER 10
WAN

10.1 Overview

This chapter discusses the NBG6818's **WAN** screens. Use these screens to configure your NBG6818 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 46 LAN and WAN



10.2 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 10.4 on page 73).
- Use the **NAT & Port Forwarding** screen to enable NAT, set a default server and change your NBG6818's port forwarding settings (Section 10.5 on page 81).
- Use the **Passthrough** screen to configure your NBG6818's ALGs and VPN pass-through settings (Section 10.6 on page 83)
- Use the **Port Trigger** screen to configure your NBG6818's trigger port settings (Section 10.7 on page 85).
- Use the **Dynamic DNS** screen to change your NBG6818's DDNS settings (Section 10.8 on page 87).
- Use the **UPnP** screen to enable UPnP on your NBG6818 (Section 10.9 on page 88).

10.3 What You Need To Know

The information in this section can help you configure the screens for your WAN connection, as well as enable/disable some advanced features of your NBG6818.

10.3.1 Configuring Your Internet Connection

Encapsulation Method

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

WAN IP Address

The WAN IP address is an IP address for the NBG6818, which makes it accessible from an outside network. It is used by the NBG6818 to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the NBG6818 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 NBG6818 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 NBG6818's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

WAN MAC Address

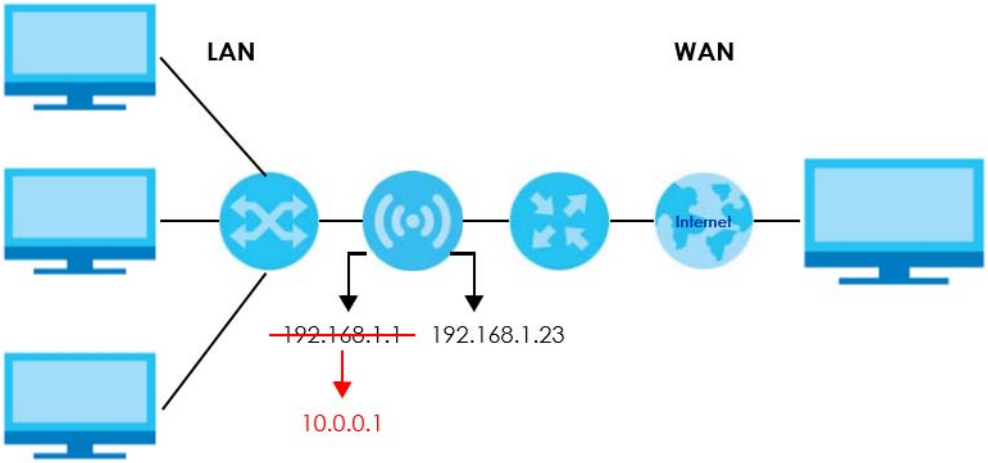
The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

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.

Auto-IP Change

When the NBG6818 gets a WAN IP address or a DNS server IP address which is in the same subnet as the LAN IP address 192.168.1.1, Auto-IP-Change allows the NBG6818 to change its LAN IP address to 10.0.0.1 automatically. If the NBG6818's original LAN IP address is 10.0.0.1 and the WAN IP address is in the same subnet, such as 10.0.0.3, the NBG6818 switches to use 192.168.1.1 as its LAN IP address.

Figure 47 Auto-IP-Change Example



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

- The NBG6818 must be in **Router Mode** (see Section 14.7 on page 125 for more information) for Auto-IP-Change to become active.
- The NBG6818 is set to receive a dynamic WAN IP address.

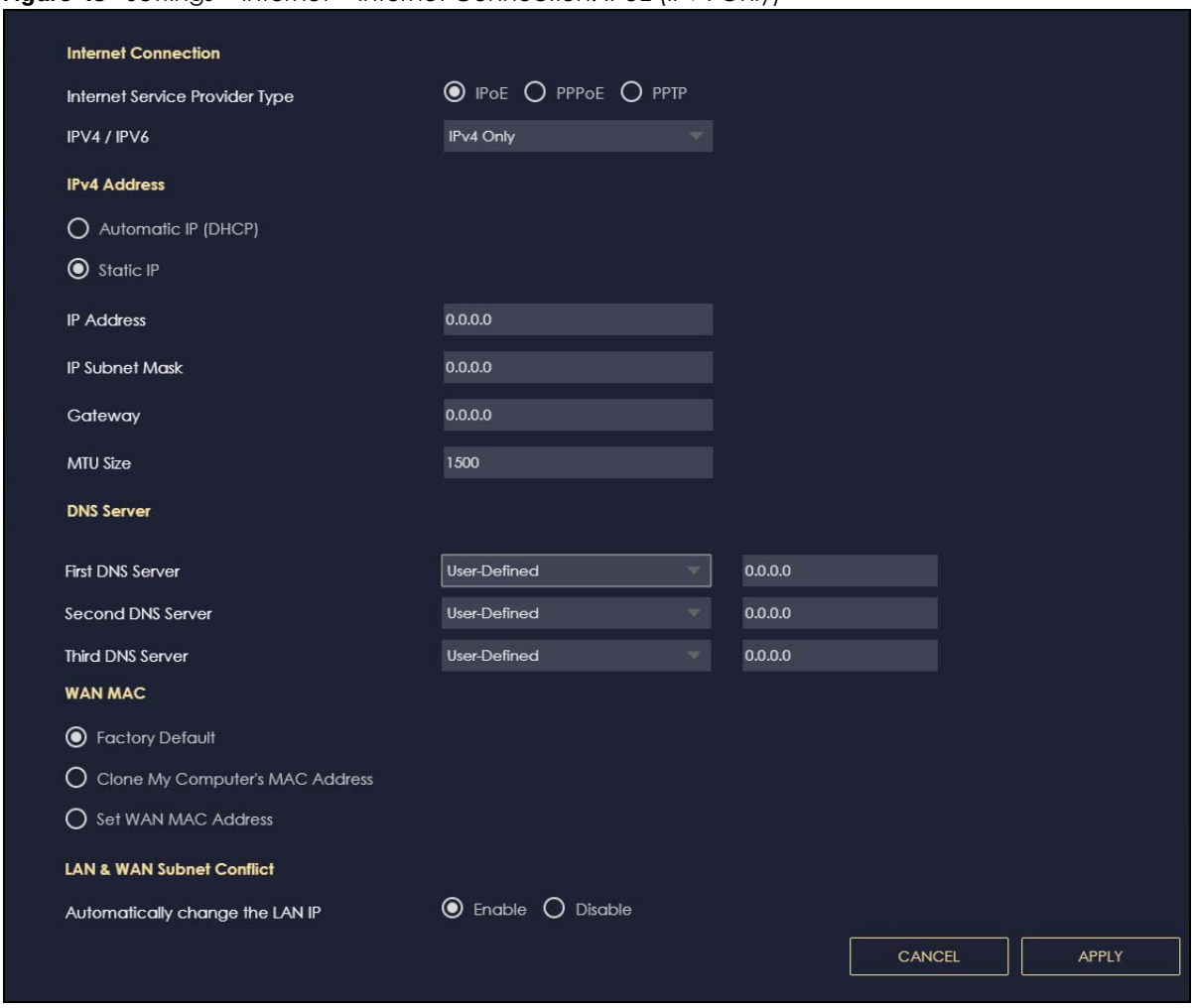
10.4 Internet Connection Screen

Use this screen to change your NBG6818's Internet access settings. The screen varies depending on the encapsulation method you select. Click **Settings** > **Internet** > **Internet Connection**.

10.4.1 IPoE Encapsulation

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

Figure 48 Settings > Internet > Internet Connection: IPoE (IPv4 Only)



The following table describes the labels in this screen.

Table 27 Network > WAN > Internet Connection: IPoE Encapsulation

LABEL	DESCRIPTION
Internet Connection	
Internet Service Provider Type	You must choose the **IPoE** option when the WAN port is used as a regular Ethernet.
IPv4 / IPv6	Select **IPv4 Only** if you want the NBG6818 to run IPv4 only. Select **Dual Stack** to allow the NBG6818 to run IPv4 and IPv6 at the same time.
IPv4 Address	
Automatic IP (DHCP)	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Static IP	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**.
IP Subnet Mask	Enter the **Subnet Mask** in this field.
Gateway	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 NBG6818 divides it into smaller fragments.
DNS Server	

Table 27 Network > WAN > Internet Connection: IPoE Encapsulation (continued)

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. 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 Once the WAN MAC address is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.	
Factory Default	Select this option to have the WAN interface use the factory assigned default MAC address. By default, the NBG6818 uses the factory assigned MAC address to identify itself.
Clone My Computer's MAC Address	Select this option to have the WAN interface use a different MAC address by cloning the MAC address of another device or computer. Enter the IP address of the device or computer whose MAC you are cloning.
Set WAN MAC Address	Select this option to have the WAN interface use a manually specified MAC address. Enter the MAC address in the fields.
LAN & WAN Subnet Conflict	
Automatically change the LAN IP	Select this option to have the NBG6818 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG6818 gets a dynamic WAN IP address in the same subnet as the LAN IP address. See Section 10.3.1 on page 72 for more information. The NAT, DHCP server and firewall functions on the NBG6818 are still available in this mode.
IPv6 Address This section is NOT available when you select **IPv4 Only** in the **IPv4/IPv6** field.	
Automatic IP (DHCP)	Select this option if you want to obtain an IPv6 address from a DHCPv6 server. • Select **DUID-LL (Default)** to have the NBG6818 use DUID-LL (DUID Based on Link-layer Address) for identification when exchanging DHCPv6 messages. • Select **DUID-LLT** to have the NBG6818 use DUID-LLT (DUID Based on Link-layer Address Plus Time) for identification when exchanging DHCPv6 messages.
Static IP Address	Select this option if you have a fixed IPv6 address assigned by your ISP.
IPv6 Address	Enter the IPv6 address assigned by your ISP.
Prefix length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
Gateway	Enter the IPv6 address of the next-hop gateway. The gateway helps forward packets to their destinations.
Link Local Only	Select this option to use the link-local address which uniquely identifies a device on the local network (the LAN).
IPv6 DNS Server This section is NOT available when you select **IPv4 Only** in the **IPv4/IPv6** field.	
First DNS Server Second DNS Server Third DNS Server	Select **User-Defined** and enter the IPv6 DNS server address assigned by the ISP to have the NBG6817 use the IPv6 DNS server addresses you configure manually. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IPv6 address of a computer in order to access it.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.4.2 PPPoE Encapsulation

The NBG6818 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).

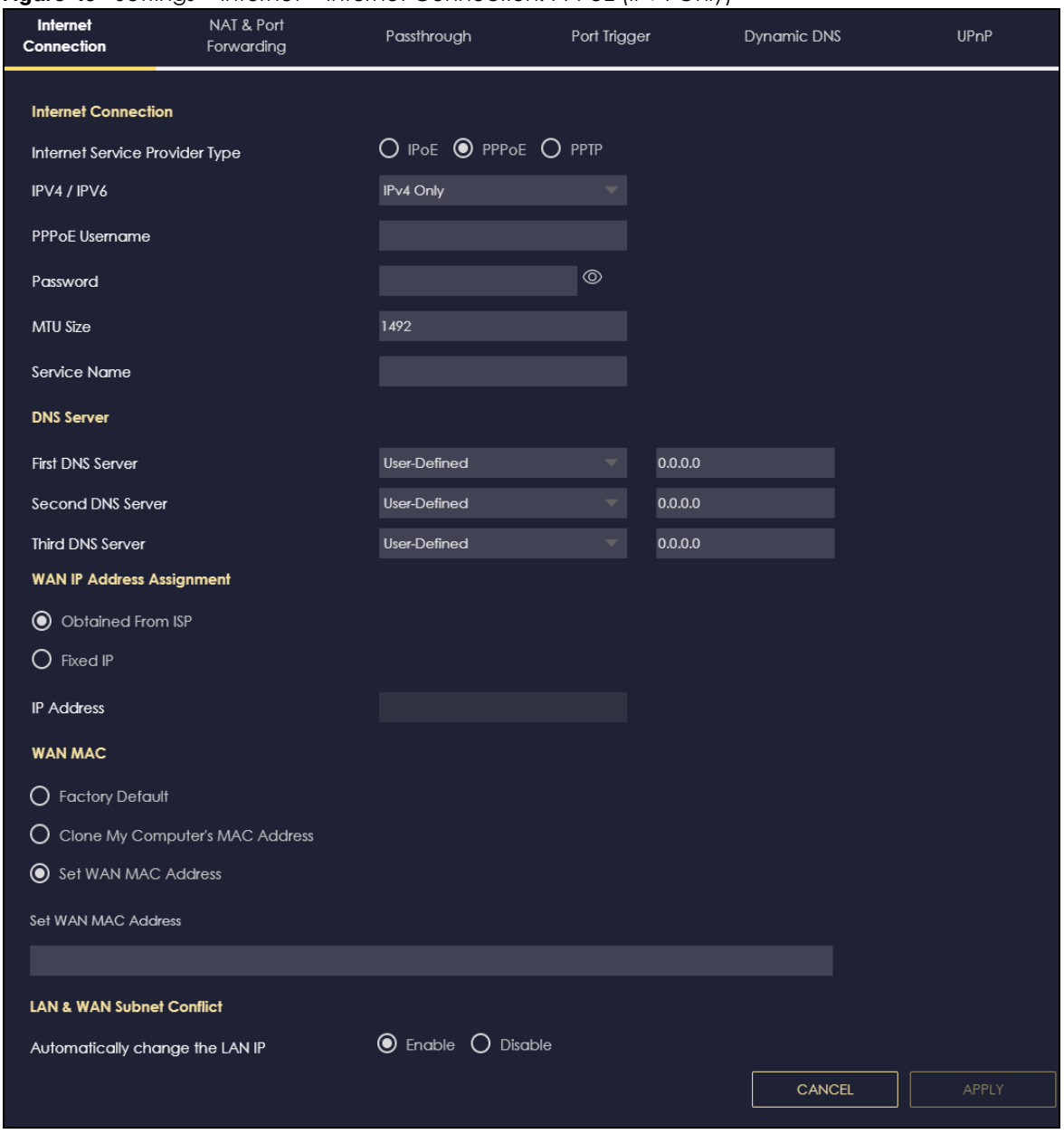
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

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 NBG6818 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG6818 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 49 Settings > Internet > Internet Connection: PPPoE (IPv4 Only)



The following table describes the labels in this screen.

Table 28 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
Internet Connection	
Internet Service Provider Type	Select **PPPoE** if you connect to your Internet via dial-up.
IPv4 / IPv6	Select **IPv4 Only** if you want the NBG6818 to run IPv4 only. Select **Dual Stack** to allow the NBG6818 to run IPv4 and IPv6 at the same time.
PPPoE Username	Type the user name given to you by your ISP.

Table 28 Network > WAN > Internet Connection: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
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 NBG6818 can receive and process.
Service Name	Enter the PPPoE service name specified in the ISP account.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. 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 IP Address Assignment	
Obtained from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Fixed IP	Select this option and enter your WAN IP address if the ISP assigned a fixed IP address.
WAN MAC Address The MAC address section allows users to configure the WAN port's MAC address by using the NBG6818'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 My Computer's MAC 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.
IPv6 Address This section is NOT available when you select **IPv4 Only** in the **IPv4/IPv6** field.	
Automatic IP (DHCP)	Select this option if you want to obtain an IPv6 address from a DHCPv6 server. • Select **DUID-LL (Default)** to have the NBG6818 use DUID-LL (DUID Based on Link-layer Address) for identification when exchanging DHCPv6 messages. • Select **DUID-LLT** to have the NBG6818 use DUID-LLT (DUID Based on Link-layer Address Plus Time) for identification when exchanging DHCPv6 messages.
Static IP Address	Select this option if you have a fixed IPv6 address assigned by your ISP.
IPv6 Address	Enter the IPv6 address assigned by your ISP.
Prefix length	Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.
Gateway	Enter the IPv6 address of the next-hop gateway. The gateway helps forward packets to their destinations.
Link Local Only	Select this option to use the link-local address which uniquely identifies a device on the local network (the LAN).
IPv6 DNS Server This section is NOT available when you select **IPv4 Only** in the **IPv4/IPv6** field.	
First DNS Server Second DNS Server Third DNS Server	Select **User-Defined** and enter the IPv6 DNS server address assigned by the ISP to have the NBG6818 use the IPv6 DNS server addresses you configure manually. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IPv6 address of a computer in order to access it.
LAN & WAN Subnet Conflict	

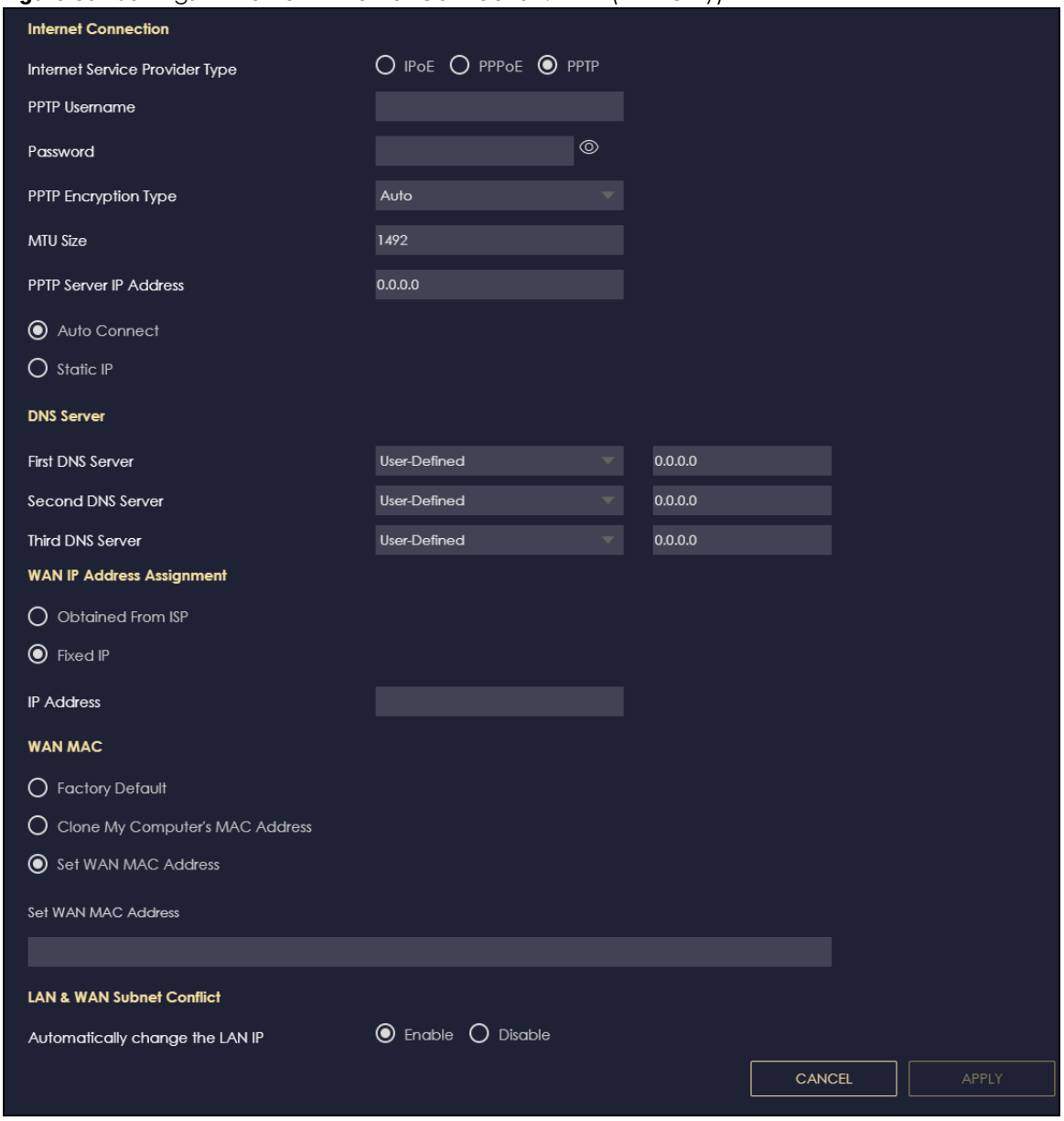
Table 28 Network > WAN > Internet Connection: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
Automatically change the LAN IP	Select this option to have the NBG6818 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG6818 gets a dynamic WAN IP address in the same subnet as the LAN IP address. See Section 10.3.1 on page 72 for more information. The NAT, DHCP server and firewall functions on the NBG6818 are still available in this mode.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.4.3 PPTP Encapsulation

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

Figure 50 Settings > Internet > Internet Connection: PPTP (IPv4 Only)



The following table describes the labels in this screen.

Table 29 Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
Internet Connection	
Internet Service Provider Type	Select **PPTP** if you want to connect the Internet via point to point tunneling protocol.
PPTP Username	Enter the user name given to you by your ISP.
Password	Enter the password associated with the user name above.
PPTP Encryption Type	Use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: **Auto** - This ISP account adjusts the encryption type automatically. **None** - This ISP account does not use MPPE. **40** - This ISP account uses 40-bit MPPE. **128** - This ISP account uses 128-bit MMPE.
MTU Size	Enter the MTU (Maximum Transmission Unit) size for each packet. If a larger packet arrives, the NBG6818 divides it into smaller fragments.
PPTP Server IP Address	Enter the IP address of the PPTP server.
Auto Connect	Select this radio button if the PPTP server did not assign you a fixed IP address.
Static IP	Select this radio button if the PPTP server assigned an IP address for your Internet connection.
IP Address	Enter the IP address provided by the PPTP server.
IP Subnet Mask	Enter the IP subnet mask in this field.
Gateway	Enter the gateway IP address in this field.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. 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 IP Address Assignment	
Obtained from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Fixed IP	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **IP Address**.
WAN MAC Address Once the WAN MAC address is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.	
Factory Default	Select this option to have the WAN interface use the factory assigned default MAC address. By default, the NBG6818 uses the factory assigned MAC address to identify itself.
Clone My Computer's MAC Address	Select this option to have the WAN interface use a different MAC address by cloning the MAC address of another device or computer. Enter the IP address of the device or computer whose MAC you are cloning.
Set WAN MAC Address	Select this option to have the WAN interface use a manually specified MAC address. Enter the MAC address in the fields.
LAN & WAN Subnet Conflict	

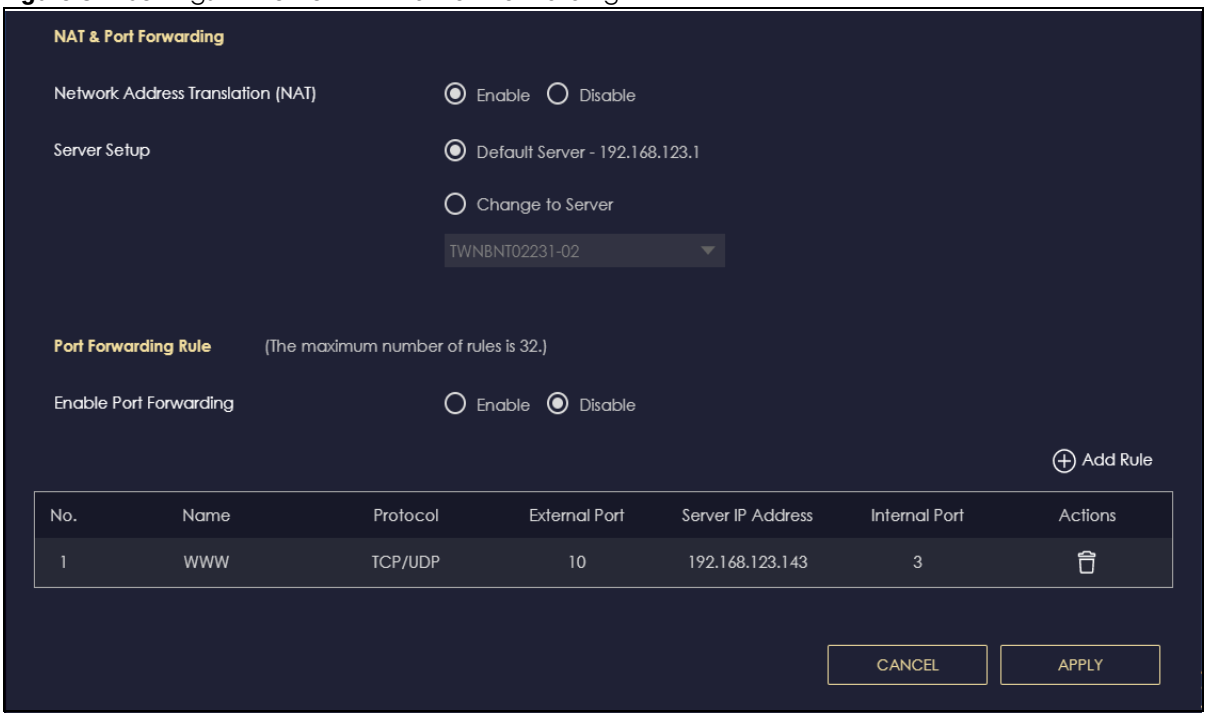
Table 29 Network > WAN > Internet Connection: PPTP Encapsulation (continued)

LABEL	DESCRIPTION
Automatically change the LAN IP	Select this option to have the NBG6818 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG6818 gets a dynamic WAN IP address in the same subnet as the LAN IP address. See Section 10.3.1 on page 72 for more information. The NAT, DHCP server and firewall functions on the NBG6818 are still available in this mode.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.5 NAT & Port Forwarding Screen

Use this screen to enable NAT, set a default server and view the summary table of your NBG6818's port forwarding settings. Click **Settings** > **Internet** > **NAT & Port Forwarding** to show the following screen.

Figure 51 Settings > Internet > NAT & Port Forwarding



The following table describes the labels in this screen.

Table 30 Expert Mode > WAN > NAT > General

LABEL	DESCRIPTION
NAT & Port Forwarding	
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.
Server Setup	

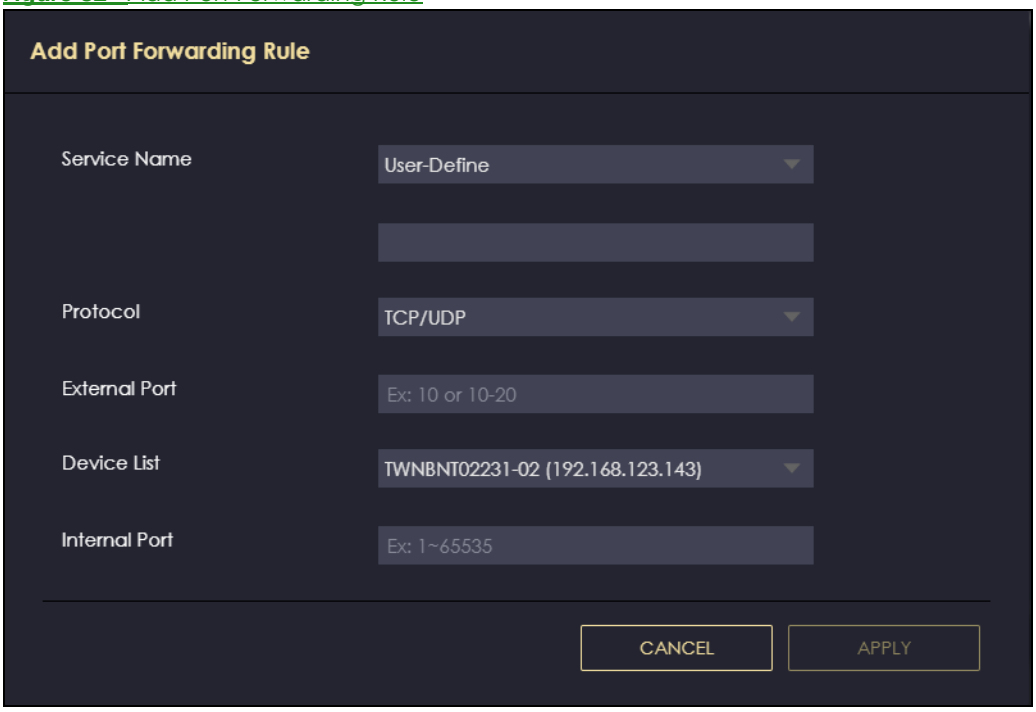
Table 30 Expert Mode > WAN > NAT > General (continued)

LABEL	DESCRIPTION
Default Server	You can decide whether you want to use the default server or specify a server manually. 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 summary table below. Select this to use the default server.
Change To Server	Select this and manually enter the server's IP address.
Port Forwarding Rule	
Enable Port Forwarding	Select **Enable** to allow port forwarding. Otherwise, select **Disable**.
No.	This is the number of an individual port forwarding server entry.
Name	This field displays a name to identify this rule.
Protocol	This is the transport layer protocol used for the service.
External Port	This shows the port number(s) that identifies the service if you select a pre-defined service.
Server IP Address	This field displays the inside IP address of the server.
Internal Port	This shows the port number(s) that identifies the service if you select a pre-defined service.
Actions	Click the icons under **Actions** to delete or edit a port forwarding rule. Click to delete an existing trigger port settings. Click to edit an existing trigger port settings.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.5.1 Add Port Forwarding Rule Screen

Use this screen to configure your NBG6818's port forwarding settings to forward incoming service requests to the server(s) on your local network. Click **Settings** > **Internet** > **NAT & Port Forwarding**> **Add Rule** to show the following screen.

Figure 52 Add Port Forwarding Rule



The following table describes the labels in this screen.

Table 31 Add Port Forwarding Rule

LABEL	DESCRIPTION
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/range and select the **Protocol**.
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.
External Port	This shows the port number(s) that identifies the service if you select a pre-defined service. If you select **User-Define** in the **Service Name** field, enter the port number(s) manually.
Device List	Select the inside IP address of the virtual server.
Internal Port	This shows the port number(s) that identifies the service if you select a pre-defined service. If you select **User-Define** in the **Service Name** field, enter an internal port number manually or leave the field blank for port range forwarding.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exist this screen without saving.

10.6 Passthrough Screen

Use this screen to change your NBG6818's ALGs and VPN pass-through settings. Click **Settings** > **Internet** > **Passthrough** to show the following screen.

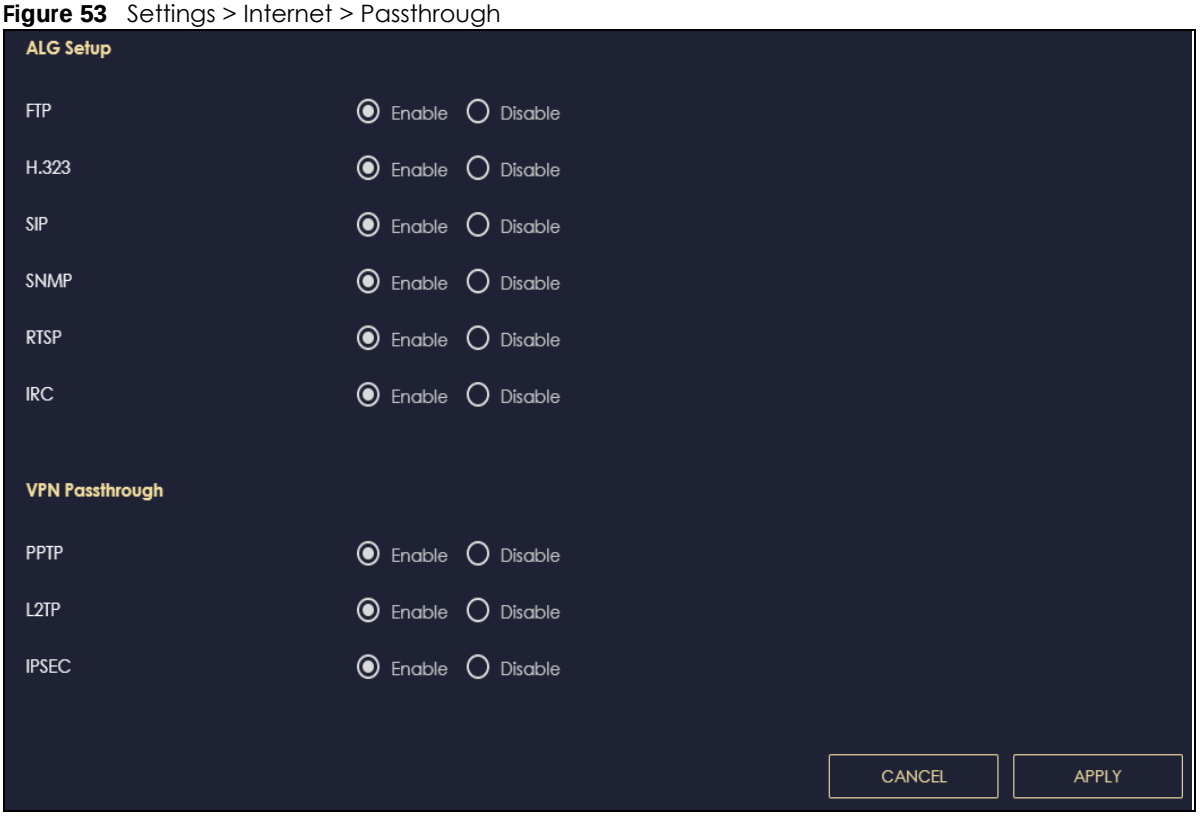
ALG Overview

Application Layer Gateway (ALG) allows the following applications to operate properly through the NBG6818's NAT.

- SIP - Session Initiation Protocol (SIP) - An application-layer protocol that can be used to create voice and multimedia sessions over Internet.
- H.323 - A teleconferencing protocol suite that provides audio, data and video conferencing.
- FTP - File Transfer Protocol - an Internet file transfer service.
- SNMP - Simple Network Management Protocol - An application-layer protocol that can be used to exchange management information between network devices.
- RTSP - Real Time Streaming Protocol - An application-layer protocol that can be used to stop, pause or play video and audio applications streaming on the Internet.
- IRC - Internet Relay Chat - An application-layer protocol that can control the relay chat applications and allow clients to have real-time communications with others on the Internet.

The ALG feature is only needed for traffic that goes through the NBG6818's NAT.

Figure 53 Settings > Internet > Passthrough



The following table describes the labels in this screen.

Table 32 Settings > Internet > Passthrough

LABEL	DESCRIPTION
ALG Setup	
FTP	Select **Enable** to allow TCP packets with a specified port destination to pass through.
H.323	Select **Enable** to allow peer-to-peer H.323 calls.

Table 32 Settings > Internet > Passthrough (continued)

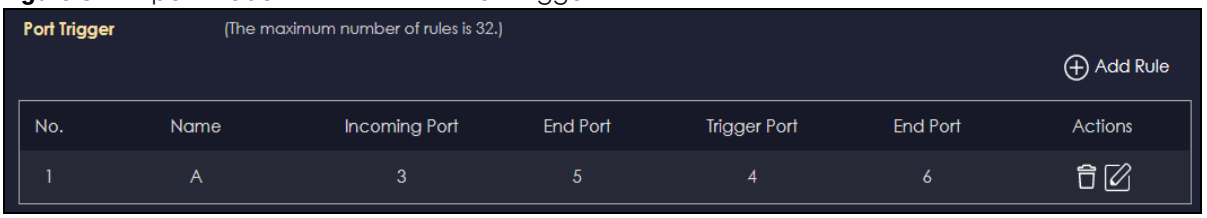
LABEL	DESCRIPTION
SIP	Select **Enable** to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
SNMP	Select **Enable** to allow a manager station to manage and monitor the NBG6818 through the network via SNMP.
RTSP	Select **Enable** to have the NBG6818 detect RTSP traffic and help build RTSP sessions through its NAT.
IRC	Select **Enable** to allow clients to have real-time communications with others on the Internet.
VPN Passthrough	
PPTP	Select **Enable** to allow VPN clients to make outbound PPTP connections. It is required in order to connect to a PPTP VPN account. If **PPTP** is disabled, then when a client sends a request to a VPN server, the server will reply to the NBG6818 and the NBG6818 will drop the request. When **PPTP** is enabled, the NBG6818 will forward the reply from the VPN server to the client that initiated the request, and the connection will establish successfully.
L2TP	Select **Enable** to allow VPN clients to make outbound L2TP connections. It is required in order to connect to a L2TP VPN account. If **L2TP** is disabled, then when a client sends a request to a VPN server, the server will reply to the NBG6818 and the NBG6818 will drop the request. When **L2TP** is enabled, the NBG6818 will forward the reply from the VPN server to the client that initiated the request, and the connection will establish successfully.
IPSEC	Select **Enable** to allow VPN clients to make outbound IPSec connections. It is required in order to connect to a IPSec VPN account. If **IPSEC** is disabled, then when a client sends a request to a VPN server, the server will reply to the NBG6818 and the NBG6818 will drop the request. When **IPSEC** is enabled, the NBG6818 will forward the reply from the VPN server to the client that initiated the request, and the connection will establish successfully.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.7 Port Trigger Screen

Use this screen to view the summary table of your NBG6818's port trigger settings. Click **Expert Mode** > **WAN** > **NAT** > **Port Trigger** to show the following screen.

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

Figure 54 Expert Mode > WAN > NAT > Port Trigger



The following table describes the labels in this screen.

Table 33 Expert Mode > WAN > NAT > Port Trigger

LABEL	DESCRIPTION
Port Trigger Rules (Max Limit: 32)	
No.	This is the rule index number.
Name	This field displays a name to identify this rule.

Table 33 Expert Mode > WAN > NAT > Port Trigger (continued)

LABEL	DESCRIPTION
Incoming Port	This field displays a port number that a server on the WAN uses when it sends out a particular service.
End Port	This field displays a port number or the ending port number in a range of port numbers.
Trigger Port	This field displays a port number that causes the NBG6818 to record the IP address of the LAN computer that sent then traffic to a server on the WAN.
Actions	Click the icons under **Actions** to delete or edit an existing trigger port settings. Click to delete an existing trigger port settings. Click to edit an existing trigger port settings.
End Port	This field displays a port number or the ending port number in a range of port numbers.

10.7.1 Add Port Trigger Rule Screen

Use this screen to configure your NBG6816's port trigger settings. Click **Expert Mode** > **WAN** > **NAT** > **Port Trigger** > **Add Rule** to show the following screen.

Figure 55 Add Port Trigger Rule

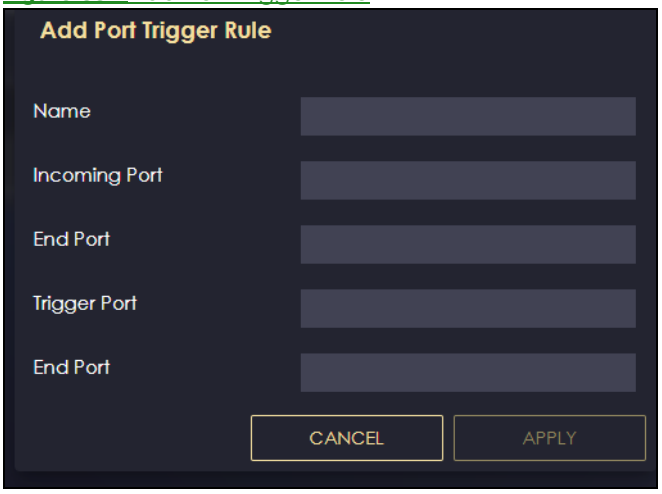


Table 34 Add Port Trigger Rule

LABEL	DESCRIPTION
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming Port	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ARMOR Z1 forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. 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 Port	The trigger port is a port (or a range of ports) that causes (or triggers) the ARMOR Z1 to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.

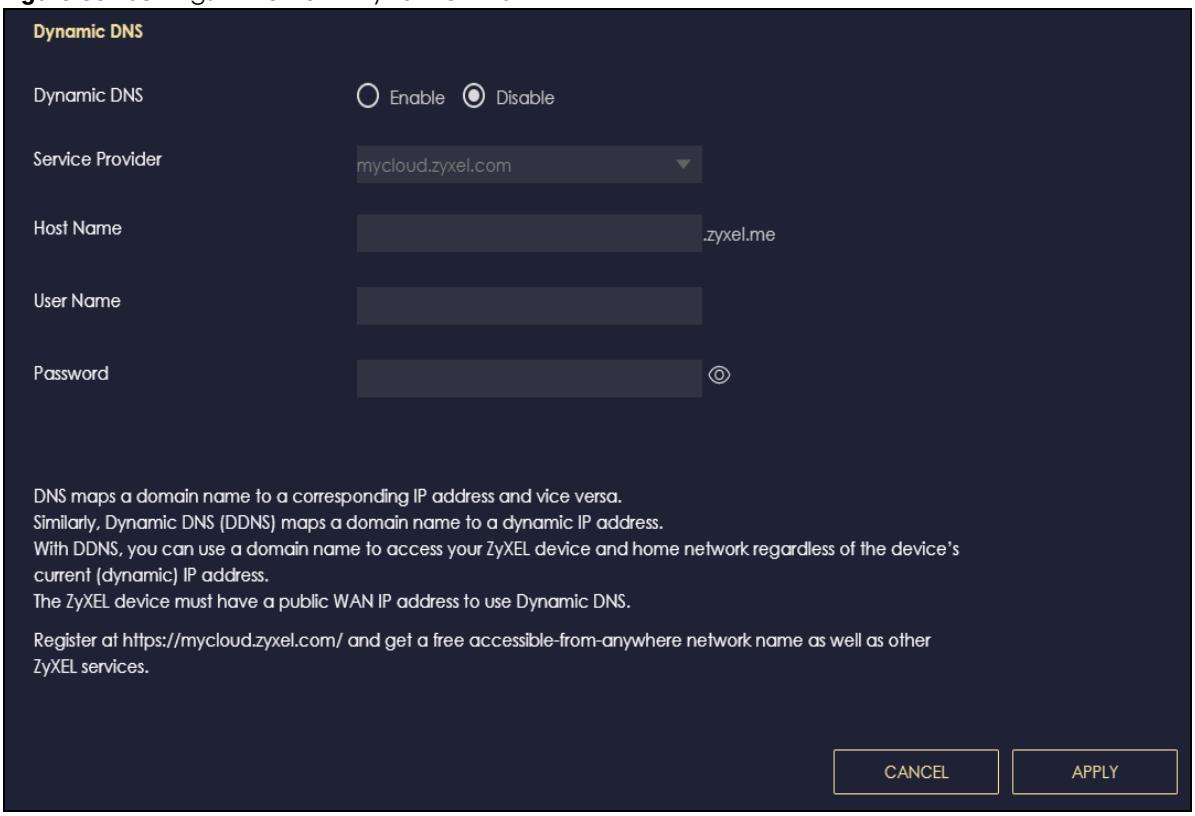
Table 34 Add Port Trigger Rule

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to exist this screen without saving.

10.8 Dynamic DNS Screen

Use this screen to change your NBG6818's DDNS settings. Click **Settings** > **Internet** > **Dynamic DNS** to show the following screen.

Figure 56 Settings> Internet > Dynamic DNS



The following table describes the labels in this screen.

Table 35 Settings > Internet > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
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.

Table 35 Settings > Internet > Dynamic DNS (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.9 UPnP Screen

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. A device can then leave a network smoothly and automatically when it is no longer in use.

See Section 10.9.1 on page 89 and Section 10.9.2 on page 91 for more information on UPnP.

Use this screen to enable UPnP on your NBG6818. Click **Settings** > **Internet** > **UPnP** to display the following screen.

Figure 57 Settings > Internet > UPnP

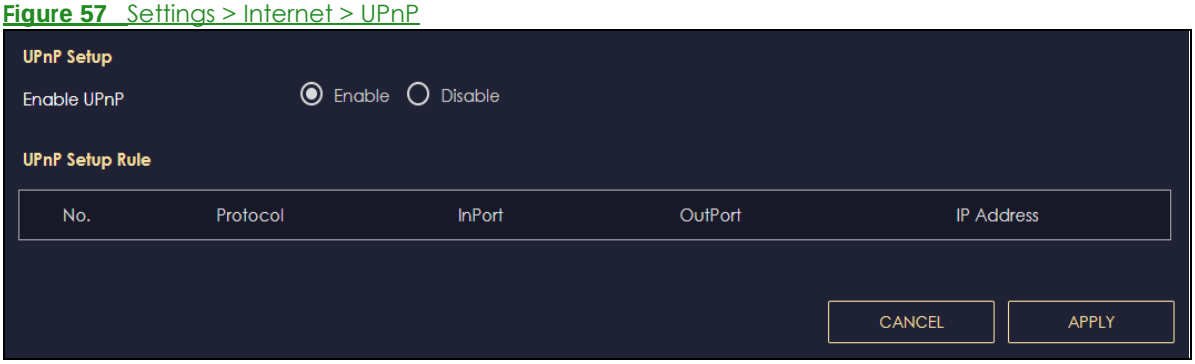


Table 36 Settings > Internet > UPnP

LABEL	DESCRIPTION
UPnP Setup	
Enable 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 NBG6818's IP address (although you must still enter the password to access the web configurator).
UPnP Setup Rule	
No.	This is the number of an individual UPnP entry.
Protocol	This is the transport layer protocol used for the service.
InPort	**InPort** is a port that a LAN computer uses when it requests a particular service. This port is only applicable to the local network. This field displays the port number of the UPnP entry.
OutPort	**OutPort** is the well-known port that the WAN server uses to reply to the LAN computer that made the request using In Port. This field displays the port number of the UPnP entry.
IP Address	This field displays the IP address of this UPnP entry.

Table 36 Settings > Internet > UPnP

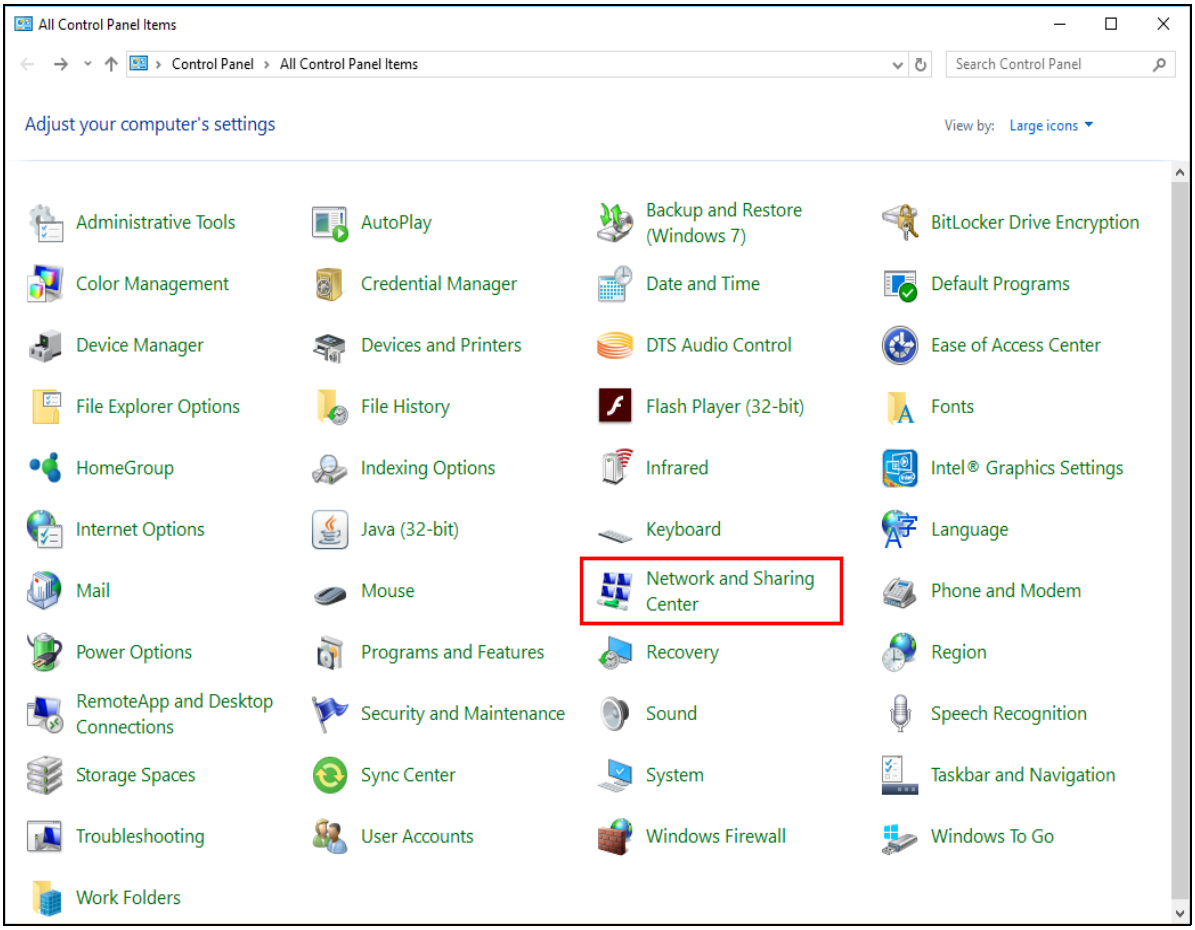
LABEL	DESCRIPTION
Apply	Click **Apply** to save your settings.
Cancel	Click **Cancel** to return to the previously saved settings.

10.9.1 Turning On UPnP in Windows 7 Example

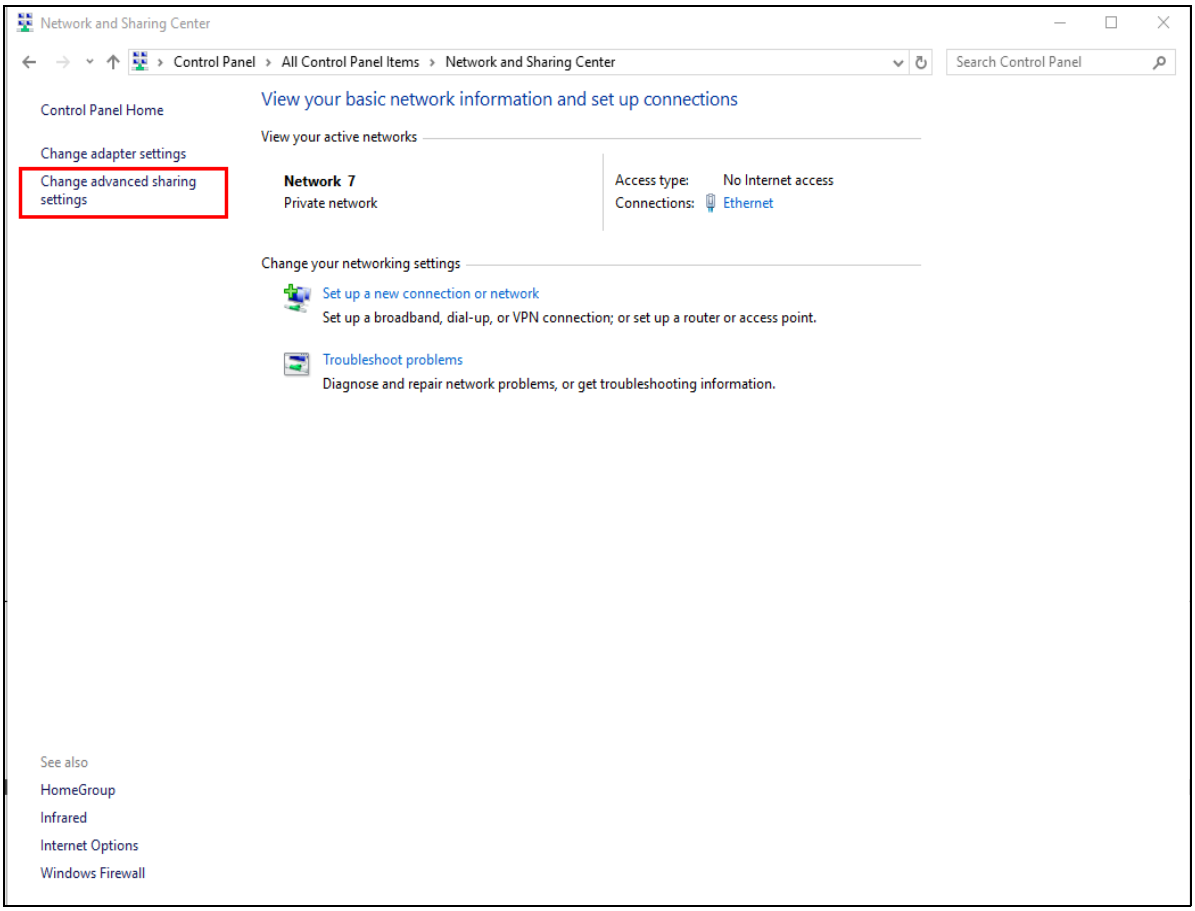
This section shows you how to use the UPnP feature in Windows 7. UPnP server is installed in Windows 7. Activate UPnP on the NBG6818 in **Settings** > **Internet** > **UPnP**.

Make sure the computer is connected to a LAN port of the NBG6818. Turn on your computer and the NBG6818.

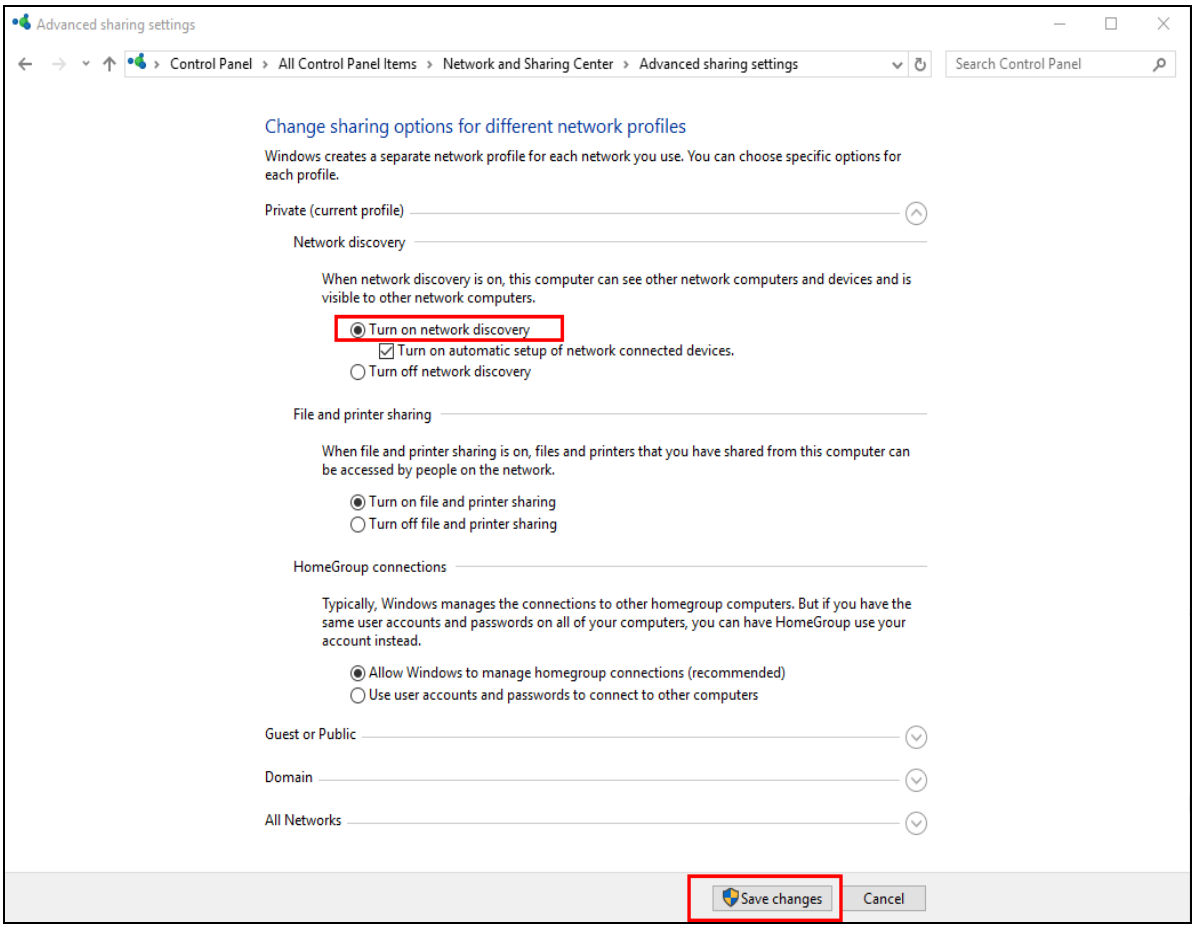
1 Click the start icon, **Control Panel** and then the **Network and Sharing Center**.



2 Click **Change Advanced Sharing Settings**.



3 Select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers.

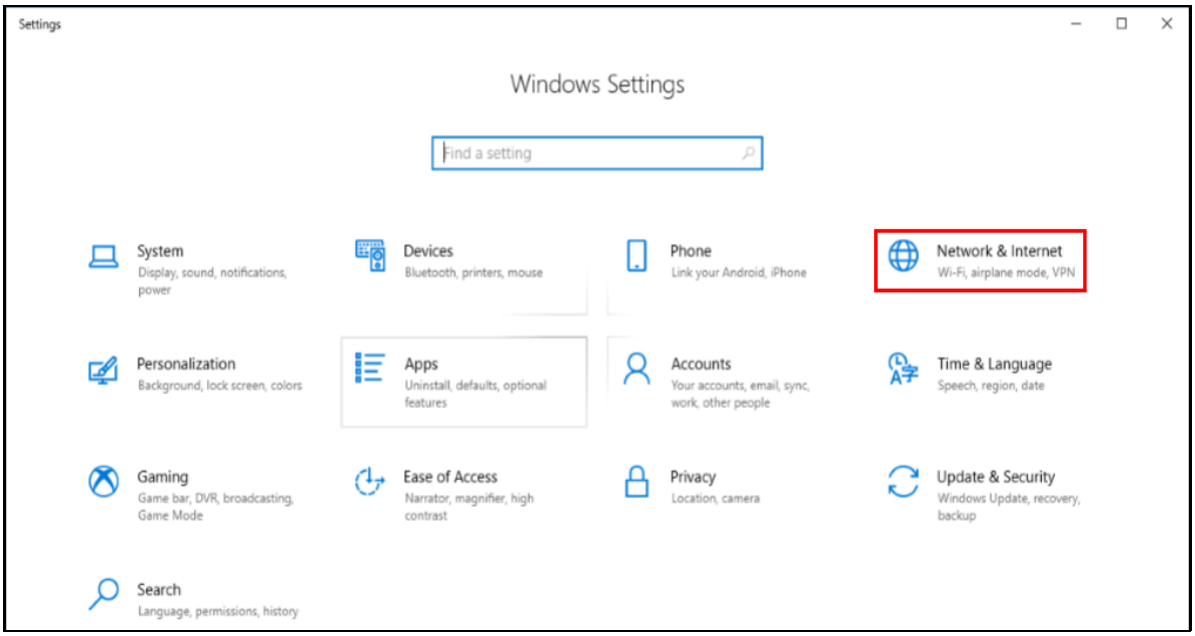


10.9.2 Turning on UPnP in Windows 10 Example

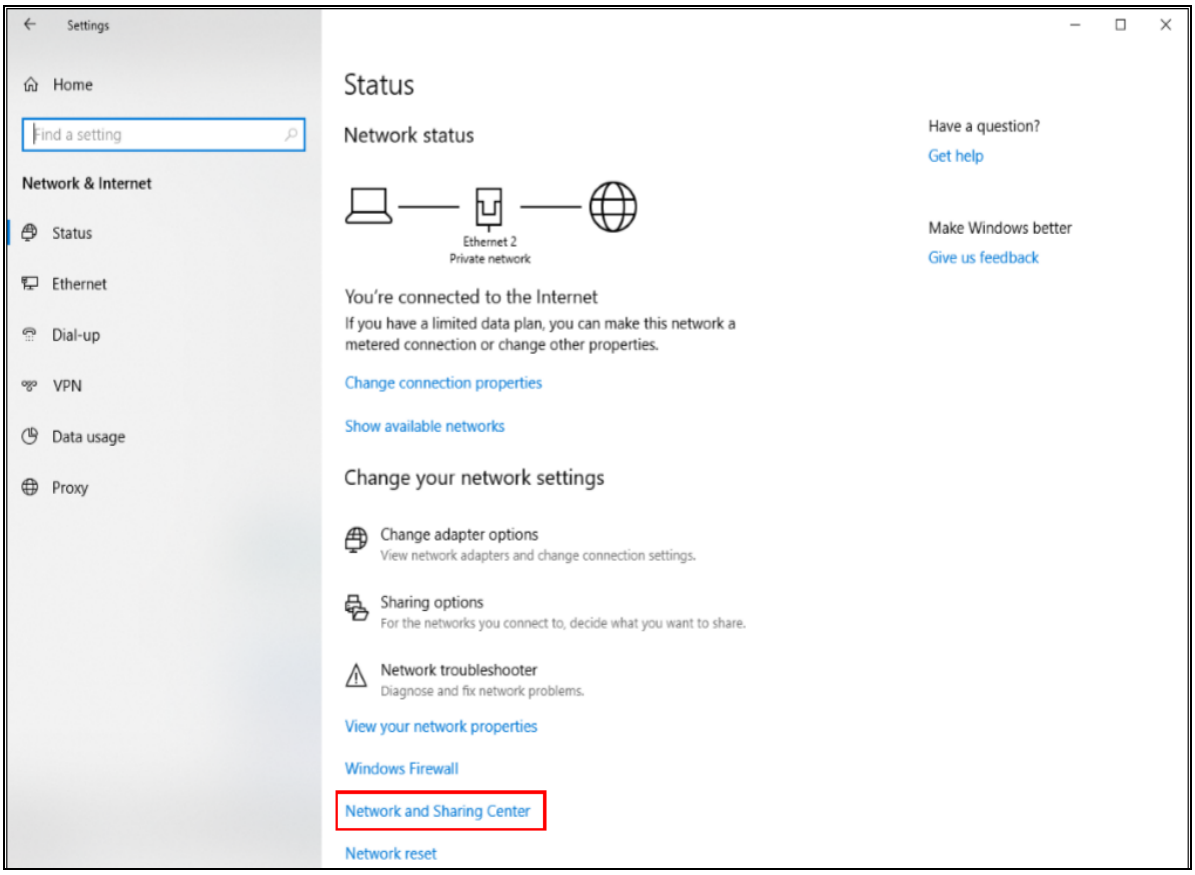
This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the NBG6818 in **Settings** > **Internet** > **UPnP**.

Make sure the computer is connected to the LAN port of the NBG6818. Turn on your computer and the NBG6818.

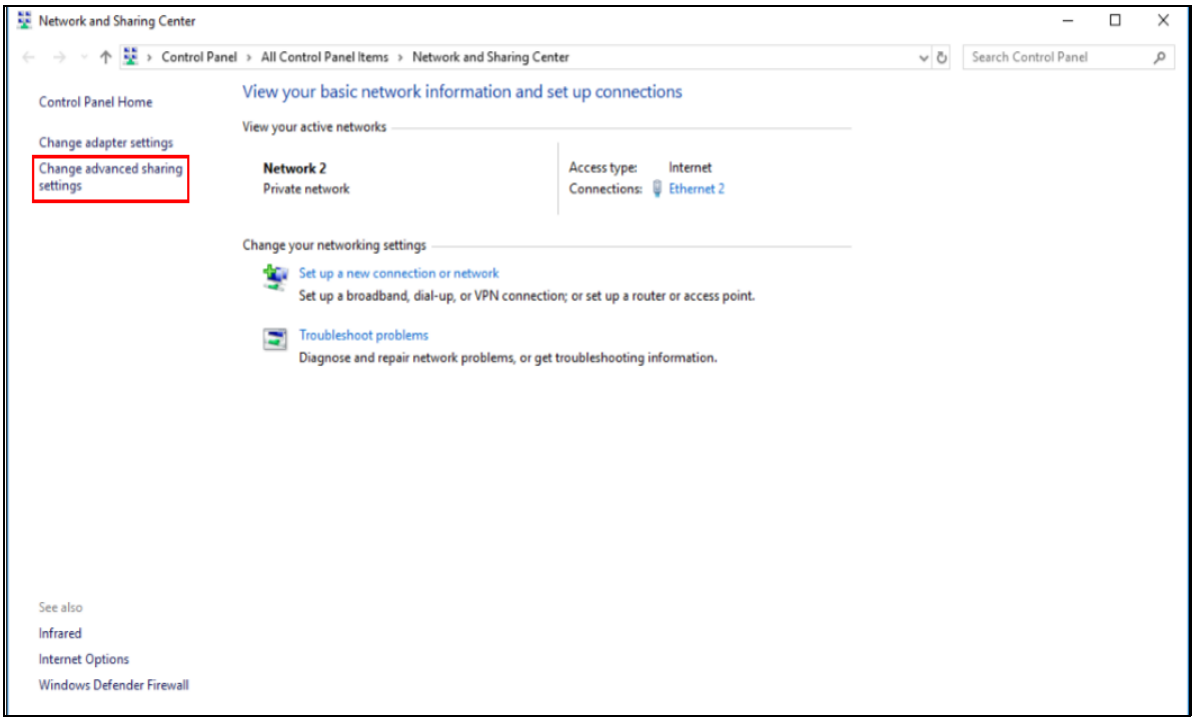
1 Click the start icon, **Settings** and then **Network & Internet**.



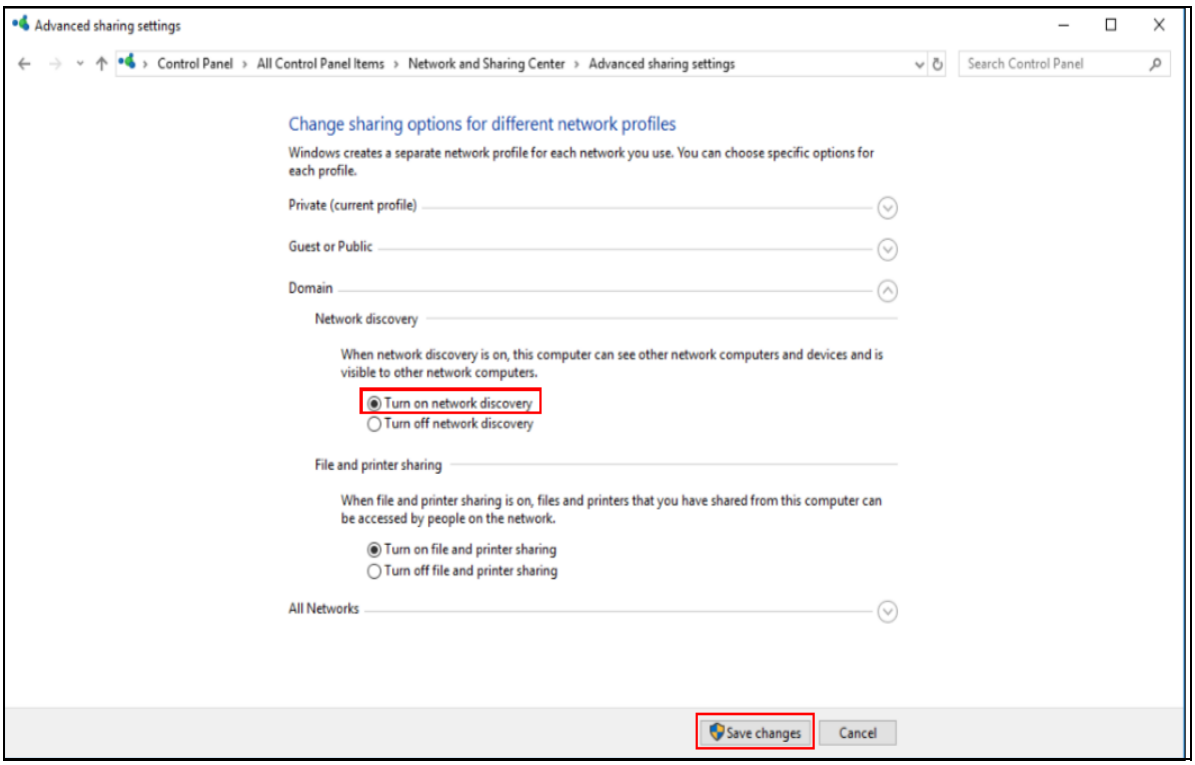
2 Click **Network and Sharing Center**.



3 Click **Change advanced sharing settings**.



4 Under **Domain**, select **Turn on network discovery** and click **Save Changes**. Network discovery allows your computer to find other computers and devices on the network and other computers on the network to find your computer. This makes it easier to share files and printers



CHAPTER 11
Wireless LAN

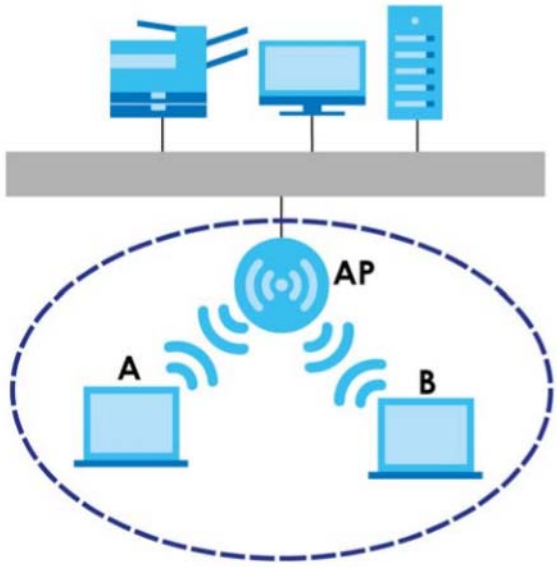
11.1 Overview

This chapter discusses how to configure the wireless network settings in your NBG6818. The NBG6818 is able to function both 2.4GHz and 5GHz network at the same time. You can have different wireless and wireless security settings for 2.4GHz and 5GHz wireless LANs. Click **Settings > WiFi** to configure **wireless LAN 2.4G** or **wireless LAN 5G**.

See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 58 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 NBG6818 is the AP.

11.1.1 What You Can Do

- Use the **Main WiFi** screen to enable or disable the 2.4GHz or 5GHz wireless LAN, set up wireless security between the NBG6818 and the wireless clients, and make other basic configuration changes (Section 11.2 on page 98).
- Use the **Guest WiFi** screen to set up multiple wireless networks on your NBG6818 (Section 11.3 on page 99).
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the NBG6818 (Section 11.4 on page 100).

- Use the **WPS** screen to quickly set up a wireless network with strong security, without having to configure security settings manually (Section 11.5 on page 102).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off (Section 11.6 on page 104).

11.1.2 What You Should Know

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Wireless Security Overview

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

SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; 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.

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.

User Authentication

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

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

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

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

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

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

Encryption

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

The types of encryption you can choose depend on the type of user authentication. (See page 96 for information about this.)

Table 37 Types of Encryption for Each Type of Authentication

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

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **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 WPA, and device B supports WPA and WPA2. Therefore, you should set up **WPA** or **WPA-PSK** 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 NBG6818, you can also select an option (**WPA/WPA-PSK Compatible**) to support WPA/WPA-PSK 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/WPA-PSK Compatible** option in the NBG6818.

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.

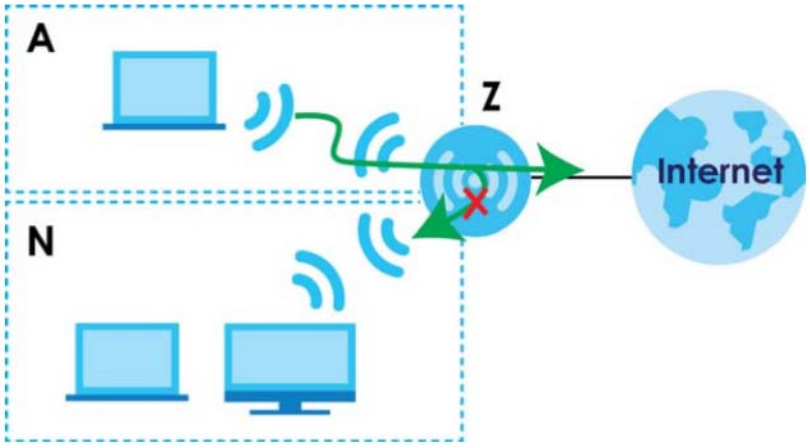
Guest WLAN

Guest WLAN allows you to set up a wireless network where users can access to Internet via the NBG6818 (**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.

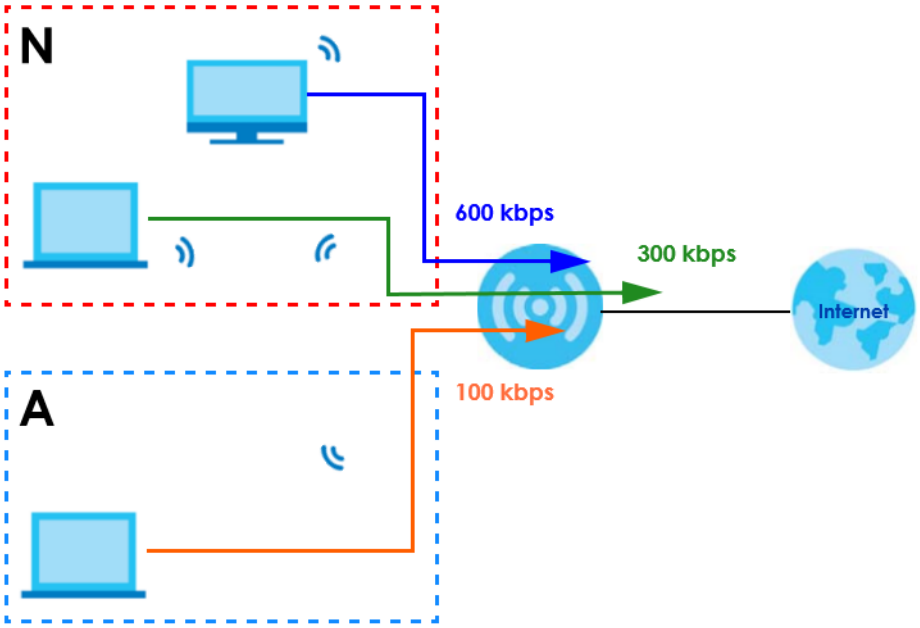
Figure 59 Guest Wireless LAN Network



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 60 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 7.2 on page 47.

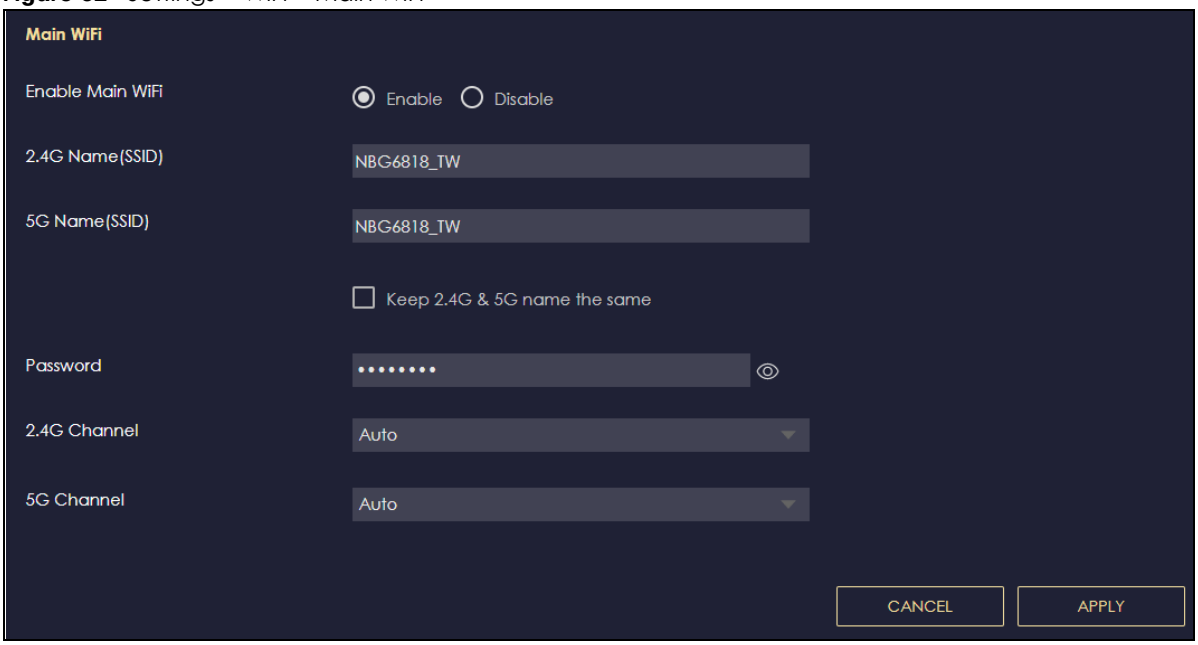
11.2 Main WiFi Screen

Use this screen to configure the SSID and wireless security of the NBG6818's default wireless LAN.

Note: If you are configuring the NBG6818 from a computer connected to the wireless LAN and you change the NBG6818'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 NBG6818's new settings.

Click **Settings** > **WiFi** > **Main WiFi** to show the following screen.

Figure 61 Settings > WiFi > Main WiFi



The following table describes the labels in this screen.

Table 38 Settings > WiFi > Main WiFi

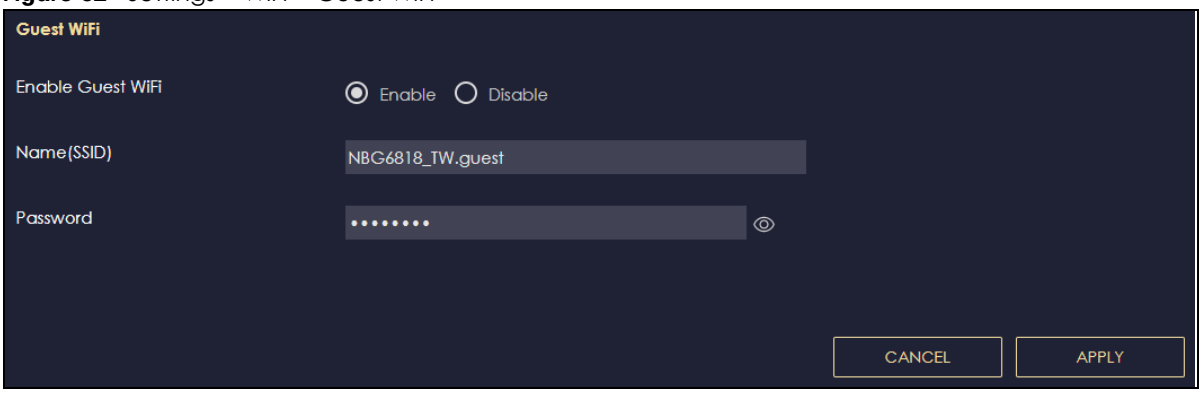
LABEL	DESCRIPTION
Main WiFi	
Enable Main WiFi	Select **Enable** to activate the 2.4GHz and/or 5GHz wireless LAN. Select **Disable** to turn it off.
2.4G/5G Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN. Click the **Keep 2.4G & 5G name the same** check box to use the same SSID for 2.4G and 5G wireless network.
Password	The password has two uses. • Manual: Manually enter the same password on the Zyxel Device and the client. Enter 8-63 ASCII characters or exactly 64 hexadecimal ('0-9', 'a-f') characters. • WPS: When using WPS, the Zyxel Device sends this password to the client. Click the **Eye** icon to show or hide the password of your wireless network. When the **Eye** icon is slashed, you'll see the password in plain text. Otherwise, it is hidden.
2.4G/5G Channel	Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

11.3 Guest WiFi Screen

This screen allows you to enable and configure guest wireless network settings on the NBG6818.

Click **Settings** > **WiFi** > **Guest WiFi** to show the following screen.

Figure 62 Settings > WiFi > Guest WiFi



The following table describes the labels in this screen.

Table 39 Settings > WiFi > Guest WiFi

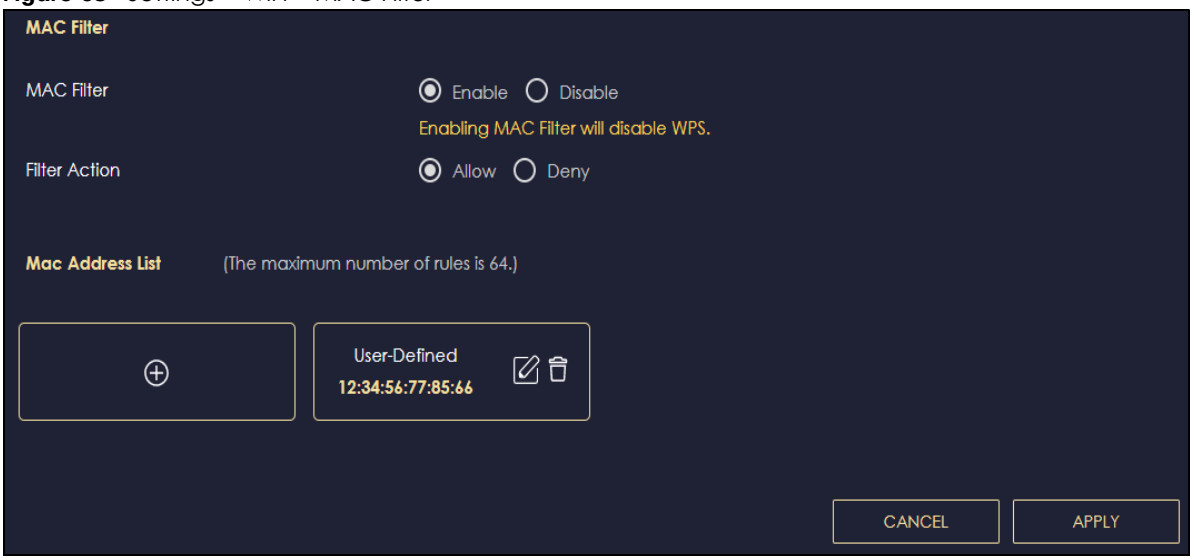
LABEL	DESCRIPTION
Enable Guest WiFi	Select **Enable** to activate the guest WiFi. Select **Disable** to turn it off.
Name (SSID)	An SSID profile is the set of parameters relating to one of the NBG6818's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is 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.
Password	The password has two uses. • Manual: Manually enter the same password on the Zyxel Device and the client. Enter 8-63 ASCII characters or exactly 64 hexadecimal ('0-9', 'a-f') characters. • WPS: When using WPS, the Zyxel Device sends this password to the client. Click the **Eye** icon to show or hide the password of your wireless network. When the **Eye** icon is slashed, you'll see the password in plain text. Otherwise, it is hidden.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

11.4 MAC Filter Screen

The MAC filter screen allows you to configure the NBG6818 to give exclusive access to devices (**Allow**) or exclude devices from accessing the NBG6818 (**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.

Use this screen to change your NBG6818's MAC filter settings. Click **Settings** > **WiFi** > **MAC Filter** to show following screen.

Figure 63 Settings > WiFi > MAC Filter



The following table describes the labels in this screen.

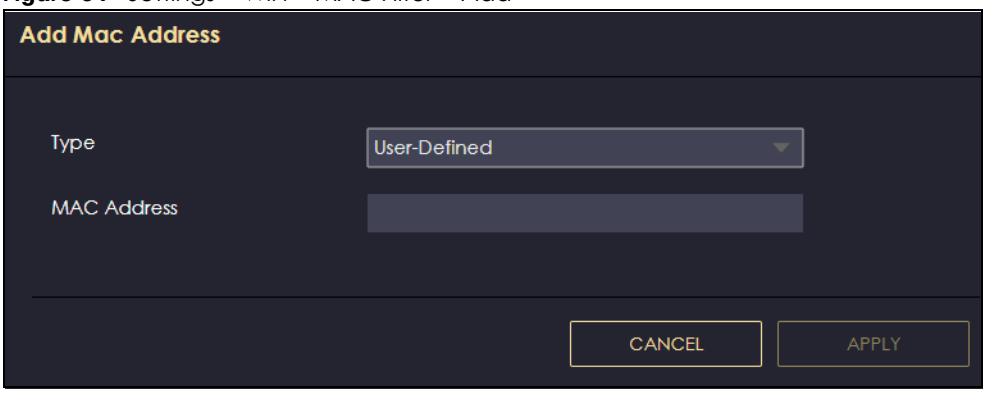
Table 40 Settings > WiFi > MAC Filter

LABEL	DESCRIPTION
MAC Filter	Select to turn on (**Enable**) or off (**Disable**) MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Filter Summary** table. Select **Allow** to permit access to the NBG6818, MAC addresses not listed will be denied access to the NBG6818. Select **Deny** to block access to the NBG6818, MAC addresses not listed will be allowed to access the NBG6818.
MAC Address List (Max Limit : 64)	
MAC Address	This field displays the MAC address of the wireless station. Click to configure the MAC address. Click to delete the MAC address.
Add	Click to add a rule in the MAC filter summary table.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

11.4.1 Add MAC Address Screen

Use this screen to configure the MAC address you want to add to the MAC address list. Click **Settings** > **WiFi** > **MAC Filter** > **Add** to show the following screen.

Figure 64 Settings > WiFi > MAC Filter > Add



The following table describes the labels in this screen.

Table 41 Settings > WiFi > MAC Filter > Add

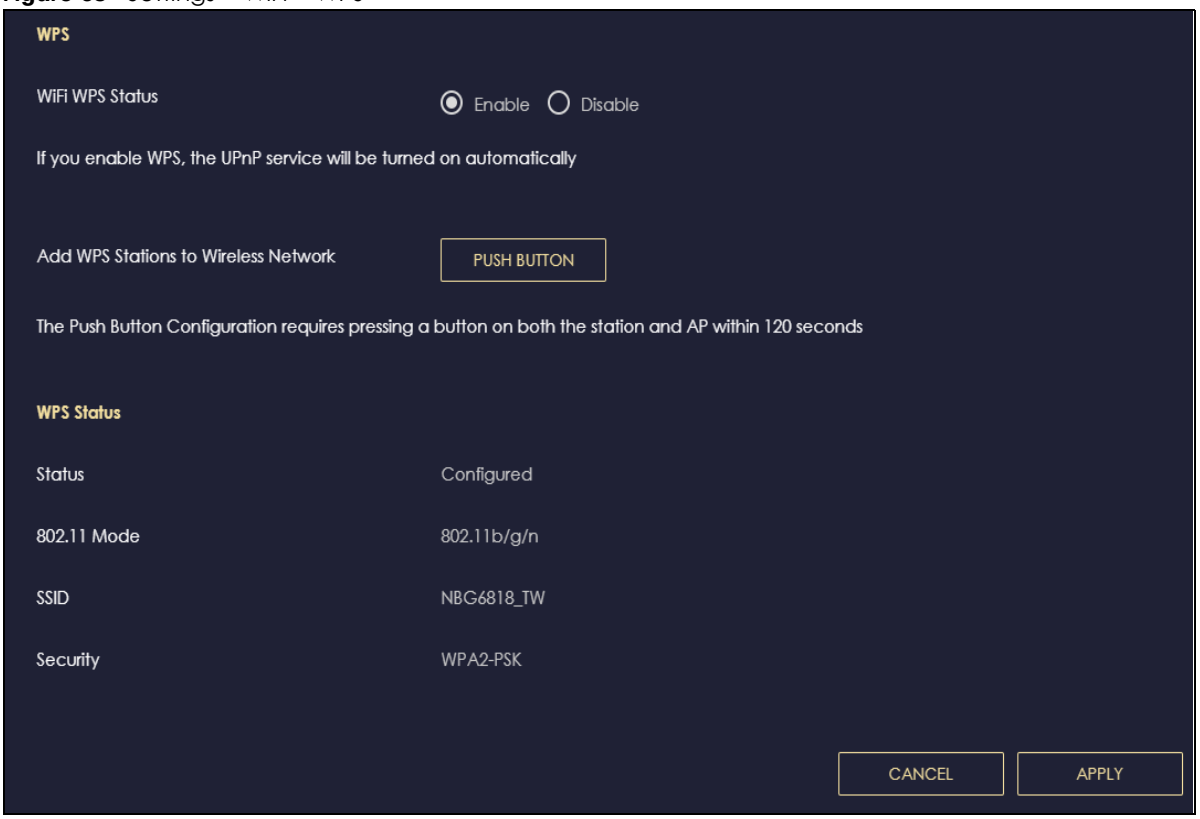
LABEL	DESCRIPTION
Type	This field displays the MAC address of the wireless station. If you select **User-Defined**, enter the MAC address(es) manually.
MAC Address	Enter a MAC address manually in this field if you select **User-Defined** in the **Type** field.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to exist this screen without saving.

11.5 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. Click **Settings** > **WiFi** > **WPS** to show the following screen.

Note: With WPS, wireless clients can only connect to the wireless network using the first SSID on the NBG6818.

Figure 65 Settings > WiFi > WPS



The following table describes the labels in this screen.

Table 42 Settings > WiFi > WPS

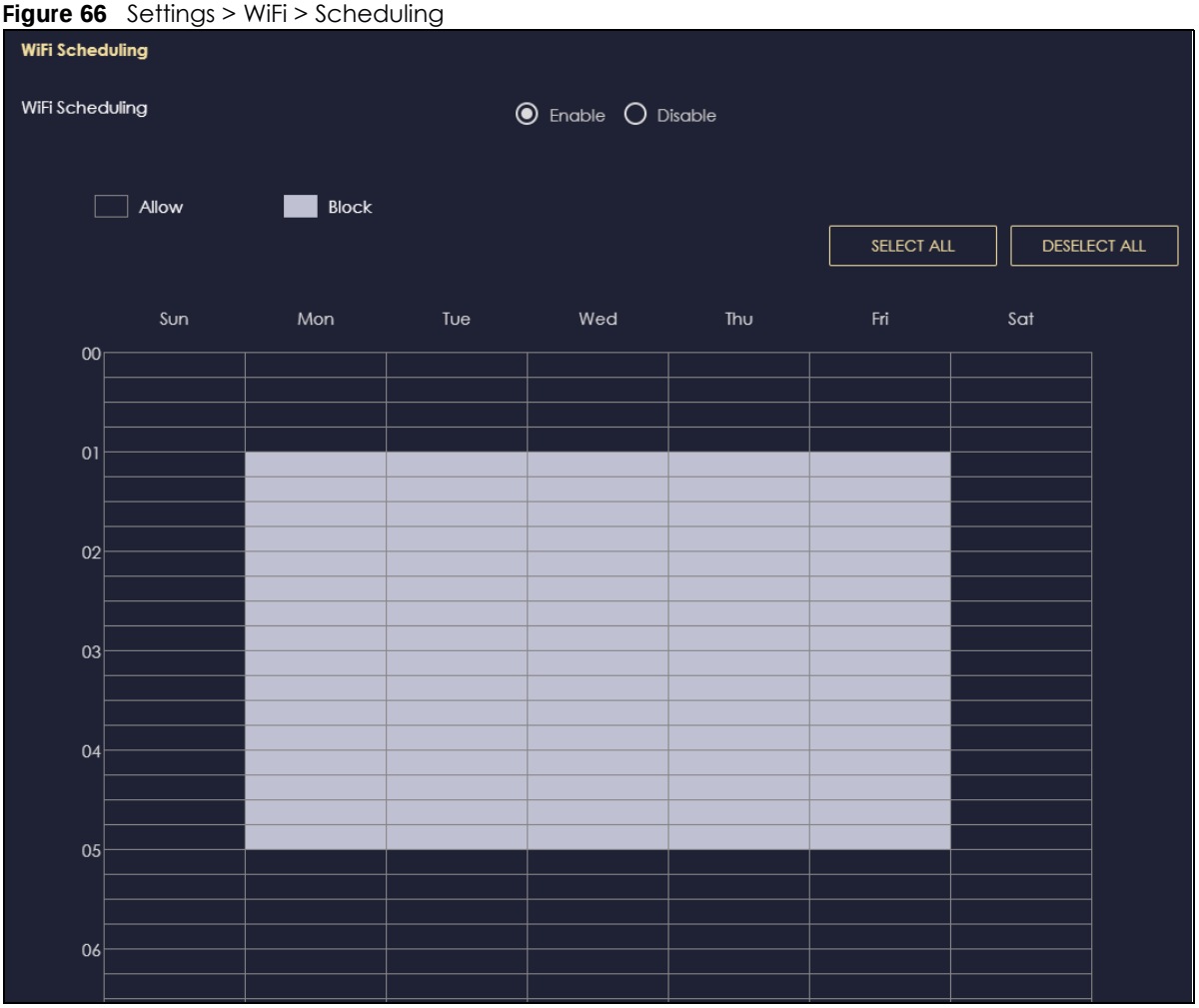
LABEL	DESCRIPTION
WPS	
WiFi WPS Status	Select **Enable** to turn on the WPS feature. Otherwise, select **Disable**.
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.
WPS Status	
Status	This displays **Configured** when the NBG6818 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 NBG6818 or you click **Release Configuration** to remove the configured wireless and wireless security settings.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the NBG6818.
SSID	This is the name of the wireless network (the NBG6818's first SSID).
Security	This is the type of wireless security employed by the network.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

11.6 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. The y-axis shows the time period in days. The x-axis shows the time period in hours.

Click **Settings > WiFi > Scheduling** to show the following screen.

Figure 66 Settings > WiFi > Scheduling



The following table describes the labels in this screen.

Table 43 Expert Mode > Wireless > Scheduling

LABEL	DESCRIPTION
WiFi Scheduling	Select **Enable** to activate the wireless LAN scheduling feature. Select **Disable** to turn it off.
Select All	Click **Select All** or click gray blocks to specify days and times to turn the Wireless LAN on or off. If you click **Select All** you can not select any specific days and times.
Deselect All	Click **Deselect All** to remove all the wireless LAN scheduling.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

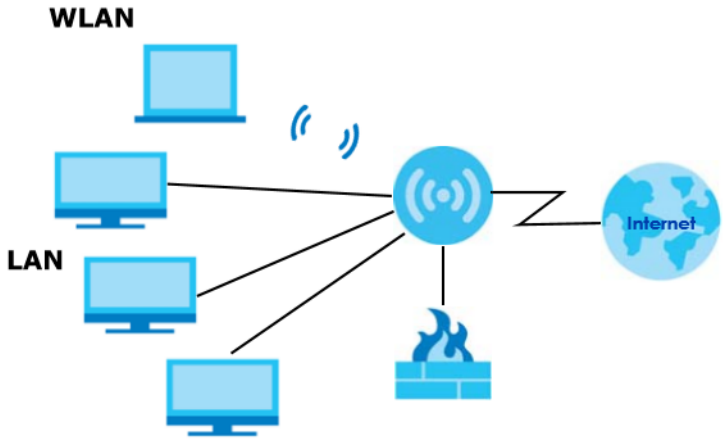
CHAPTER 12
LAN

12.1 Overview

This chapter describes how to configure LAN settings.

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building.

Figure 67 LAN Example



The LAN screens can help you configure a manage IP address, and partition your physical network into logical networks.

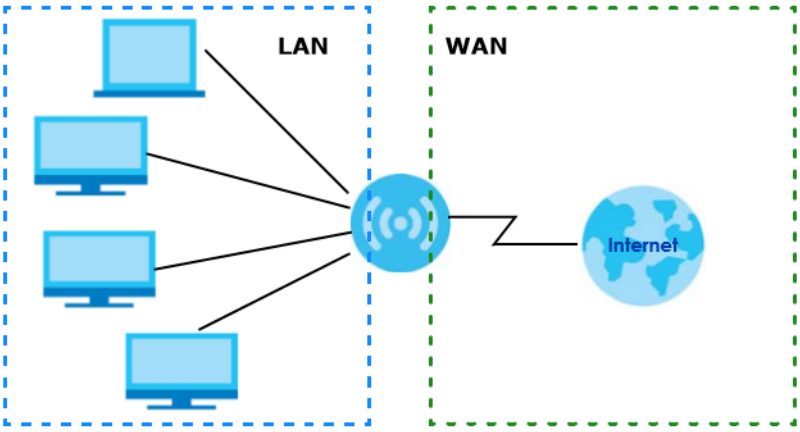
12.2 What You Can Do

- Use the **LAN IP** screen to configure the IP addresses for your NBG6818 on the LAN (Section 12.4 on page 106).
- Use the **IPv6 LAN** screen to configure the IPv6 address for your NBG6818 on the LAN (Section 12.5 on page 110).

12.3 What You Need To Know

The actual physical connection determines whether the NBG6818 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 68 LAN and WAN IP Addresses



The LAN parameters of the NBG6818 are preset in the factory with the following values:

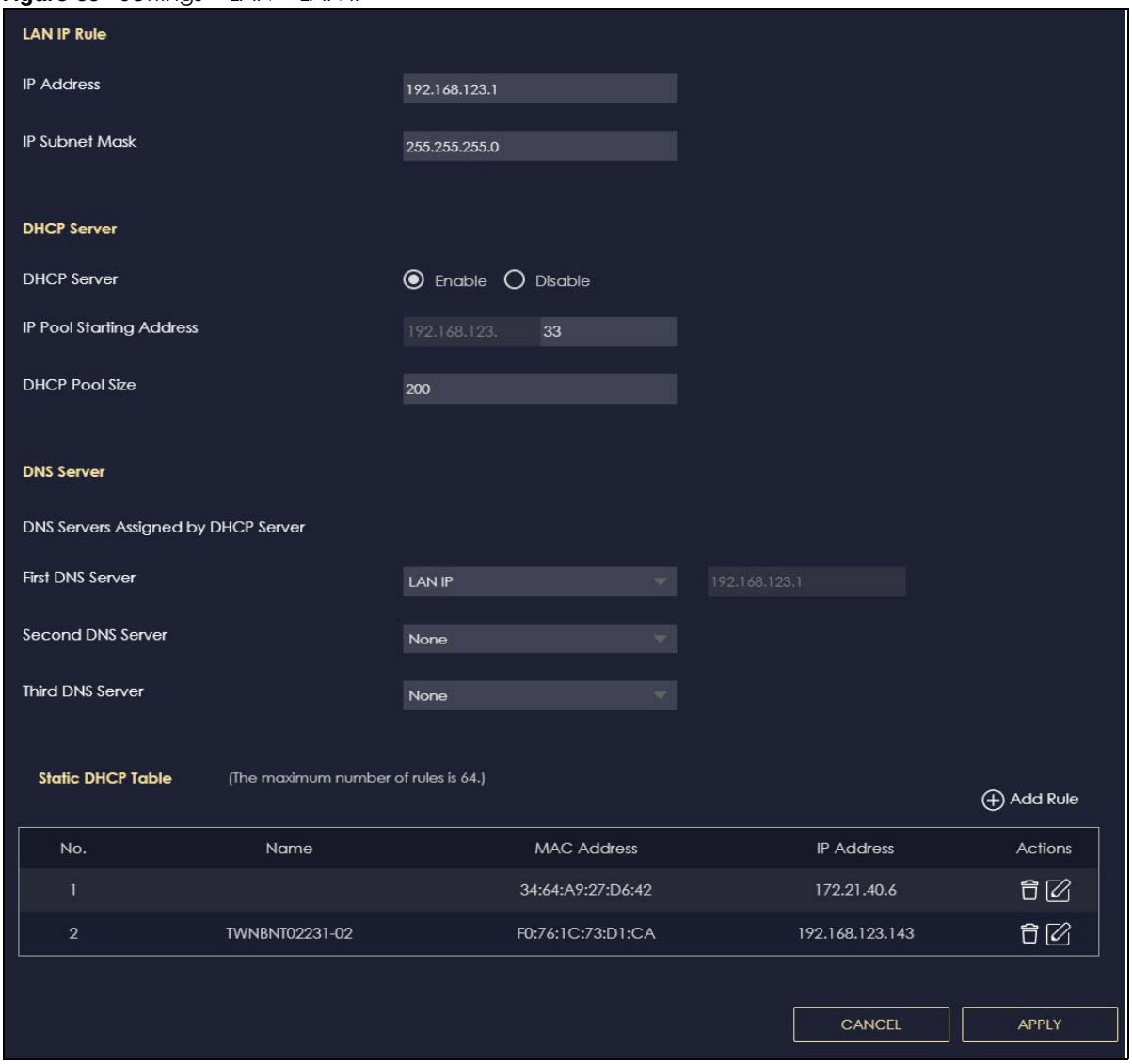
- IPv4 address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 128 client IPv4 addresses starting from 192.168.1.33.

These parameters should work for the majority of installations.

12.4 LAN IP Screen

Use this screen to change the IP address for your NBG6818. Click **Settings > LAN > LAN IP** to show the following screen.

Figure 69 Settings > LAN > LAN IP



The following table describes the labels in this screen.

Table 44 Settings > LAN > LAN IP

LABEL	DESCRIPTION
LAN IP Rule	
IP Address	Type the IP address of your NBG6818 in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG6818 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 NBG6818.
DHCP Server	

Table 44 Settings > LAN > LAN IP (continued)

LABEL	DESCRIPTION
DHCP Server	Select **Enable** to activate DHCP for LAN. Select **Disable** to stop the NBG6818 acting as a DHCP server. 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. When configured as a server, the NBG6818 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.
DHCP Pool Size	This field specifies the size, or count of the IP address pool for LAN.
DNS Server DNS Servers Assigned by DHCP Server	
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the NBG6818'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. Select **LAN IP** and the field to the right displays the (read-only) the default gateway IP address of your computer. 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.
Static DHCP Table	
No.	This is the index number of the static IP table entry (row).
Name	This field displays a name to identify this rule.
MAC Address	This field displays the MAC address of a computer on your LAN, or the MAC address you manually configured.
IP Address	This field displays the LAN IP address of a computer on your LAN, or the LAN address you manually configured.
Actions	Click the icons under **Actions** to delete or edit an existing static IP. Click  to delete an existing static IP. Click  to edit an existing static IP.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to begin configuring this screen afresh.

12.4.1 Static DHCP Table-Add/Edit Rule Screen

Use this screen to configure the static DHCP. Click **Settings** > **LAN** > **LAN IP** > **Add Rule** or **Settings** > **LAN** > > **LAN IP** > **Edit** to show the following screens.

Figure 70 Settings > LAN > LAN IP > Add Rule

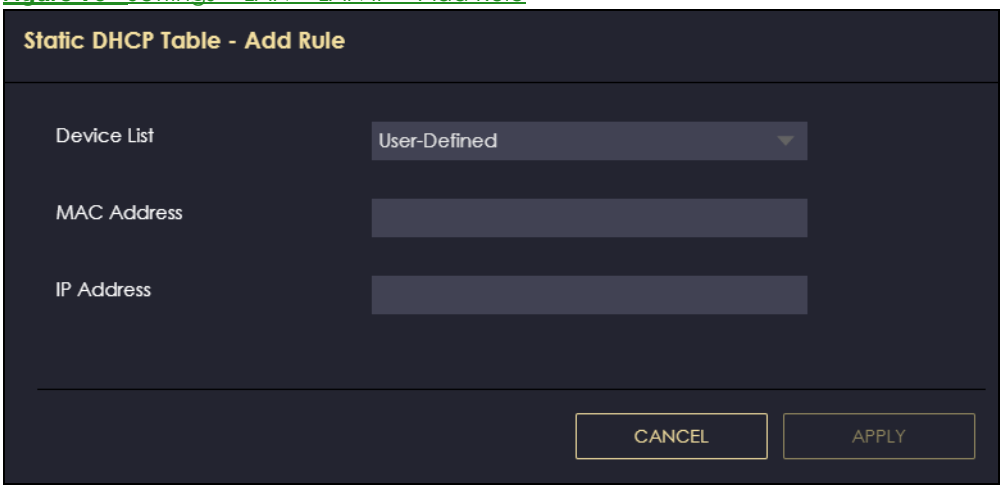
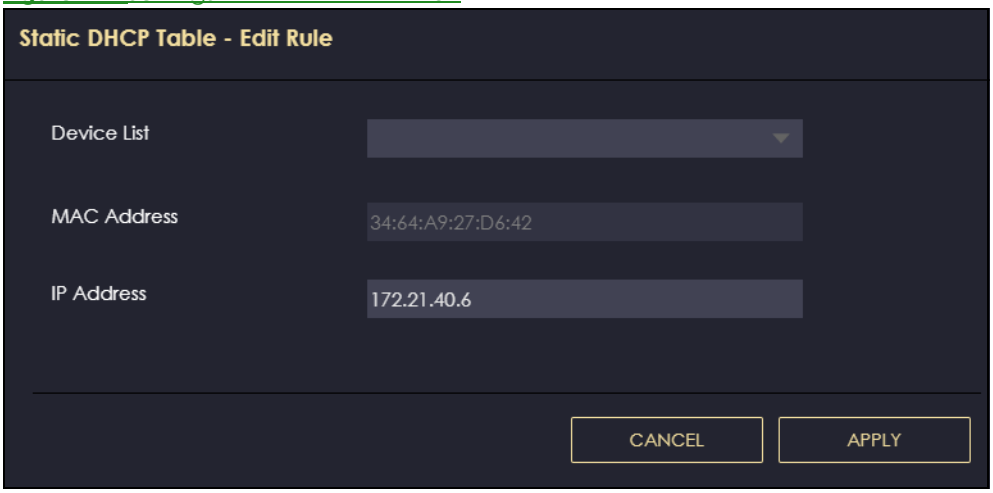


Figure 71 Settings > LAN > LAN IP > Edit



The following table describes the labels in these screens.

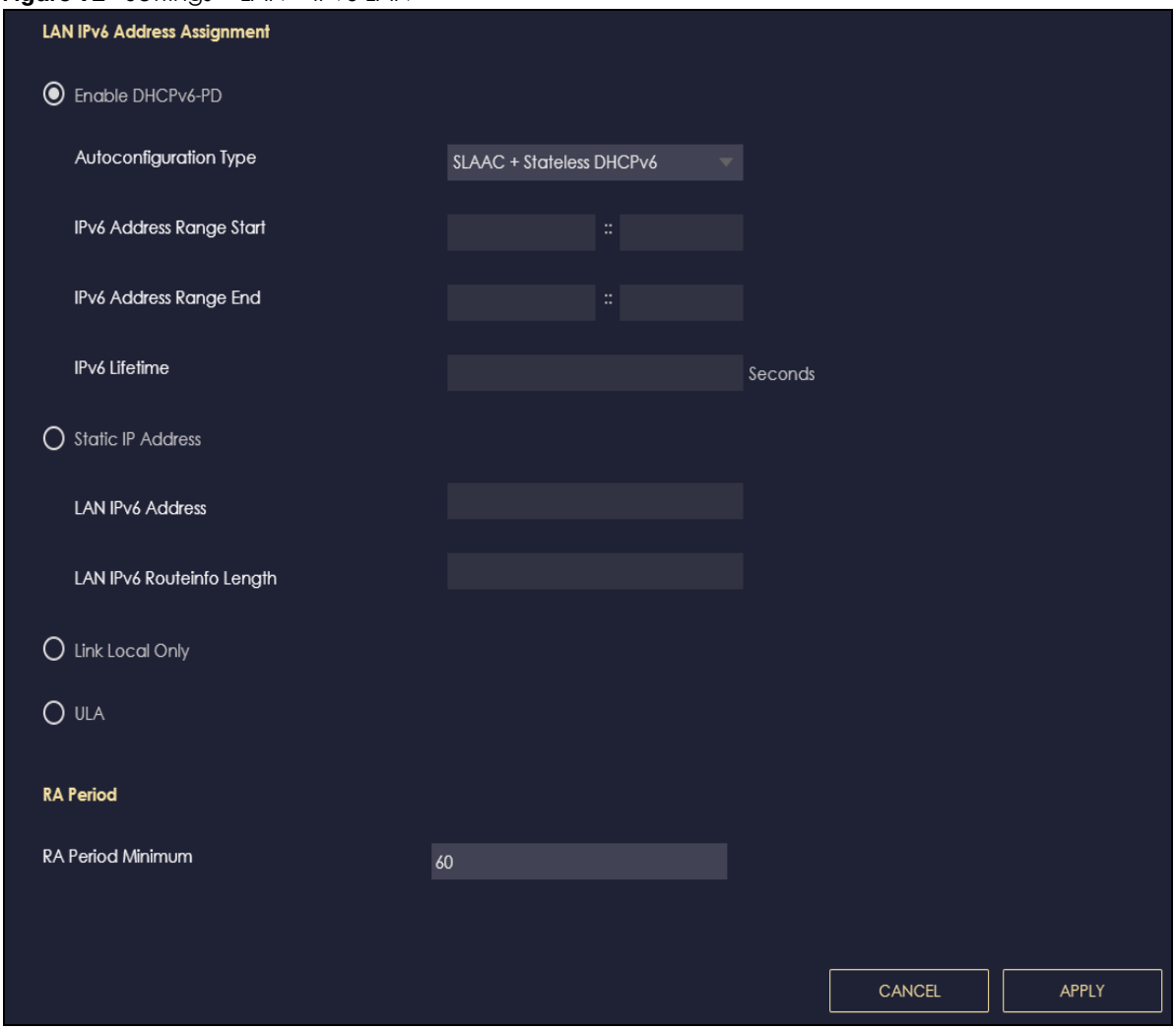
Table 45 Settings > LAN > LAN IP > Add Rule/Edit

LABEL	DESCRIPTION
Device LIst	This field lists the system name of the LAN user device which is connected to the NBG6818 and assigned an IP address. Select a LAN user device from the list to automatically detect the MAC address of a computer on your LAN. Otherwise, select **User-Defined** to enter the MAC address of a computer on your LAN in the **MAC Address** field.
MAC Address	This field displays the MAC address of a computer on your LAN. If you select **User-Defined** in the **Device List** field, enter the MAC address(es) manually.
IP Address	This field displays the IP address of a computer on your LAN. If you select **User-Defined** in the **Device List** field, enter the IP address(es) manually.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to exist this screen without saving.

12.5 IPv6 LAN Screen

Use this screen to configure the IP address for your NBG6818 on the LAN. Click **Settings** > **LAN** > **IPv6 LAN** to show the following screen.

Figure 72 Settings > LAN > IPv6 LAN



The following table describes the labels in this screen.

Table 46 Settings > Expert Mode > LAN > IPv6 LAN

LABEL	DESCRIPTION
LAN IPv6 Address Assignment	
Enable_DHCPv6-PD Select this option to use DHCPv6 prefix delegation. The NBG6818 will obtain an IPv6 prefix from the ISP or a connected uplink router for the LAN.	

Table 46 Settings > Expert Mode > LAN > IPv6 LAN (continued)

LABEL	DESCRIPTION
Autoconfiguration Type	Select **SLAAC + RDNSS** to enable IPv6 stateless auto-configuration on this interface. The interface will generate an IPv6 IP address itself from a prefix obtained from an IPv6 router in the network. Select **SLAAC + Stateless DHCPv6** to enable IPv6 stateless auto-configuration on this interface. The interface will get an IPv6 address from an IPv6 router and the DHCP server. The IP address information gets through DHCPv6. Select **Stateful DHCPv6** to allow a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients.
IPv6 Address range (Start)	Enter the beginning of the range of IP addresses that this address object represents.
IPv6 Address range (End)	Enter the end of the range of IP address that this address object represents.
IPv6 Lifetime	Enter the IPv6 lifetime in the LAN.
Static IP Address Select this option to manually enter an IPv6 address if you want to use a static IP address.	
LAN IPv6 Address	Enter the LAN IPv6 address you want to assign to your NBG6818 in hexadecimal notation.
LAN IPv6 Routeinfo Length (48~64)	Enter the 48 to 64 address prefix length to specify in an IPv6 address compose the network address.
Prefix Valid Lifetime	Enter the valid lifetime for the prefix.
Link Local Only Select this option to only use the link local address on the NBG6818 interfaces in the LAN.	
ULA Select this option to identify a unique local address of the NBG6818 in the LAN.	
RA period	
Minimum RA period	Enter the minimum time in seconds between router advertisement messages.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 13
Security

13.1 Overview

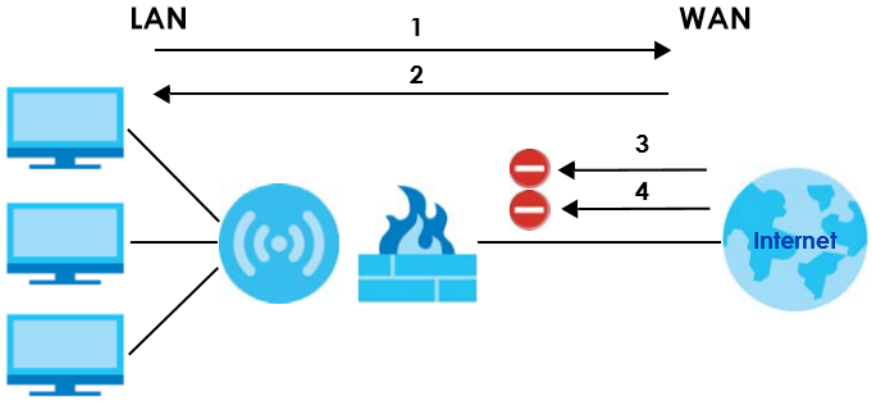
Use these screens to enable and configure the firewall that protects your NBG6818 and your LAN from unwanted or malicious traffic.

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 73 Default Firewall Action



13.1.1 What You Can Do

- Use the **IPv4 Firewall** screen to enable or disable the NBG6818's IPv4 firewall (Section 13.2 on page 113).
- Use the **IPv6 Firewall** screen to enable or disable the NBG6818's IPv6 firewall (Section 13.3 on page 116).

13.1.2 What You Need To Know

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

About the NBG6818 Firewall

The NBG6818'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 **IPv4 Firewall** or **IPv6 Firewall** tab under **Security** and then click the **Enable Firewall** check box). The NBG6818's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG6818 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 NBG6818 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 NBG6818 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.

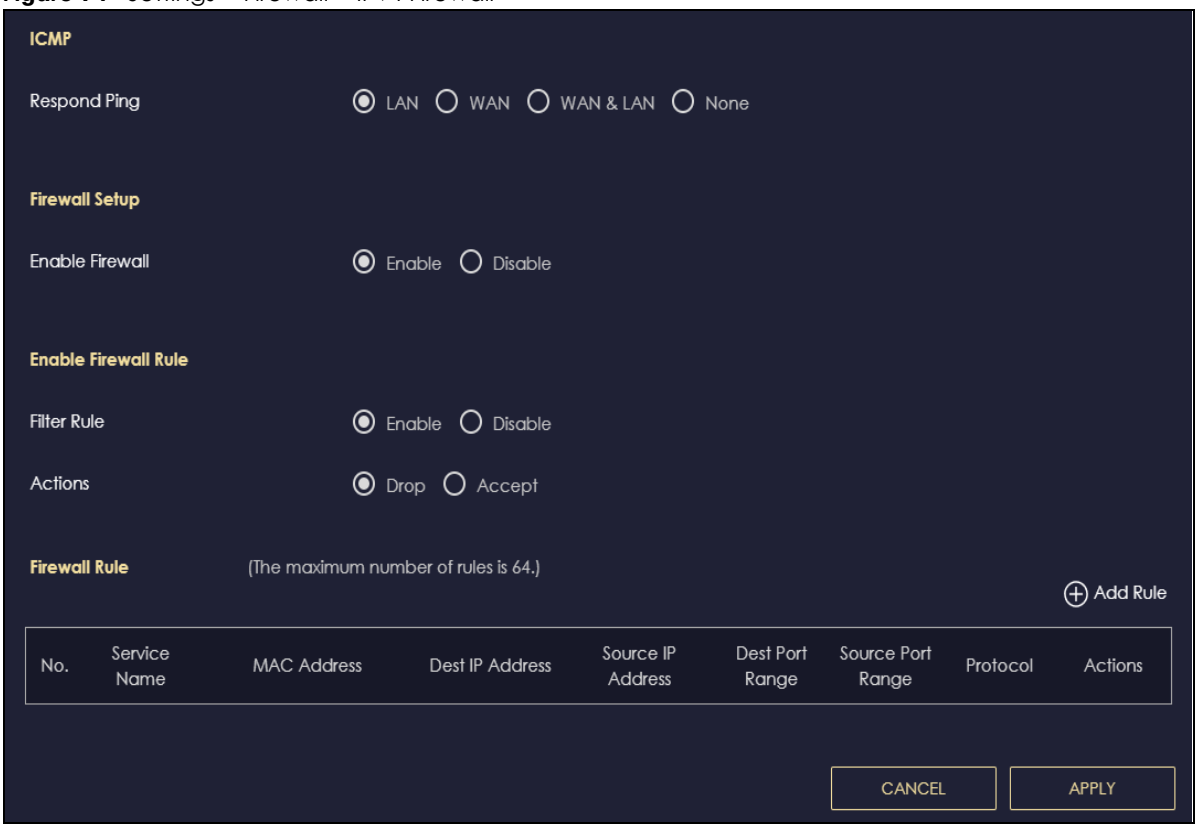
Guidelines For Enhancing Security With Your Firewall

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.

13.2 IPv4 Firewall Screen

Use this screen to enable or disable the NBG6818's IPv4 firewall. Click **Settings** > **Firewall** > **IPv4 Firewall** to show the following screen.

Figure 74 Settings > Firewall > IPv4 Firewall



The following table describes the labels in this screen.

Table 47 Settings > Firewall > IPv4 Firewall

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 NBG6818 will not respond to any incoming Ping requests when **None** 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.
Firewall Setup	
Enable Firewall	Select **Enable** to activate the firewall. The NBG6818 performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Enable Firewall Rule	
Filter Rule	Select **Enable** to activate the firewall rules that you define (see Add Firewall Rule below).
Actions	Select **Drop** to silently discard the packets which meet the firewall rules. The others are accepted. Select **Accept** to allow the passage of the packets which meet the firewall rules. The others are blocked.
Firewall Rule	
No.	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.

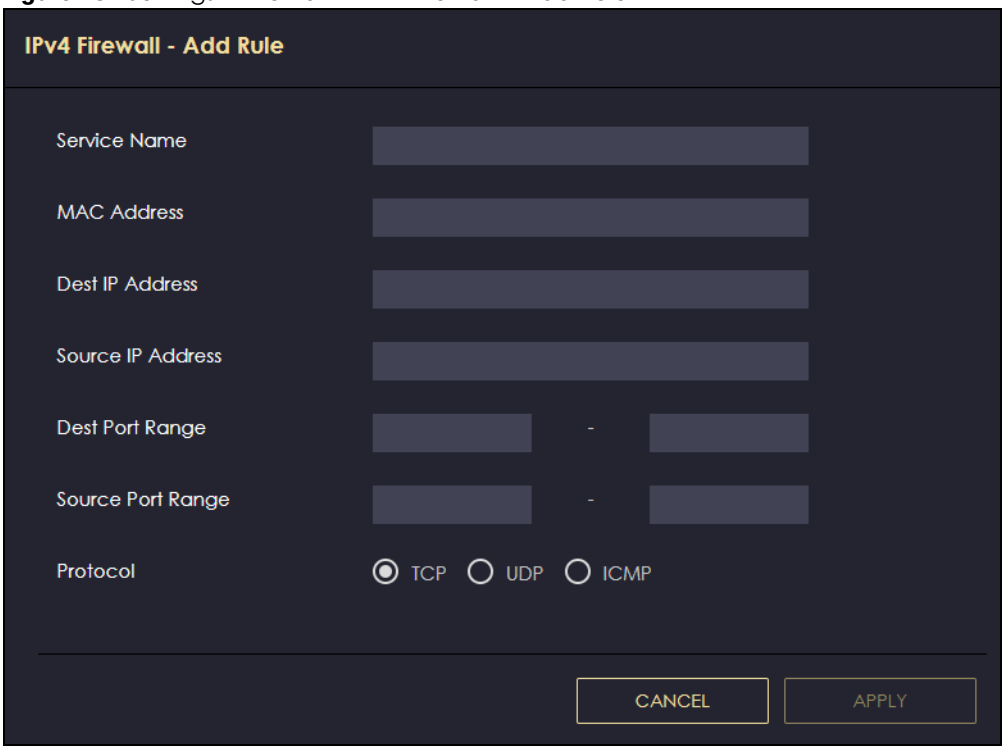
Table 47 Settings > Firewall > IPv4 Firewall (continued)

LABEL	DESCRIPTION
Dest IP Address	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP Address	This is the IP address of the computer from which traffic for the application or service is initialized.
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.
Protocol	This is the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
Actions	Click to remove the firewall rule. Click to edit the firewall rule.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to start configuring this screen again.

13.2.1 IPv4 Firewall-Add Rule Screen

Use this screen to configure IPv4 firewall rule. Click **Settings** > **Firewall** > **IPv4 Firewall** > **Add Rule** to open the following screen.

Figure 75 Settings > Firewall > IPv4 Firewall > Add Rule



The following table describes the labels in this screen.

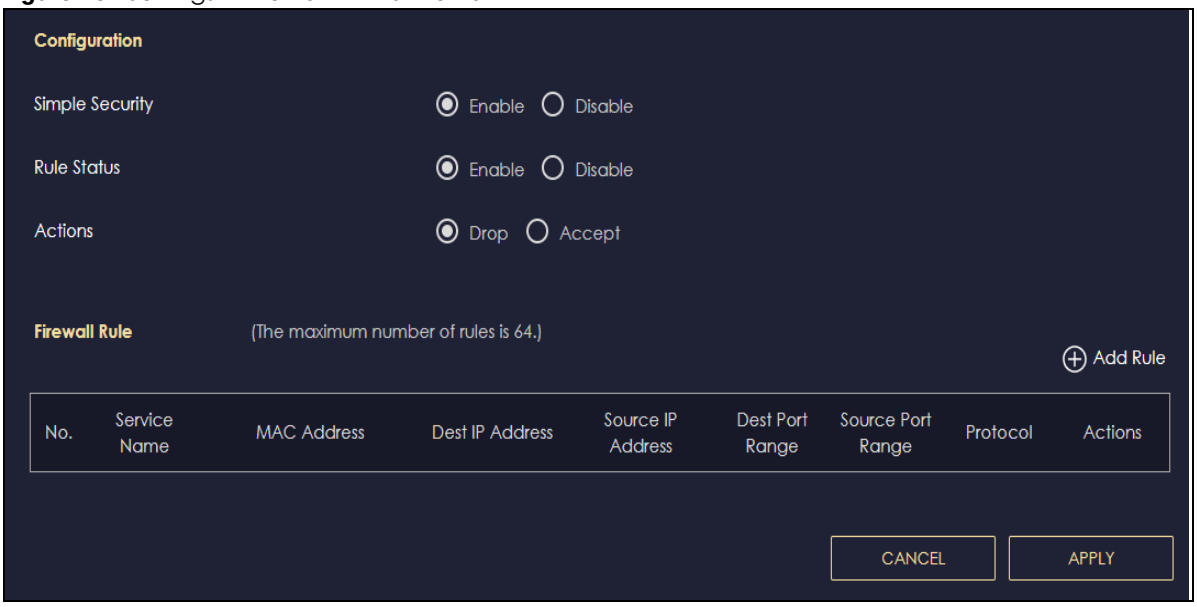
Table 48 Settings > Firewall > IPv4 Firewall > Add Rule

LABEL	DESCRIPTION
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 NBG6818 applies the firewall rule to traffic initiating from this computer.
Source IP Address	Enter the IP address of the computer that initializes traffic for the application or service. The NBG6818 applies the firewall rule to traffic initiating from this computer.
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.
Protocol	Select the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to exist this screen without saving.

13.3 IPv6 Firewall Screen

Use this screen to enable and create IPv6 firewall rules to filter IPv6 traffic. Click **Settings** > **Firewall** > **IPv6 Firewall** to show the following screen.

Figure 76 Settings > Firewall > IPv6 Firewall



The following table describes the labels in this screen.

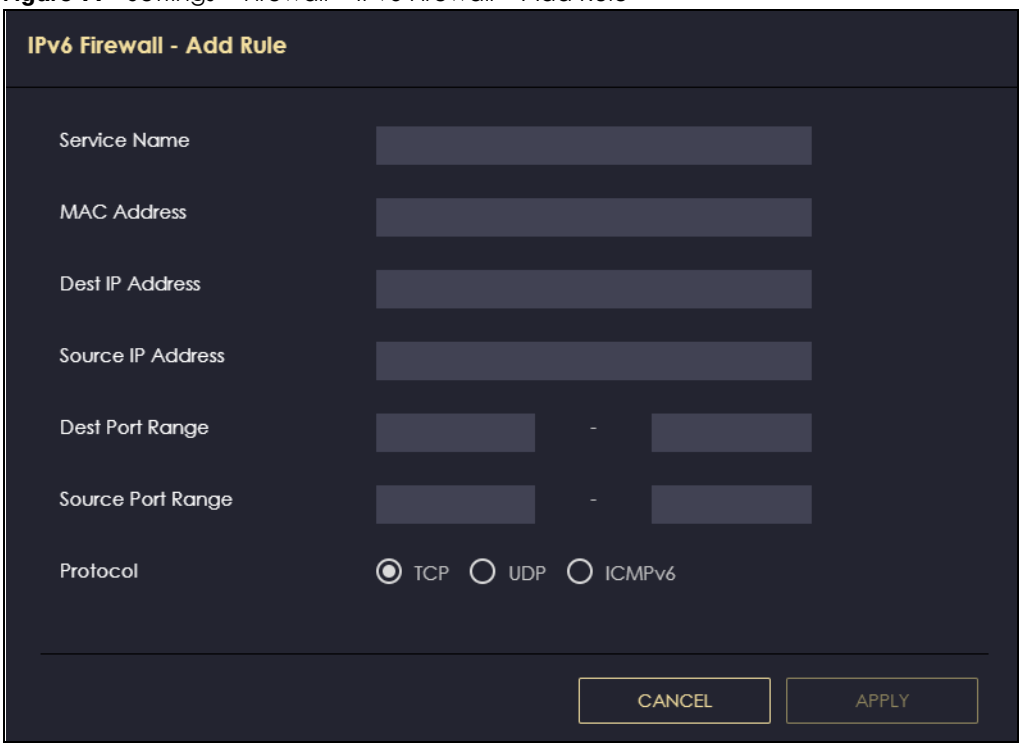
Table 49 Settings > Firewall > IPv6 Firewall

LABEL	DESCRIPTION
Configuration	
Simple Security	
Rule Status	
Action	Select **DROP** to silently discard the packets which meet the firewall rules. The others are accepted. Select **ACCEPT** to allow the passage of the packets which meet the firewall rules. The others are blocked.
Firewall Rule	
No.	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Service Name	This is a name that identifies or describes the firewall rule.
MAC Address	This is the MAC address of the computer for which the firewall rule applies.
Dest IP Address	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP Address	This is the IP address of the computer to which traffic for the application or service is initialized.
Dest Port Range	This is the port number/range of the destination that defines the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	This is the port number/range of the source that defines the traffic type, for example TCP port 80 defines web traffic.
Protocol	This is the protocol (**TCP**, **UDP** or **ICMPv6**) used to transport the packets for which you want to apply the firewall rule.
Actions	Click  to remove the firewall rule. Click  to edit the firewall rule.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to restore your previously saved settings.

13.3.1 IPv6 Firewall-Add Rule Screen

Use this screen to configure IPv4 firewall rule. Click **Settings** > **Firewall** > **IPv6 Firewall** > **Add Rule** to open the following screen.

Figure 77 Settings > Firewall > IPv6 Firewall > Add Rule



The following table describes the labels in this screen.

Table 50 Settings > Firewall > IPv4 Firewall > Add Rule

LABEL	DESCRIPTION
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 NBG6818 applies the firewall rule to traffic initiating from this computer.
Source IP Address	Enter the IP address of the computer that initializes traffic for the application or service. The NBG6818 applies the firewall rule to traffic initiating from this computer.
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.
Protocol	Select the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to exist this screen without saving.

CHAPTER 14
System

14.1 Overview

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

14.2 What You Can Do

- Use the **Status** screen to view the basic information of the NBG6818 (Section 14.3 on page 119)
- Use the **General Setting** screen to set the timeout period of the management session (Section 14.4 on page 121).
- Use the **Remote Access** screen to configure the interface/s from which the NBG6818 can be managed remotely and specify a secure client that can manage the NBG6818 (Section 14.5 on page 122).
- Use the **Maintenance** screen to upload firmware, reboot the NBG6818 without turning the power off or reset the NBG6816 to factory default (Section 14.6 on page 124).
- Use the **Operating Mode** screen select how you want to use your NBG6818 (Section 14.7 on page 125).
- Use the **Logs** screen to see the logs for the activity on the NNG6816 (Section 14.8 on page 126).

14.3 Status Screen

Use this screen to view some basic information of your NBG6816. Click **Settings** > **System** > **Status** to show the following screen.

Figure 78 Settings > System > Status

The following table describes the labels in this screen.

Table 51 Settings > System > Status

LABEL	DESCRIPTION
System	
Model Name	This is the model name of your device.
Firmware Version	This is the firmware version.
System Operation Mode	This is the device mode to which the NBG6818 is set - Router Mode, see Section 14.7 on page 125 for more information.
Enable IPv4 Firewall	This shows if the IPv4 firewall is enable on the NBG6818.
Enable IPv6 Simple Security	This shows if the IPv6 firewall is enable on the NB6818.
System Uptime	This is the total time the NBG6818 has been on.
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.

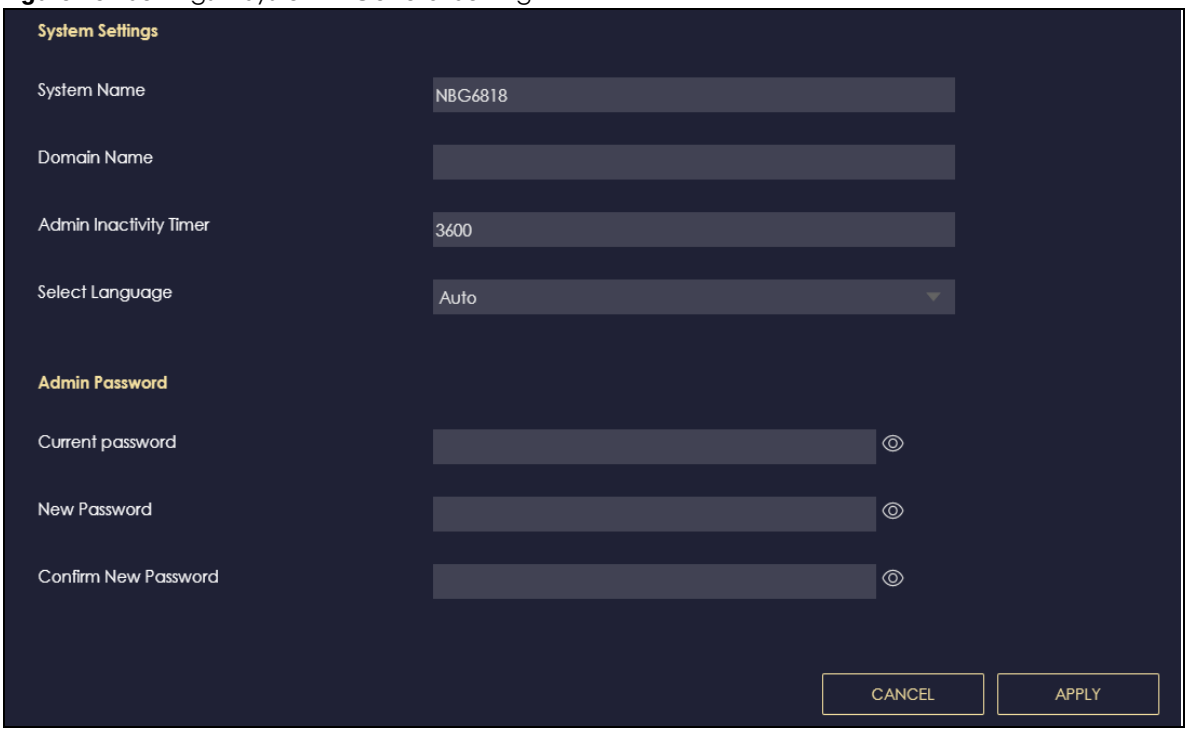
Table 51 Settings > System > Status (continued)

LABEL	DESCRIPTION
Gateway	This shows the WAN port's gateway IP address.
IPv6 Address	This shows the current IPv6 address of the NBG6818.
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 Server	This shows the LAN port's DHCP role - **Enable** or **Disable**.
IPv6 Address	This shows the current IPv6 address of the NBG6818 in the LAN.

14.4 General Setting Screen

Use this screen to set the management session timeout period. Click **Settings** > **System** > **General Setting** to show the following screen.

Figure 79 Settings > System > General Setting



The following table describes the labels in this screen.

Table 52 Settings > System > General Setting

LABEL	DESCRIPTION
System Settings	
System Name	System Name is a unique name to identify the NBG6818 in an Ethernet network.
Domain Name	Enter the domain name you want to give to the NBG6818.

Table 52 Settings > System > General Setting (continued)

LABEL	DESCRIPTION
Admin 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).
Select Language	Select a language you prefer from the drop-down list box. The Web Configurator language changes after a while without restarting the NBG6818.
Admin Password	
Current 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 a dot for each character you type.
Confirm New Password	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the NBG6818.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.5 Remote Access Screen

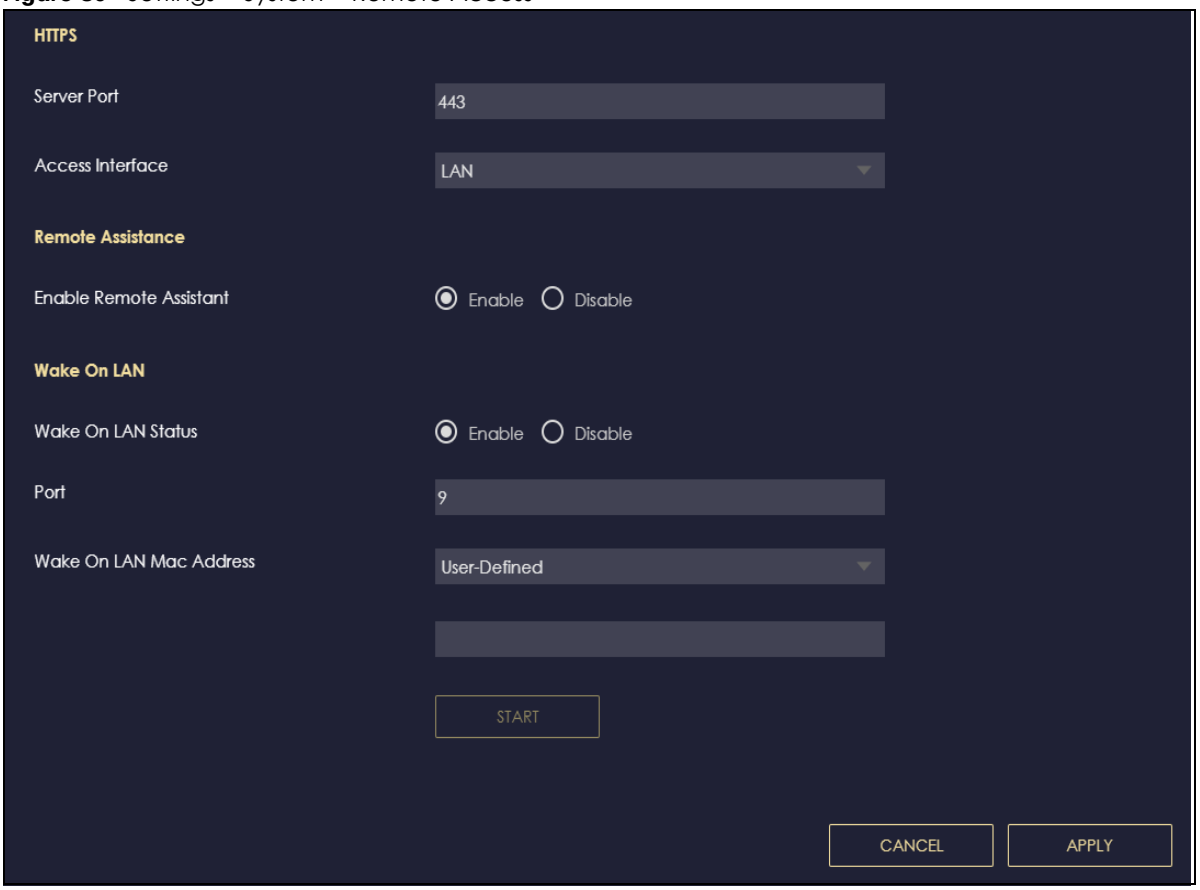
Use this screen to change your NBG6818's remote management settings. You can use HTTPS or Wake on LAN to access and manage the NBG6818.

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.

Click **Settings** > **System** > **Remote Access** to show the following screen.

Figure 80 Settings > System > Remote Access



The following table describes the labels in this screen.

Table 53 Settings > System > Remote Access

LABEL	DESCRIPTION
HTTPS	
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Interface	Select the interface(s) through which a computer may access the NBG6818 using this service.
Remote Assistance	
Enable Remote Assistant	
Wake on LAN	
Wake on LAN Status	Select **Enable** to have the NBG6818 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 MAC Address	This field displays the hostname and MAC address of the LAN device by default. Otherwise, select **User-Defined** to enter the MAC Address of the device on the network that will be turned on. A MAC address consists of six hexadecimal character pairs.

Table 53 Settings > System > Remote Access (continued)

LABEL	DESCRIPTION
Start	Click this to have the NBG6818 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 your changes back to the NBG6818.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.6 Maintenance Screen

Use this screen to upgrade firmware, restart or reset your NBG6818.

Online Firmware

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(ABCS.0)C0.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

System Restart

System restart allows you to reboot the NBG6818 without turning the power off.

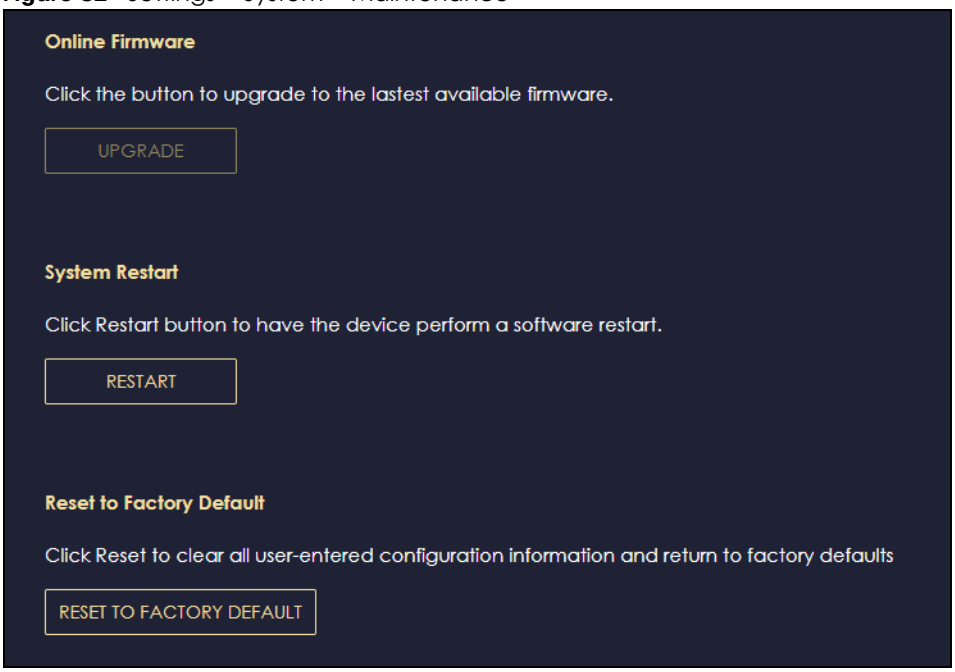
Reset to Factory Default

Click the **RESET TO FACTORY DEFAULT** button in this section to clear all user-entered configuration information and returns the NBG6818 to its factory defaults.

You can also press the **RESET** button on the rear panel to reset the factory defaults of your NBG6818.

Click **Settings** > **System** > **Maintenance** to show the following screen.

Figure 81 Settings > System > Maintenance



14.7 Operating Mode Screen

Use this screen to select how you want to use your NBG6818.

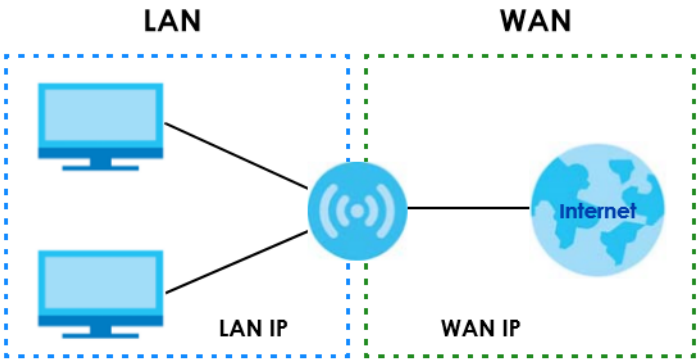
The **Operating Mode** function lets you configure your NBG6818 as a router or bridge. You can choose between **Standard (Router) Mode**, and **Bridge Mode** depending on your network topology and the features you require from your device.

The following describes the device modes available in your NBG6818.

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.

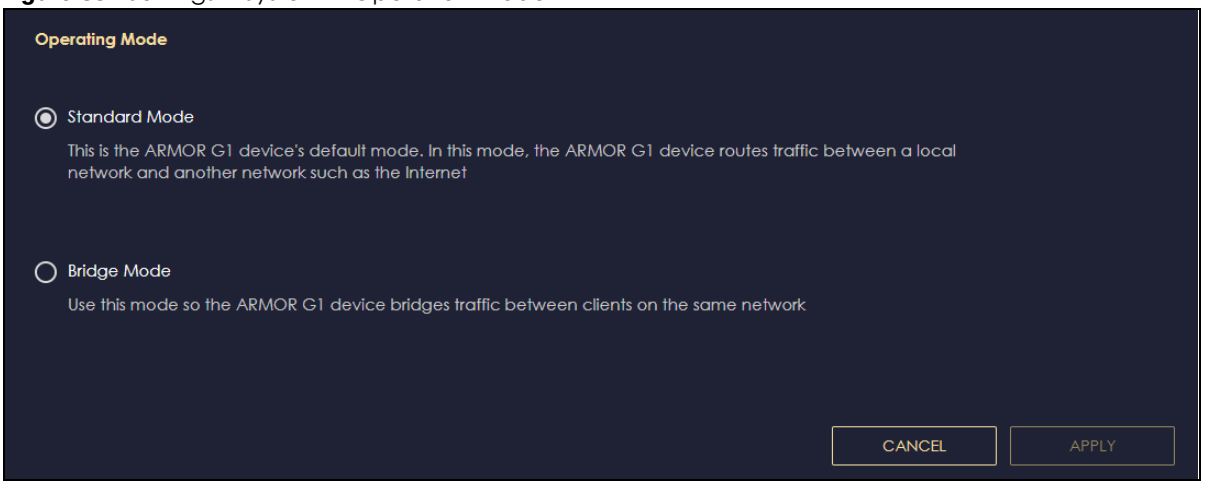
Figure 82 LAN and WAN IP Addresses in Router Mode



Bridge

Click **Settings** > **System** > **Operating Mode** to show the following screen.

Figure 83 Settings > System > Operation Mode



The following table describes the labels in this screen.

Table 54 Settings > System > Operation Mode

LABEL	DESCRIPTION
Standard Mode	Select **Standard (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.
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

14.8 Logs Screen

Use this screen to see the logged messages for the NBG6818.

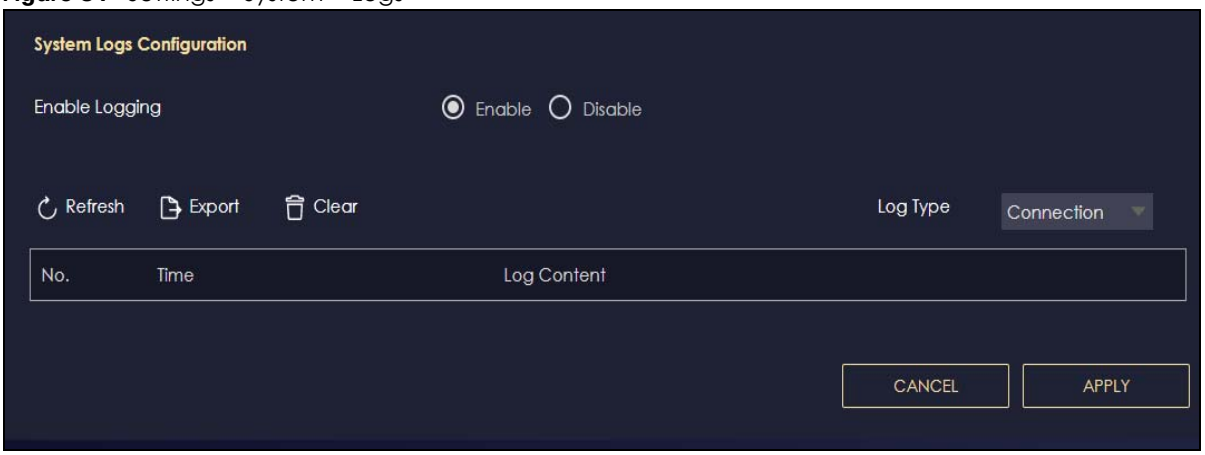
You can configure which logs to display in the Log screen.

The log wraps around and deletes the old entries after it fills. Select what logs you want to see from the **Log Type** drop list. The log choices depend on your settings above this screen. Click **Refresh** to renew the log screen. Click **Export** to save the current list of logs to your computer. Click **Clear Log** to delete all the logs.

Click **Apply** to save your settings. Click **Cancel** to start the screen afresh.

Click **Settings** > **System** > **Logs** to show the following screen.

Figure 84 Settings > System > Logs



CHAPTER 15
Troubleshooting

15.1 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
- NBG6818 Access and Login
- Internet Access
- Resetting the NBG6818 to Its Factory Defaults
- Wireless Connections
- USB Device Problems

15.2 Power, Hardware Connections, and LEDs

The NBG6818 does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the NBG6818.
2. Make sure the power adaptor or cord is connected to the NBG6818 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 NBG6818.
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 12.
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 NBG6818.

5 If the problem continues, contact the vendor.

15.3 NBG6818 Access and Login

I don't know the IP address of my NBG6818.

6 The default IP address of the NBG6818 in **Router Mode** is **192.168.1.1**. If the NBG6818 obtains a WAN IP address in the same subnet as the LAN IP address 192.168.1.1, the default LAN IP address will be changed to 10.0.0.1 automatically. See Auto-IP Change on page 73 for more information.
The default IP address of the NBG6818 in **Access Point Mode** is **192.168.1.2**.

7 If you changed the IP address and have forgotten it, you might get the IP address of the NBG6818 in **Router 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 NBG6818 (it depends on the network), so enter this IP address in your Internet browser.

8 If your NBG6818 in **Access Point 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.

9 Reset your NBG6818 to change all settings back to their default. This means your current settings are lost. See Section 15.5 on page 132 in the **Troubleshooting** for information on resetting your NBG6818.

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 15.5 on page 132.

I cannot see or access the **Login** screen in the Web Configurator.

1 Make sure you are using the correct IP address.

2 The default IP address of the NBG6818 in **Router Mode** is **192.168.1.1**. If the NBG6818 obtains a WAN IP address in the same subnet as the LAN IP address 192.168.1.1, the default LAN IP address will be changed to 10.0.0.1 automatically. See Auto-IP Change on page 73 for more information.
The default IP address of the NBG6818 in **Access Point Mode** is **192.168.1.2**.

- If you changed the IP address (Section 12.4 on page 106), 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 NBG6818.

3 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

4 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix B on page 171.

5 Make sure your computer is in the same subnet as the NBG6818. (If you know that there are routers between your computer and the NBG6818, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 12.4 on page 106.
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG6818. See Section 12.4 on page 106.

6 Reset the device to its factory defaults, and try to access the NBG6818 with the default IP address. See Section 1.5 on page 11.

7 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the NBG6818 using another service, such as Telnet. If you can access the NBG6818, check the remote management settings and firewall rules to find out why the NBG6818 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 NBG6818.

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 NBG6818.

4 If this does not work, you have to reset the device to its factory defaults. See Section 15.5 on page 132.

15.4 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 **Expert** > **Maintenance > Operation Mode**. Check your System Operation Mode setting.

- If the NBG6818 is in **Router Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access. Your computer and the NBG6818 should be in the same subnet.
- If the NBG6818 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.

3 If the NBG6818 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 NBG6818), 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 12.

2 Reboot the NBG6818.

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 12. If the NBG6818 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 NBG6818 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 NBG6818.

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.

15.5 Resetting the NBG6818 to Its Factory Defaults

If you reset the NBG6818, you lose all of the changes you have made. The NBG6818 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 NBG6818:

1. Make sure the power LED is on.
2. Press the **RESET** button for one to four seconds to restart/reboot the NBG6818.
3. Press the **RESET** button for longer than five seconds to set the NBG6818 back to its factory-default configurations.

   If the NBG6818 restarts automatically, wait for the NBG6818 to finish restarting, and log in to the Web Configurator. The password is "1234".

   If the NBG6818 does not restart automatically, disconnect and reconnect the NBG6818's power. Then, follow the directions above again.

15.6 Wireless Connections

I cannot access the NBG6818 or ping any computer from the WLAN.

1. Make sure the wireless LAN is enabled on the NBG6818.
2. Make sure the wireless adapter on your computer 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 NBG6818.
4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG6818.
5. Check that both the NBG6818 and the wireless adapter on your computer 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 NBG6818.
7. Make sure you allow the NBG6818 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 enable parental control in the **Parental Control** screen, set up rules and turn on the rules. Make sure that the keywords that you type are listed in the rule's **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 Keyword Blocking URL Checking section in the Applications chapter.

I cannot access the Web Configurator after I switched to AP mode.

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

Refer to Appendix B on page 141 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.

15.7 USB Device Problems

I cannot access or see a USB device that is connected to the NBG6818.

1. Disconnect the problematic USB device, then reconnect it to the NBG6818.
2. Ensure that the USB device has power.
3. Check your cable connections.
4. Restart the NBG6818 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 NBG6818 and try to connect to it again with your computer.
6. If the problem persists, contact your vendor.

What kind of USB devices do the NBG6818 support?

1. It is strongly recommended to use version 2.0 or higher USB storage devices (such as NTFS or FAT32 file system, USB hard drives) and/or USB devices. Other USB products are not guaranteed to function properly with the NBG6818.
2. The NBG6818 do not support 3G/4G USB dongles.

APPENDIX A
Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

See *http://www.zyxel.com/homepage.shtml* and also *http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml* for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications Corporation
- http://www.zyxel.com

Asia

China

- Zyxel Communications (Shanghai) Corp.
  Zyxel Communications (Beijing) Corp.
  Zyxel Communications (Tianjin) Corp.
- http://www.zyxel.cn

India

- Zyxel Technology India Pvt Ltd
- http://www.zyxel.in

Kazakhstan

- Zyxel Kazakhstan
- http://www.zyxel.kz

Korea

- Zyxel Korea Corp.
- http://www.zyxel.kr

Malaysia

- Zyxel Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philippines

- Zyxel Philippines
- http://www.zyxel.com.ph

Singapore

- Zyxel Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- Zyxel Communications Corporation
- http://www.zyxel.com/tw/zh/

Thailand

- Zyxel Thailand Co., Ltd
- http://www.zyxel.co.th

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- http://www.zyxel.com/vn/vi

Europe

Austria

- Zyxel Deutschland GmbH
- http://www.zyxel.de

Belarus

- Zyxel BY
- http://www.zyxel.by

Belgium

- Zyxel Communications B.V.
- http://www.zyxel.com/be/nl/
- http://www.zyxel.com/be/fr/

Bulgaria

- Zyxel България
- http://www.zyxel.com/bg/bg/

Czech Republic

- Zyxel Communications Czech s.r.o
- http://www.zyxel.cz

Denmark

- Zyxel Communications A/S
- http://www.zyxel.dk

Estonia

- Zyxel Estonia
- http://www.zyxel.com/ee/et/

Finland

- Zyxel Communications
- http://www.zyxel.fi

France

- Zyxel France
- http://www.zyxel.fr

Germany

- Zyxel Deutschland GmbH
- http://www.zyxel.de

Hungary

- Zyxel Hungary & SEE
- http://www.zyxel.hu

Italy

- Zyxel Communications Italy
- http://www.zyxel.it/

Latvia

- Zyxel Latvia
- http://www.zyxel.com/lv/lv/homepage.shtml

Lithuania

- Zyxel Lithuania
- http://www.zyxel.com/lt/lt/homepage.shtml

Netherlands

- Zyxel Benelux
- http://www.zyxel.nl

Norway

- Zyxel Communications
- http://www.zyxel.no

Poland

- Zyxel Communications Poland
- http://www.zyxel.pl

Romania

- Zyxel Romania
- http://www.zyxel.com/ro/ro

Russia

- Zyxel Russia
- http://www.zyxel.ru

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- http://www.zyxel.sk

Spain

- Zyxel Communications ES Ltd
- http://www.zyxel.es

Sweden

- Zyxel Communications
- http://www.zyxel.se

Switzerland

- Studerus AG

- http://www.zyxel.ch/

Turkey

- Zyxel Turkey A.S.
- http://www.zyxel.com.tr

UK

- Zyxel Communications UK Ltd.
- http://www.zyxel.co.uk

Ukraine

- Zyxel Ukraine
- http://www.ua.zyxel.com

Latin America

Argentina

- Zyxel Communication Corporation
- http://www.zyxel.com/ec/es/

Brazil

- Zyxel Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

Ecuador

- Zyxel Communication Corporation
- http://www.zyxel.com/ec/es/

Middle East

Israel

- Zyxel Communication Corporation
- http://il.zyxel.com/homepage.shtml

Middle East

- Zyxel Communication Corporation
- http://www.zyxel.com/me/en/

North America

USA

- Zyxel Communications, Inc. - North America Headquarters
- http://www.zyxel.com/us/en/

Oceania

Australia

- Zyxel Communications Corporation
- http://www.zyxel.com/au/en/

Africa

South Africa

- Nology (Pty) Ltd.
- http://www.zyxel.co.za

APPENDIX B
Setting Up Your Computer's IP Address

Note: Your specific NBG6818 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.

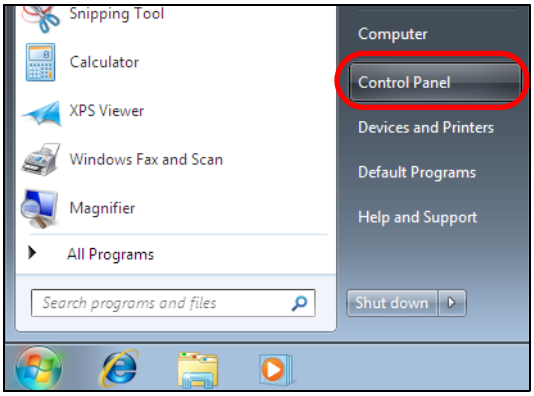
In this appendix, you can set up an IP address for:

- Windows 7 on page 141
- Mac OS X: 10.3 and 10.4 on page 145
- Mac OS X: 10.5 and 10.6 on page 148
- Linux: Ubuntu 8 (GNOME) on page 151
- Linux: openSUSE 10.3 (KDE) on page 155

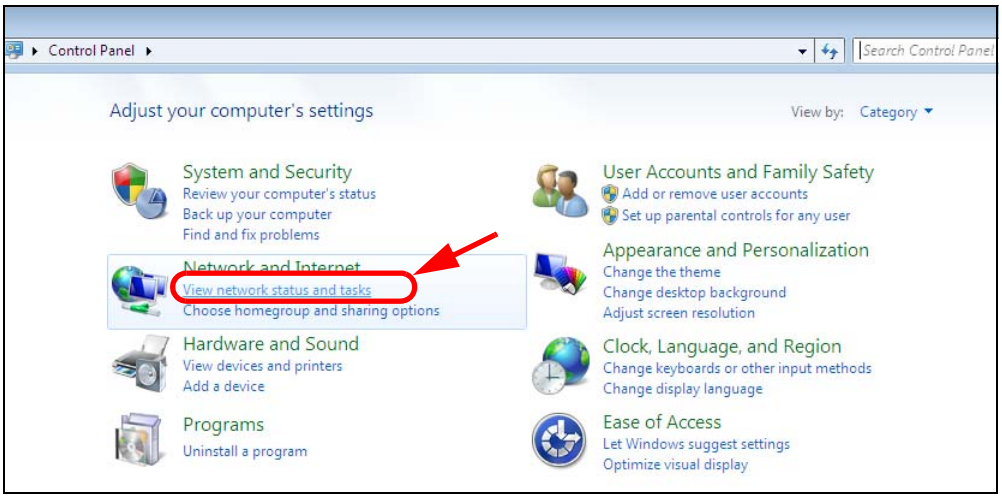
Windows 7

This section shows screens from Windows 7 Enterprise.

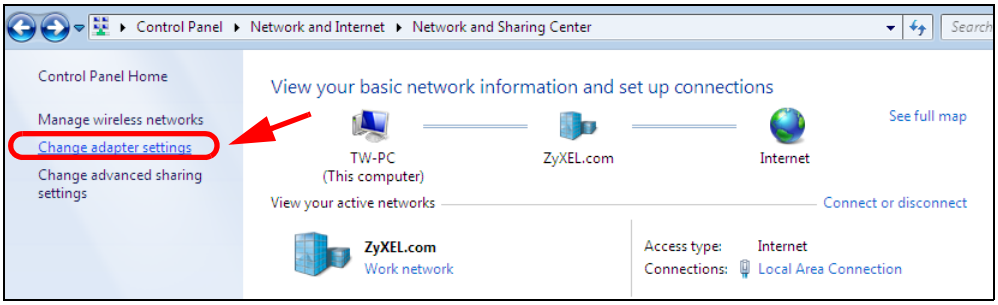
1 Click **Start** > **Control Panel**.



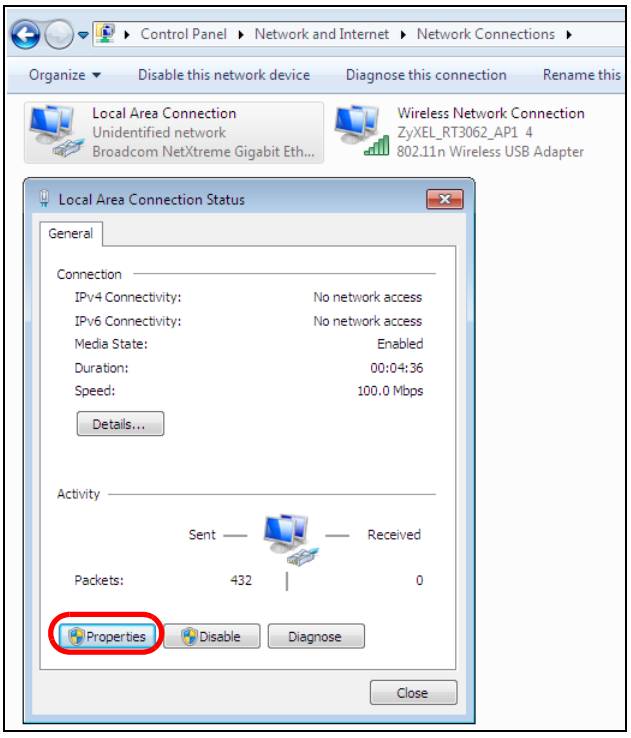
2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.



3 Click **Change adapter settings**.

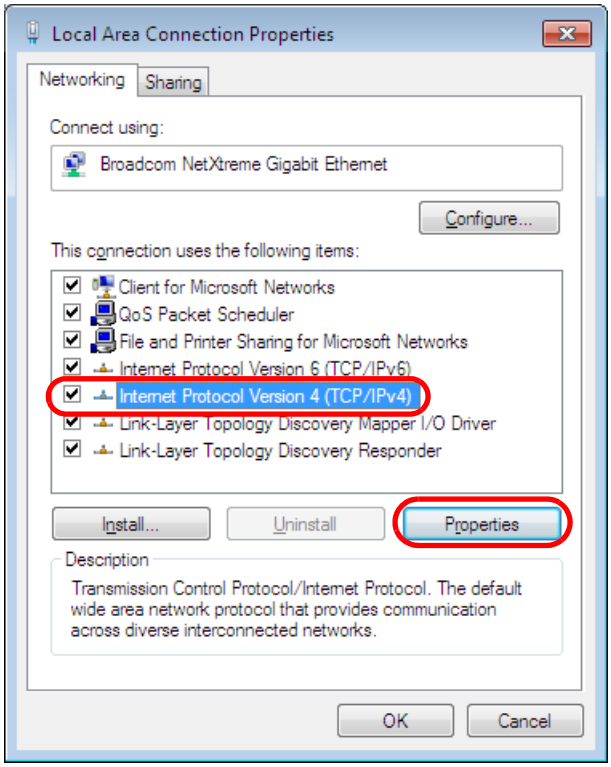


4 Double click **Local Area Connection** and then select **Properties**.

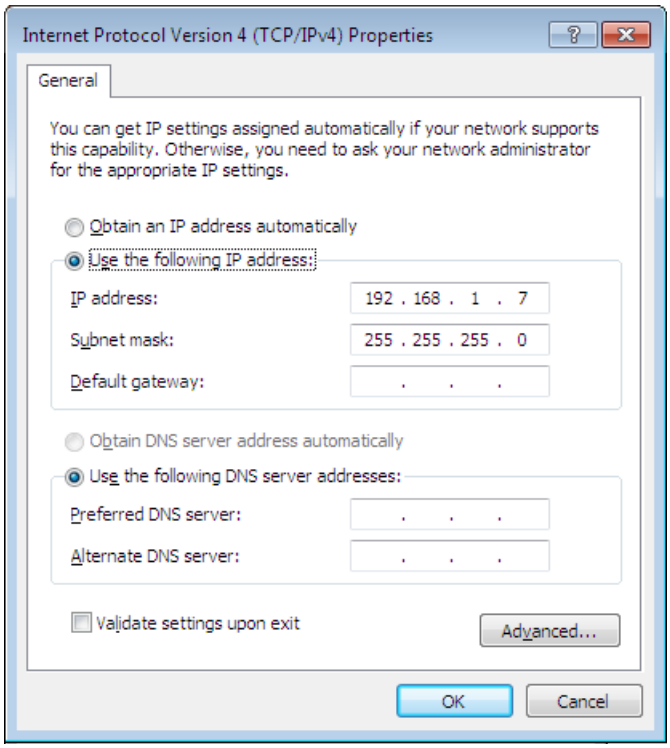


Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

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.

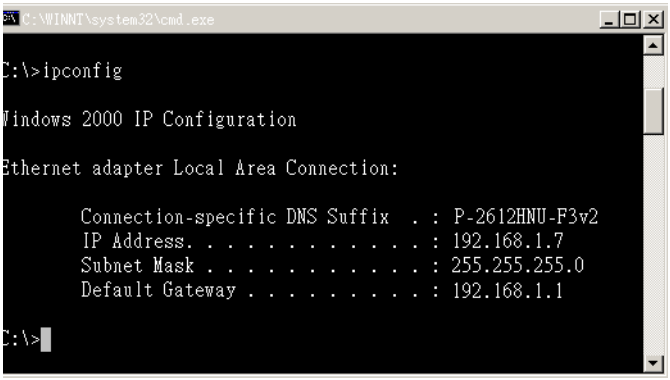
9 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

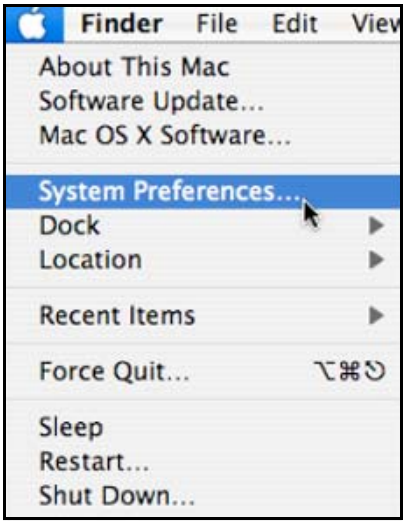
3 The IP settings are displayed as follows.



Mac OS X: 10.3 and 10.4

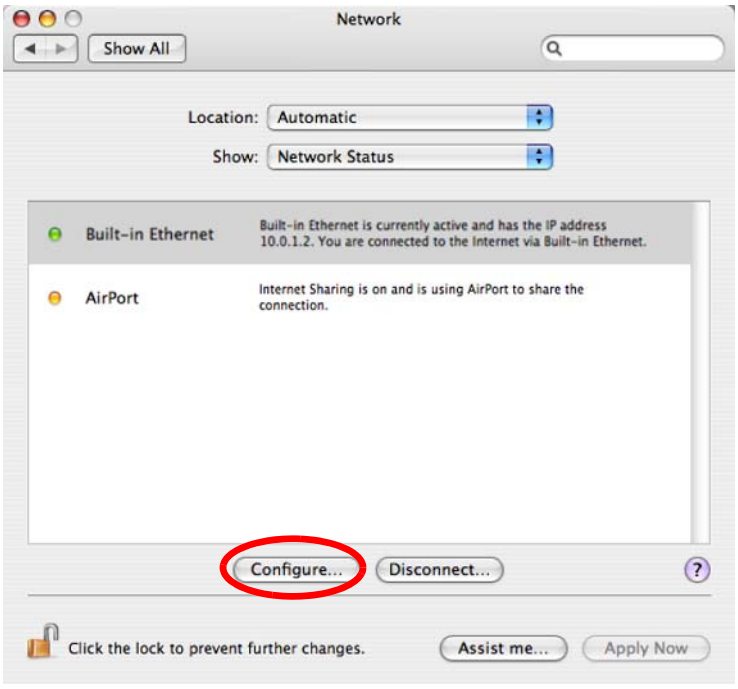
The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

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

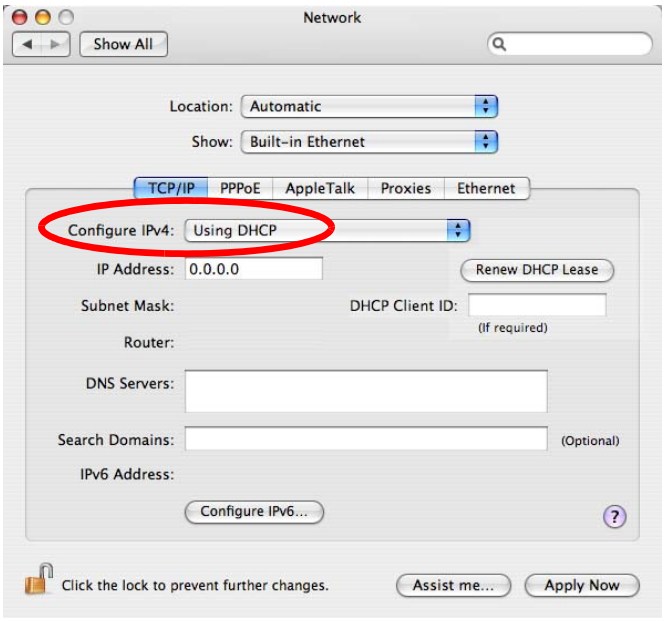


2 In the **System Preferences** window, click the **Network** icon.

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

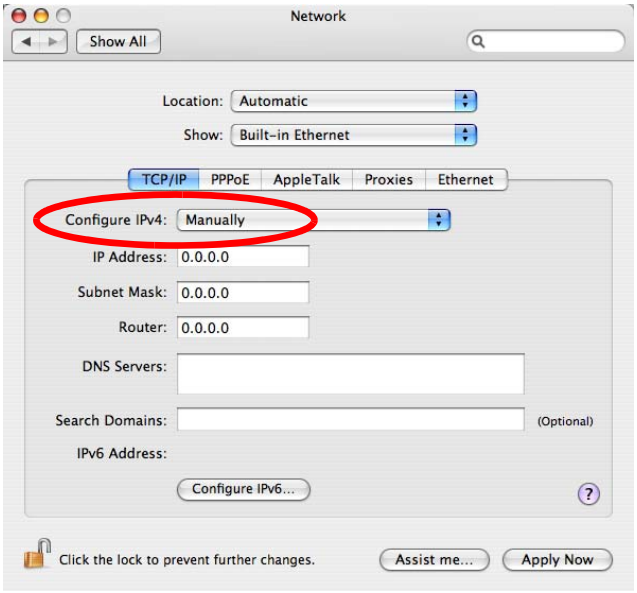


4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.



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.

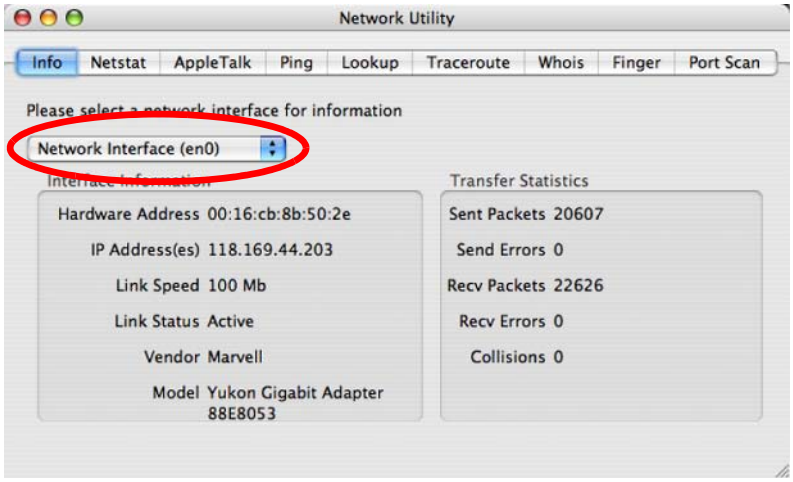


6 Click **Apply Now** and close the window.

Verifying Settings

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

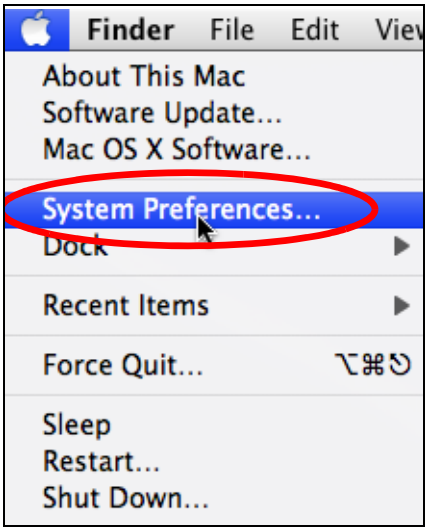
Figure 85 Mac OS X 10.4: Network Utility



Mac OS X: 10.5 and 10.6

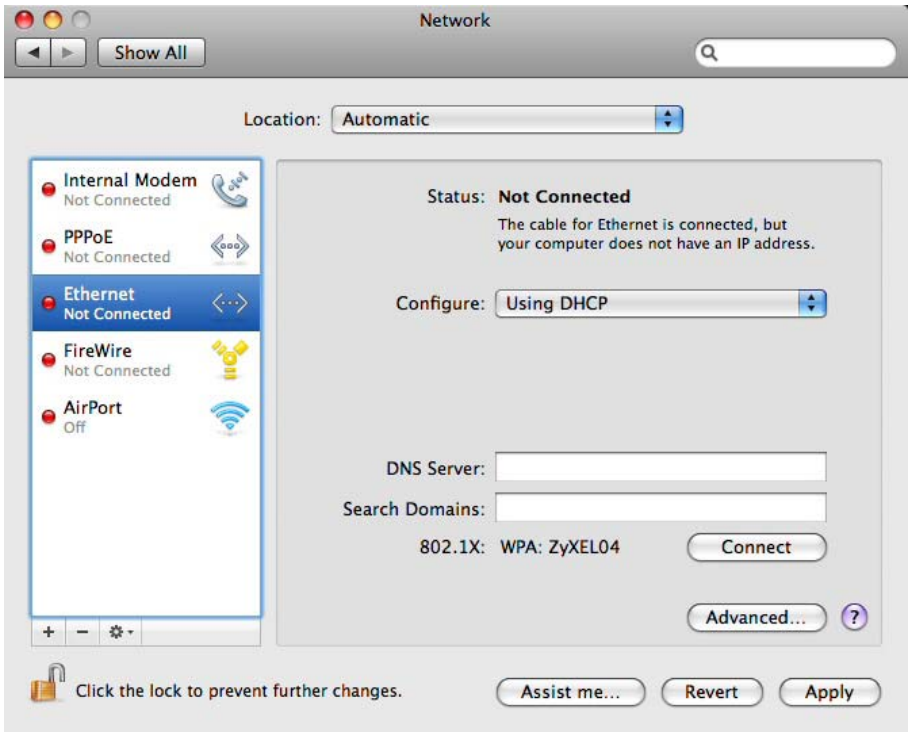
The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

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



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

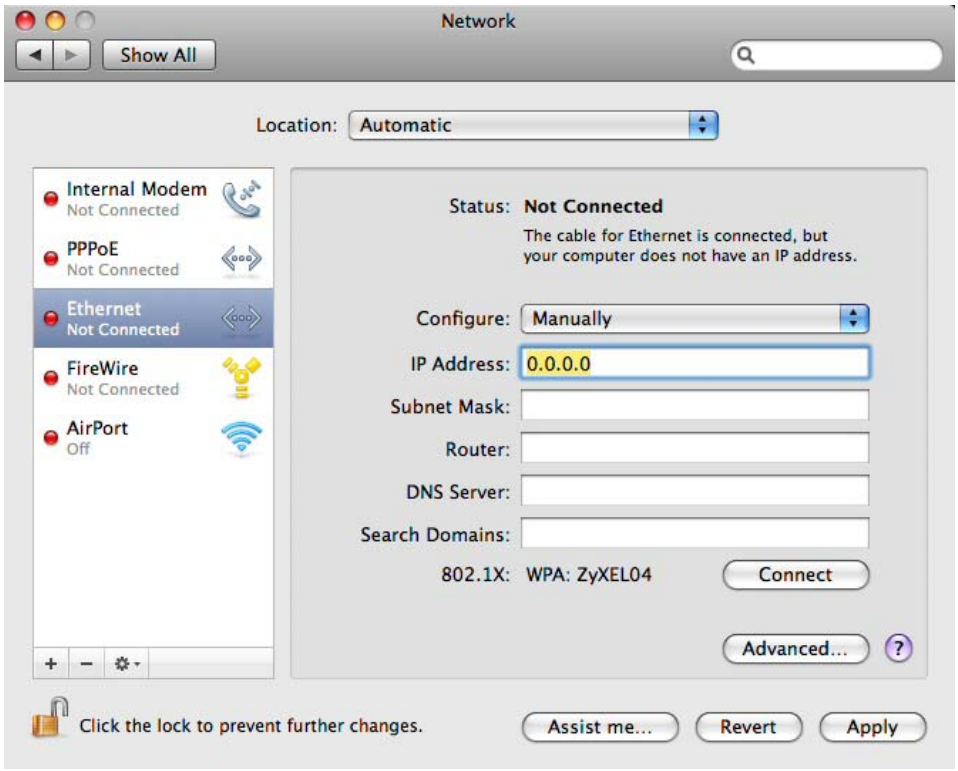
3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.



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 NBG6818.

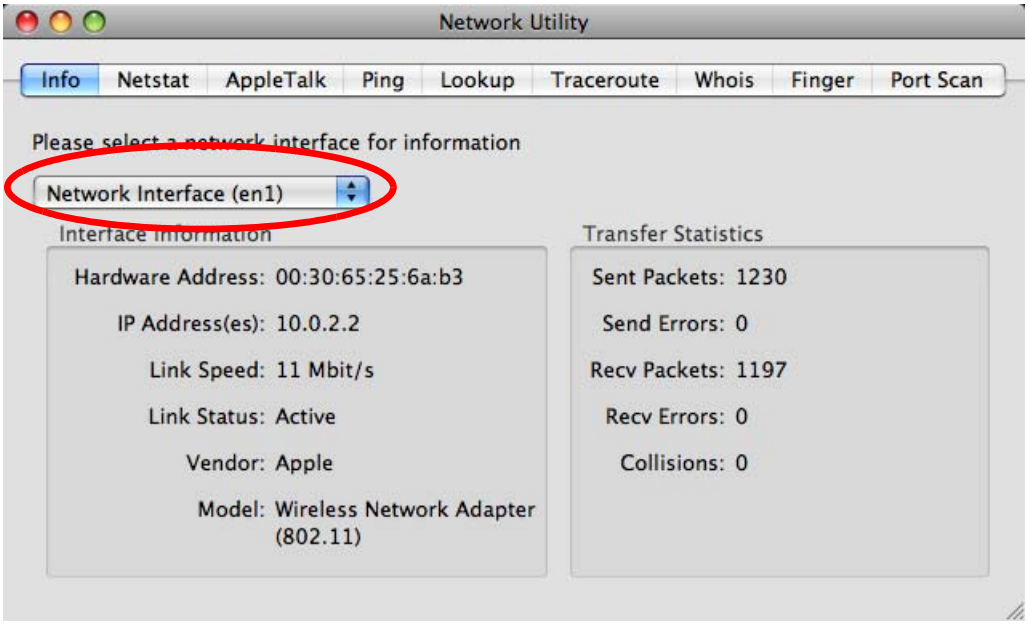


6 Click **Apply** and close the window.

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 86 Mac OS X 10.5: Network Utility



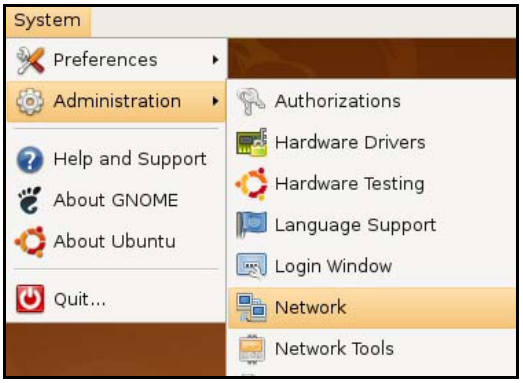
Linux: Ubuntu 8 (GNOME)

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.

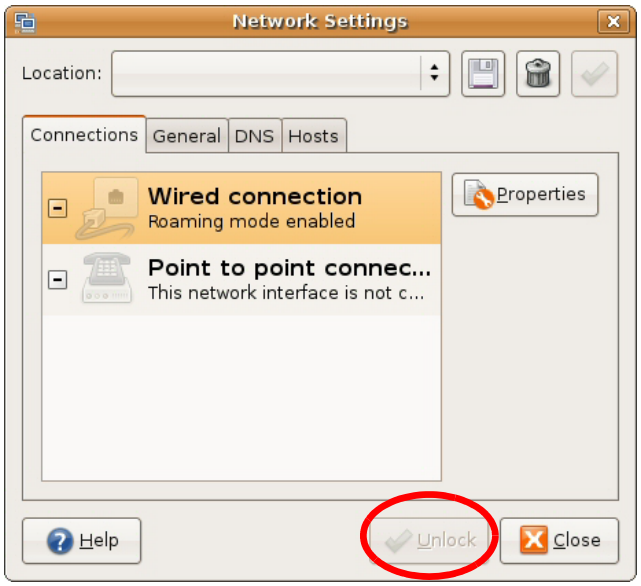
Note: Make sure you are logged in as the root administrator.

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

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

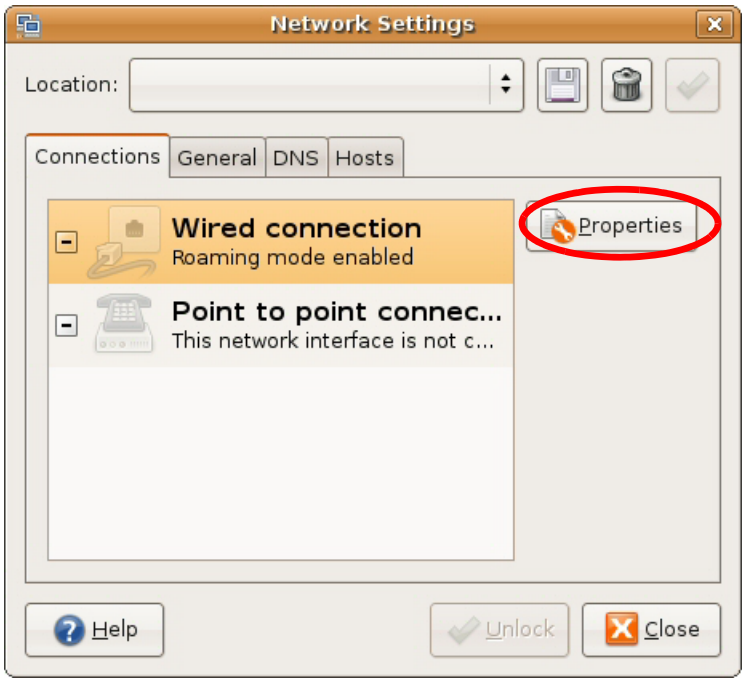


2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.



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.

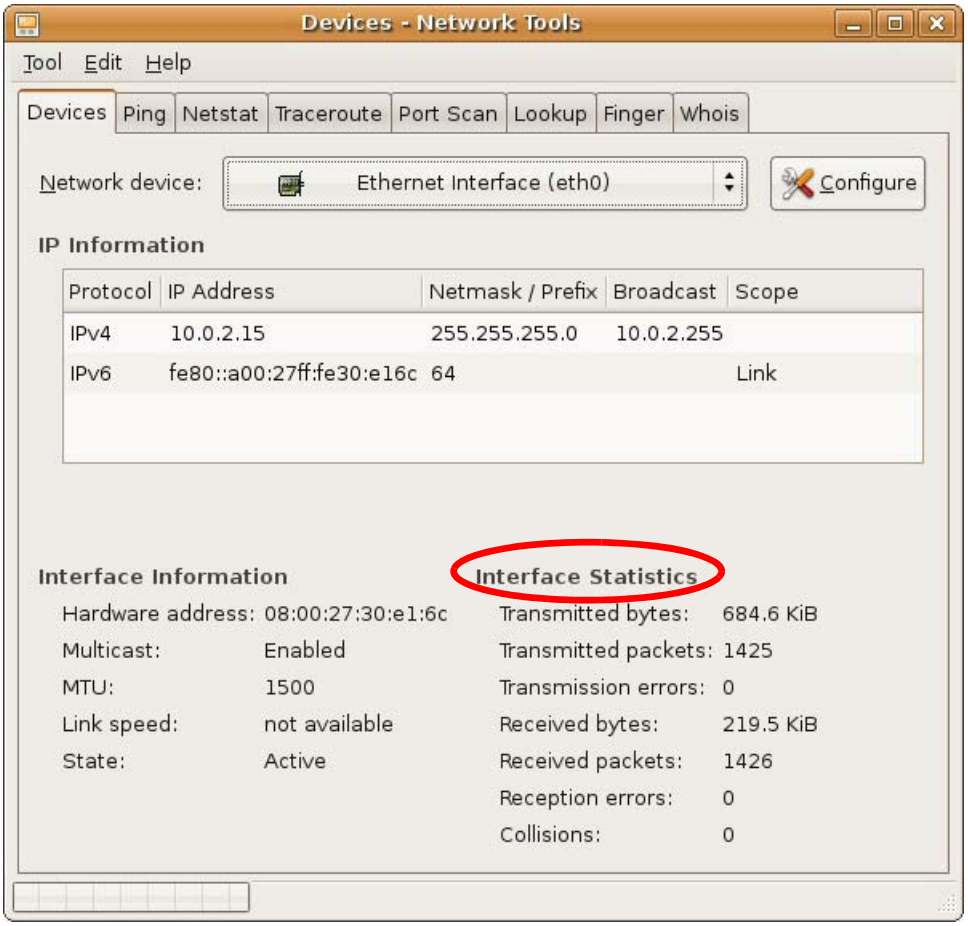
7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

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 87 Ubuntu 8: Network Tools



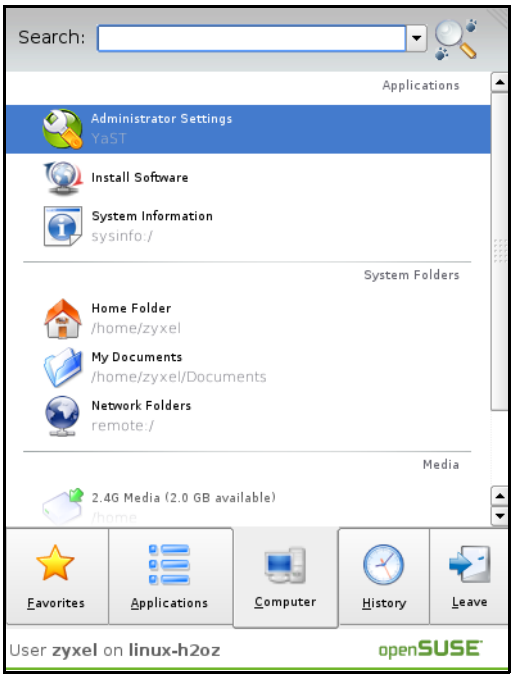
Linux: openSUSE 10.3 (KDE)

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.

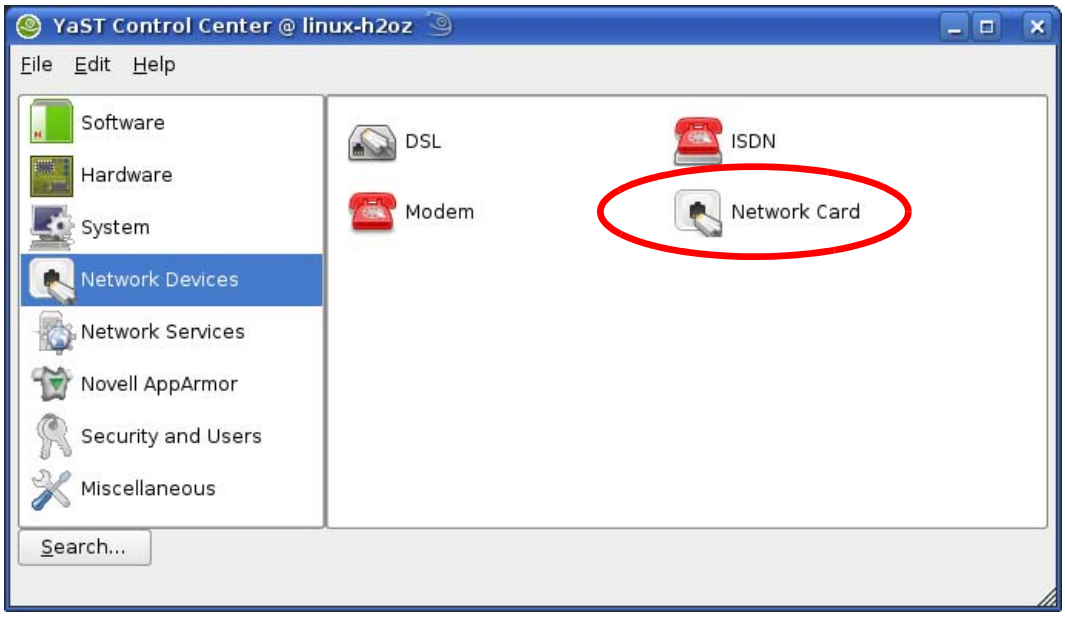
Follow the steps below to configure your computer IP address in the KDE:

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

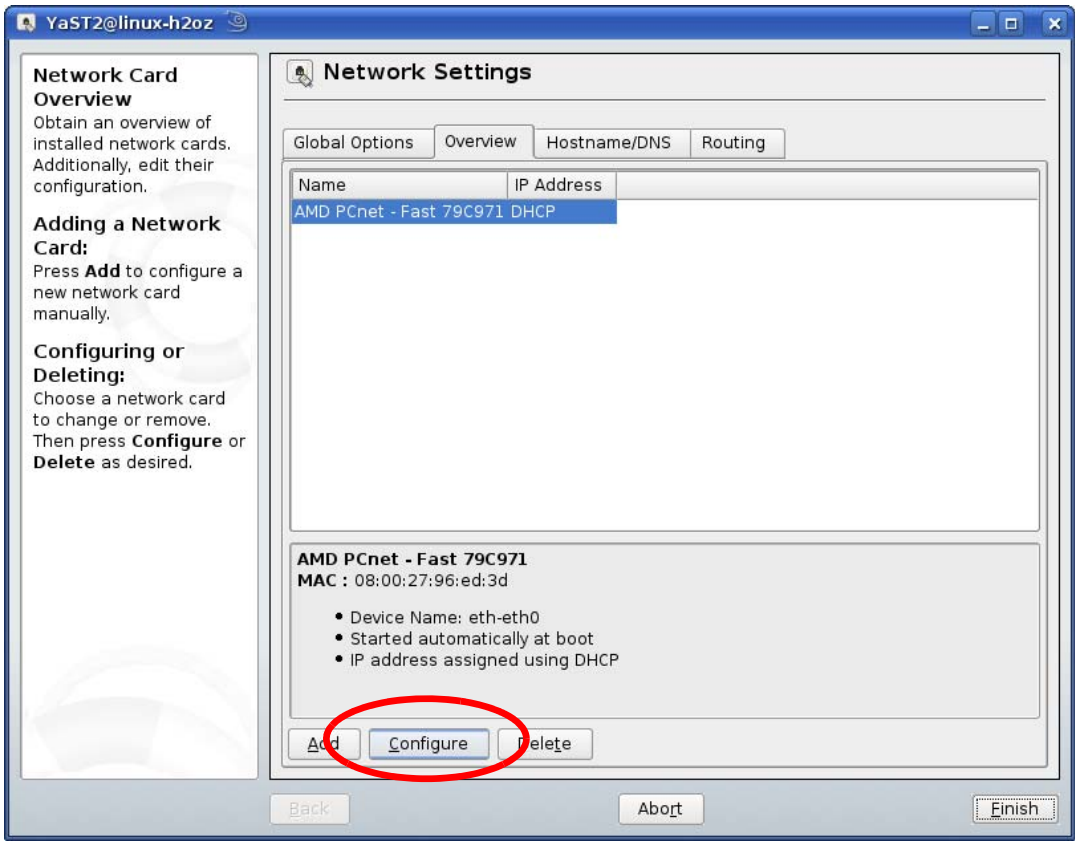


2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

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

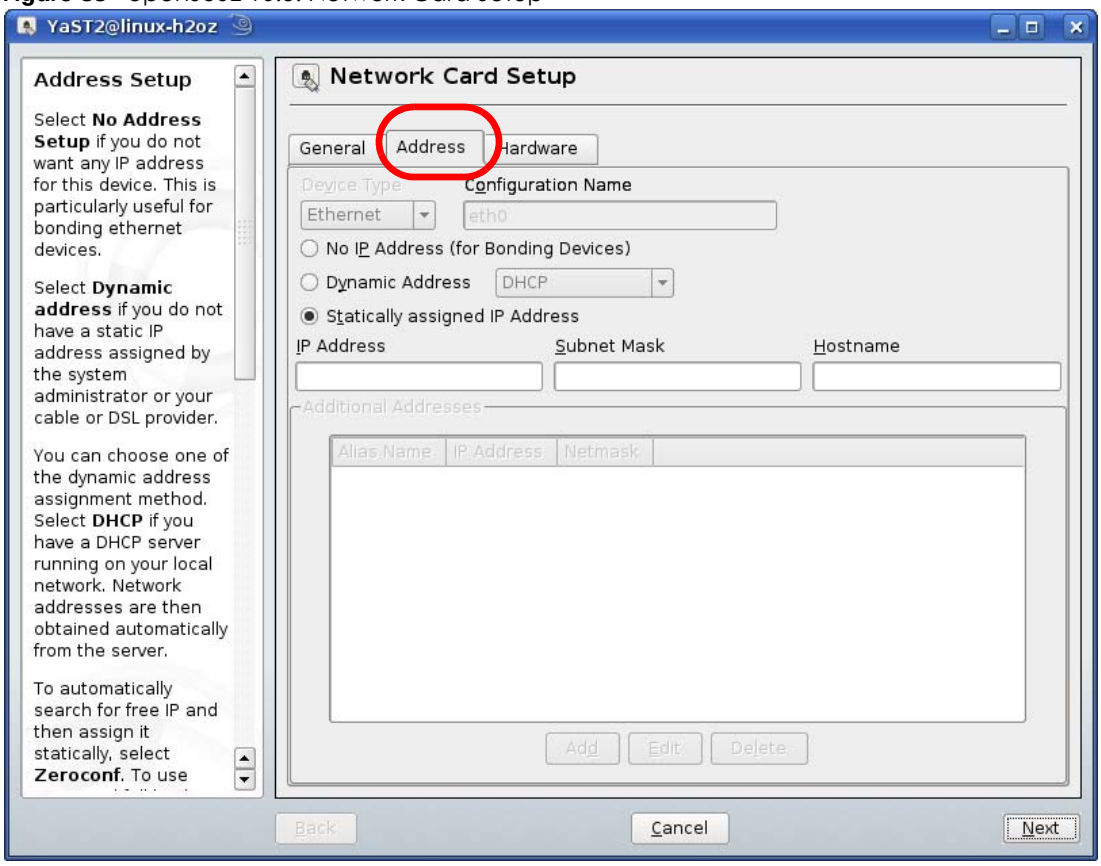


4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.



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

Figure 88 openSUSE 10.3: Network Card Setup

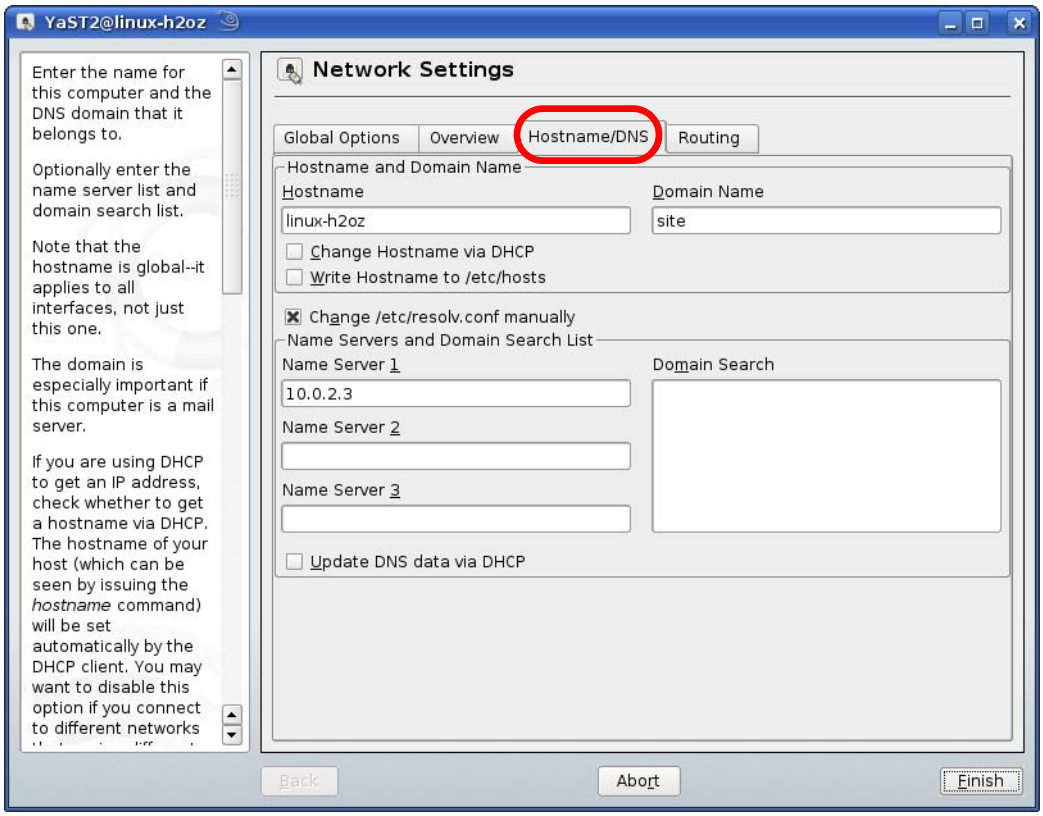


6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

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.

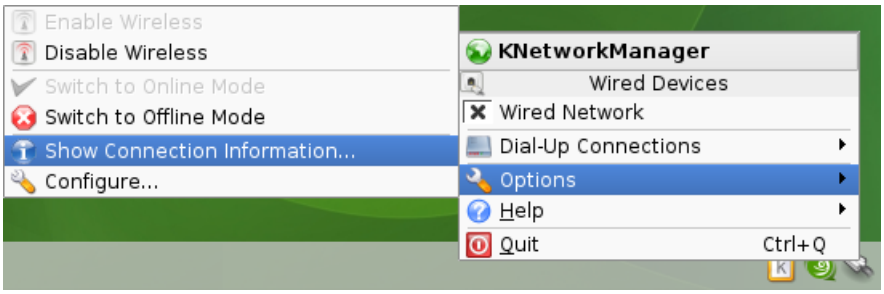


9 Click **Finish** to save your settings and close the window.

Verifying Settings

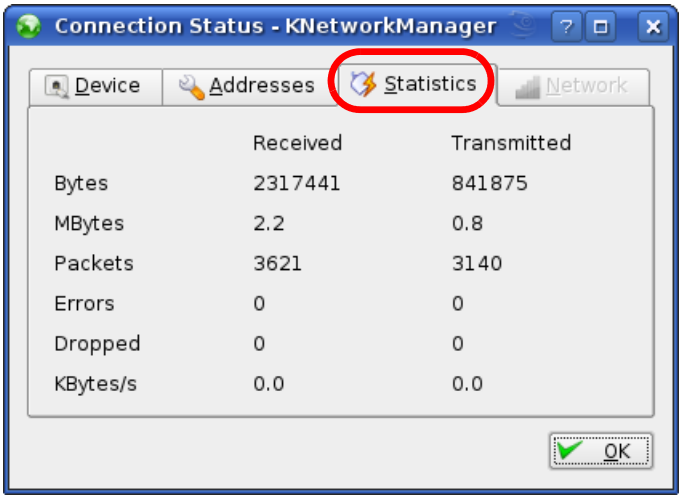
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 89 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 90 openSUSE: Connection Status - KNetwork Manager



APPENDIX C
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 55 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.
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.

Table 55 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.
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.

Table 55 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
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.

APPENDIX D
Legal Information

Copyright

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.

Regulatory Notice and Statement

UNITED STATES of AMERICA

The following information applies if you use the product within USA area.

FCC EMC Statement

- The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

  (1) This device may not cause harmful interference, and

  (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications 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 according to 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 or television reception, which is found 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:
  - Reorient or relocate the receiving antenna
  - Increase the separation between the devices
  - Connect the equipment to an outlet other than the receiver's
  - Consult a dealer or an experienced radio/TV technician for assistance

The following information applies if you use the product with RF function within USA area.

FCC Radiation Exposure Statement

- This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must be at least 20 cm from the user and must not be co-located or operating in conjunction with any other antenna or transmitter.
- Operation of this device is restricted to indoor use only, except for relevant user's manual mention that this device can be installed into the external environment.

FCC Part 68 Statement

- This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the back of this equipment is a label that contains, among other information, a product identifier in the format US: 1XXXXXXXX(part 68 ID). If requested, this number must be provided to the telephone company.
- List all applicable certification jack Universal Service Order Codes ("USOC") for the equipment. USOC JACK: RJ11C(Depend on EUT interface)
- A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

- The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.
- If this equipment US: 1XXXXXXXX(part 68 ID) causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.
- The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.
- If trouble is experienced with this equipment US: 1XXXXXXXX(part 68 ID), for repair or warranty information, please contact Zyxel Communication Inc.; 1130 N Miller street Anaheim, CA 92806-2001, USA ;TEL: 002 +1 714-6320882. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.
- Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.
- If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this US: 1XXXXXXXX(part 68 ID) does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

EUROPEAN UNION

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

Declaration of Conformity with Regard to EU Directive 2014/53/EU (Radio Equipment Directive, RED)

- Compliance information for ~~2.4GHz and/or 5GHz~~ wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED). And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5GHz 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 the 5GHz wireless LANs.
- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20cm between the radio equipment and your body.
- The maximum RF power operating for each band as follows:
  - the band 2,400 to 2,483.5 MHz is XXXX mW,
  - the bands 5,150 MHz to 5,350 MHz is XXXX mW,
  - the 5,470 MHz to 5,725 MHz is XXXX mW.

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС. **National Restrictions** • 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.
Español (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 2014/53/UE..
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. **National Restrictions** • In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage. • I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.

English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE. **National Restrictions** • 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.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. **National Restrictions** • 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 frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.
Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.

Notes:

- Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.
- 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	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

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 obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- 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.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- 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.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. 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.
- CAUTION: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic devices. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

  - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;

  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.
- CLASS 1 LASER PRODUCT
  APPAREIL À LASER DE CLASS 1
  PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.
  PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Important Safety Instructions

- Caution! The RJ-45 jacks are not used for telephone line connection.
- Caution! To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord.
- Caution! Do not use this product near water, for example a wet basement or near a swimming pool.
- Caution! Avoid using this product (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Caution! Always disconnect all telephone lines from the wall outlet before servicing or disassembling this product.
- Attention: Les prises RJ-45 ne sont pas utilisés pour la connexion de la ligne téléphonique.
- Attention: Pour réduire les risques d'incendie n'utiliser que des câbles de type 26 AWG ou des câbles de connexion plus épais.
- Attention: Ne pas utiliser ce produit près de l'eau, par exemple un sous-sol humide ou près d'une piscine.
- Attention: Évitez d'utiliser ce produit (autre qu'un type sans fil) pendant un orage. Il peut y avoir un risque de choc électrique de la foudre.
- Attention: Toujours débrancher toutes les lignes téléphoniques de la prise murale avant de réparer ou de démonter ce produit.

Environment Statement

ErP (Energy-related Products)

Zyxel products put on the EU market in compliance with the requirement of the European Parliament and the Council published Directive 2009/125/EC establishing a framework for the setting of ecodesign requirements for energy-related products (recast), so called as "ErP Directive (Energy-related Products directive) as well as ecodesign requirement laid down in applicable implementing measures, power consumption has satisfied regulation requirements which are:

- Network standby power consumption < 8W, and/or
- Off mode power consumption < 0.5W, and/or
- Standby mode power consumption < 0.5W.

(Wireless settings, please refer to ~~"Wireless"~~the chapter about wireless settings for more detail.)

European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.

台灣

以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 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，指依電信法規定作業之無線電通信。 低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- ~~電磁波曝露量 MPE 標準值 1 mW/cm^2，送測產品實測值為： XX mW/cm^2，本產品使用時建議應距離人體 XX cm。~~
- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用， 俟無干擾之虞，始得繼續使用。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作， 發射的信號應維持於操作頻帶中
- 使用無線產品時，應避免影響附近雷達系統之操作。
- ~~若使用高增益指向性天線，該產品僅應用於固定式點對點系統。~~
- 高增益指向性天線只得應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區

- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸：
  - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
  - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座 (如：北美 / 台灣電壓 110V AC，歐洲是 230V AC)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
  - 對永久連接之設備， 在設備外部須安裝可觸及之斷電裝置；
  - 對插接式之設備， 插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC if the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

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.

Index

A

Address Assignment 72
ALG 84
  and NAT 83
  and security policy 84
AP 10
AP Mode
  menu 44
  status screen 42
AP+Bridge 10
Application Layer Gateway, see ALG

B

Bridge/Repeater 10

C

certifications 167
  viewing 169
Channel 36, 43
channel 95
contact information 135
copyright 164
CPU usage 36, 43
customer support 135

D

DDNS
  service providers 116, 118
DHCP server 106
Digital Living Network Alliance 57
disclaimer 164
DLNA 57, 67
  indexing 69
  overview 67
  rescan 69
DLNA-compliant client 57
DNS Server 72
Domain Name System. See DNS.
duplex setting 36, 43
DynDNS 116, 118
DynDNS see also DDNS 116, 118

E

encryption 96
  and local (user) database 96
  key 97
  WPA compatible 97
ESSID 132

F

file sharing
  access right 65, 67
  bandwidth 67
  FTP 65
  Samba 62
  user account 63, 65
  Windows Explorer 62
  work group 62
Firewall
  guidelines 113
  ICMP packets 116
firewall
  stateful inspection 112
firmware version 35, 42
FTP
  ALG 84

G

General wireless LAN screen 98
Guest WLAN 97
Guest WLAN Bandwidth 97

H

H.323
ALG 84

I

IP Address 107

L

LAN 105
LAN overview 105
LAN setup 105
Link type 36, 43
local (user) database 96
and encryption 96
Local Area Network 105

M

MAC 100
MAC address 72, 95
cloning 72
MAC address filter 95
MAC address filtering 100
MAC filter 100
managing the device
good habits 11
using the web configurator. See web configurator.
using the WPS. See WPS.
MBSSID 10
Media access control 100
media client 67
media file 67, 68
type 68
media server
overview 67
meida file play 67
Memory usage 36, 43
mode 10

N

NAT
and ALG 83
Navigation Panel 37, 44
navigation panel 37, 44

O

operating mode 10

P

Point-to-Point Protocol over Ethernet 76
port speed 36, 43
PPPoE 76
dial-up connection

Q

Quality of Service (QoS) 102

R

RADIUS server 96
Reset button 11
Reset the device 11
Router Mode
status screen 34

S

Samba 58
Scheduling 104
security policy
and ALG 84
Service Set 99
Service Set IDentification 99
Service Set IDentity. See SSID.
SIP
ALG 84
SSID 36, 43, 95, 99
stateful inspection firewall 112
Status 34
Subnet Mask 107
System General Setup 121
System restart 124

U

user authentication 96
local (user) database 96
RADIUS server 96

V

VoIP pass through
see also ALG

W

WAN (Wide Area Network) 71
WAN MAC address 72
warranty 169
note 169
Web Configurator
how to access 54
Overview 54
web configurator 10
windows media player 67
wireless channel 132
wireless LAN 132
wireless LAN scheduling 104
Wireless network
basic guidelines 94
channel 95
encryption 96
example 94
MAC address filter 95
overview 94
security 95
SSID 95
Wireless security 95
overview 95
type 95
wireless security 132
Wireless tutorial 47
Wizard setup 16
WLAN button 11
work group 57
name 57
Windows 57
WPA compatible 97
WPS 10