

User's Guide

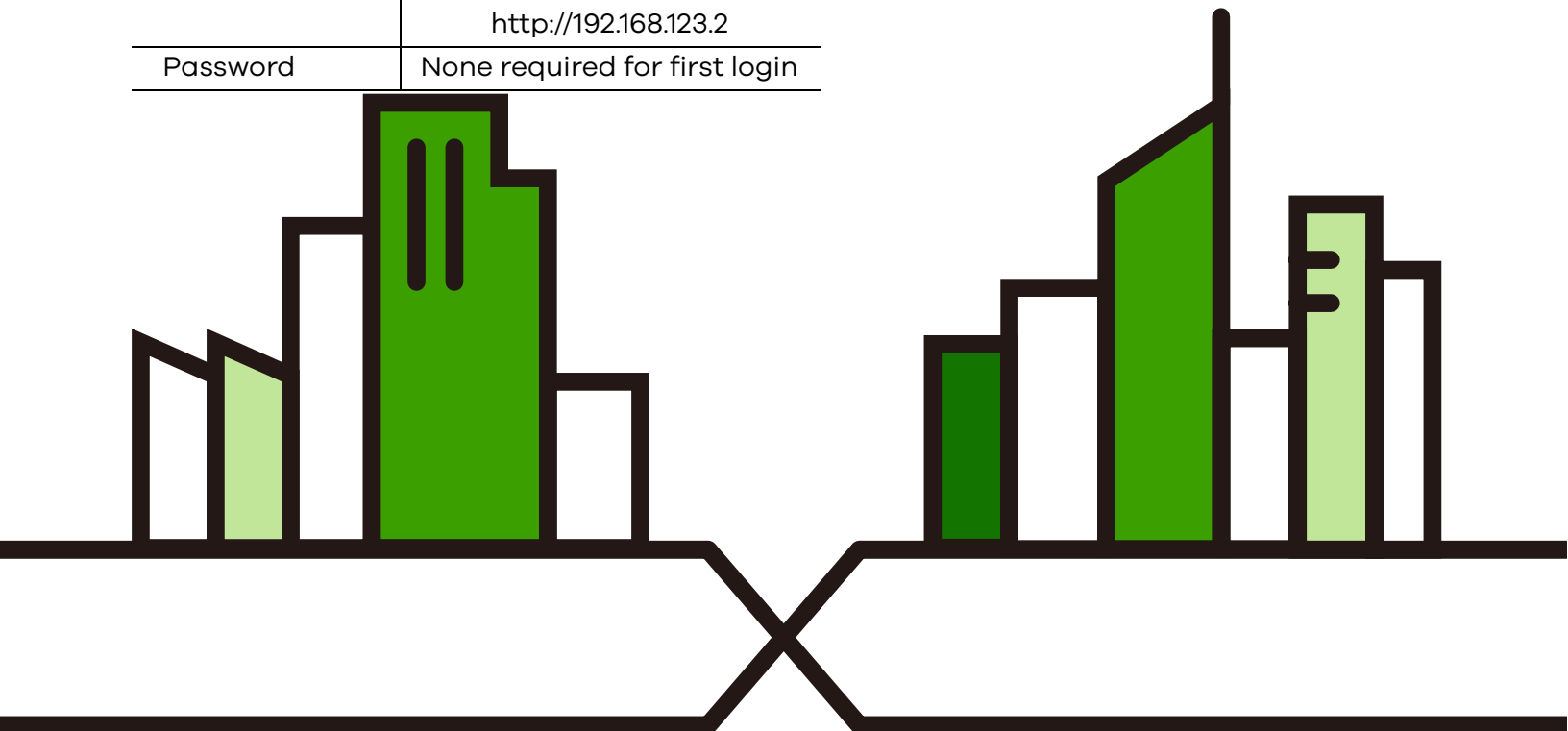
ARMOR G5

AX6000 Multi-Gigabit Security WiFi Router
Model: NBG7815

Default Login Details

LAN IP Address Standard (Router) Mode	http://zyxelwifi.com OR http://zyxelwifi.net OR http://192.168.123.1
Bridge Mode	http://DHCP-assigned IP OR http://192.168.123.2
Password	None required for first login

Version 1.00 Edition 4, 05/2022



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 NBG7815 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 NBG7815.



Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this guide.

Warnings tell you about things that could harm you or your device.










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

Syntax Conventions

- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Settings > WiFi > Main WiFi** means you first click **Settings** in the navigation panel, then the **WiFi** sub menu and finally the **Main WiFi** tab to get to that screen.

Icons Used in Figures

Figures in this user guide may use the following generic icons. The NBG7815 icon is not an exact representation of your device.

NBG7815 	Wireless Device 	Laptop Computer 
Switch 	Firewall 	Server 
Internet 	Desktop Computer 	Smartphone 

Contents Overview

User's Guide	10
Introduction	11
Hardware Installation and Connection	20
Wizard	25
Tutorials	35
Web Configurator	51
Standard Mode Status	58
Bridge Mode Status	61
Technical Reference	64
Applications	65
WAN	85
Wireless LAN	109
LAN	121
Security	131
System	138
Troubleshooting and Appendices	148
Troubleshooting	149

Table of Contents

Document Conventions	3
Contents Overview	4
Table of Contents	5
Part I: User's Guide	10
Chapter 1	
Introduction	11
1.1 NBG7815 Overview	11
1.2 Applications for the NBG7815	12
1.3 Operating Modes for the NBG7815	17
1.3.1 Standard (Router) Mode	17
1.3.2 Bridge Mode	18
1.4 Ways to Manage the NBG7815	18
1.5 Good Habits for Managing the NBG7815	19
Chapter 2	
Hardware Installation and Connection	20
2.1 Rear Panel	20
2.2 Front Panel LED	20
2.3 Mounting	21
2.3.1 Wall Mounting	21
2.3.2 Desk Placement	23
2.4 Resetting the NBG7815	23
2.4.1 How to Use the Reset Button	23
2.5 WPS Button	24
Chapter 3	
Wizard	25
3.1 Wizard Overview	25
3.2 Accessing the Wizard	25
Chapter 4	
Tutorials	35
4.1 Tutorials Overview	35
4.2 Run a Speed Test	35

4.3 Configure the NBG7815's WiFi Networks	36
4.4 Enable or Disable a Guest WiFi Network	39
4.5 Add Clients to a Profile	40
4.6 Configure a Profile's WiFi Schedule	40
4.7 Pause or Resume Internet Access on a Profile	42
4.8 Turn on or off the NBG7815's LED (Light)	43
4.9 Change Your NBG7815 Operating Mode	44
4.10 Configure a Port Forwarding Rule	45
4.11 Configure NBG7815 as an OpenVPN Server	47
4.12 Configure NBG7815 as an OpenVPN Client	49
Chapter 5	
Web Configurator.....	51
5.1 Web Configurator Overview	51
5.2 Accessing the Web Configurator	51
5.3 Navigation Panel	53
5.3.1 Standard Mode Navigation Panel	54
5.3.2 Bridge Mode Navigation Panel	56
Chapter 6	
Standard Mode Status	58
6.1 Standard Mode Overview	58
6.2 Standard Mode Status	58
Chapter 7	
Bridge Mode Status.....	61
7.1 Bridge Mode Overview	61
7.2 What You Can Do	61
7.3 Setting your NBG7815 to Bridge Mode	61
7.3.1 Accessing the Web Configurator in Bridge Mode	62
7.4 Bridge Mode Status	62
Part II: Technical Reference.....	64
Chapter 8	
Applications	65
8.1 Applications Overview	65
8.1.1 What You Can Do	65
8.1.2 What You Need To Know	65
8.1.3 Before You Begin	66
8.2 Parental Control	66

8.2.1 Device Setup	67
8.3 OpenVPN Server/Client	70
8.3.1 OpenVPN Server	70
8.3.2 OpenVPN Account	72
8.3.3 OpenVPN Client	73
8.4 USB Application	75
8.4.1 SAMBA Server	76
8.4.2 FTP Server	78
8.4.3 USB Media Sharing	80
8.5 Access Your Shared Files From a Computer	81
8.5.1 Using File Explorer	81
8.5.2 Using an FTP Program	82
Chapter 9	
WAN	85
9.1 WAN (Wide Area Network) Overview	85
9.2 What You Can Do	85
9.3 What You Need To Know	86
9.3.1 Configuring Your Internet Connection	86
9.4 Internet Connection	88
9.4.1 IPoE Encapsulation	88
9.4.2 PPPoE Encapsulation	91
9.4.3 PPTP Encapsulation	94
9.5 NAT and Port Forwarding	97
9.5.1 Add Port Forwarding Rule	99
9.6 Passthrough	100
9.7 Port Trigger	102
9.7.1 Add Port Trigger Rule	103
9.8 Dynamic DNS	104
9.9 UPnP	105
9.9.1 Turning on UPnP in Windows 10 Example	106
Chapter 10	
Wireless LAN	109
10.1 Wireless LAN Overview	109
10.1.1 What You Can Do	109
10.1.2 What You Should Know	110
10.2 Main WiFi	113
10.3 Guest WiFi	116
10.4 MAC Filter	117
10.4.1 Add MAC Address	118
10.5 WPS	118
10.6 Scheduling	120

Chapter 11	
LAN	121
11.1 LAN (Local Area Network) Overview	121
11.2 What You Can Do	121
11.3 What You Need To Know	121
11.4 LAN IP	122
11.4.1 Static DHCP Table-Add/Edit Rule	125
11.4.2 Configure LAN Screen in Bridge Mode	126
11.5 IPv6 LAN	128
Chapter 12	
Security	131
12.1 Security Overview	131
12.1.1 What You Can Do	131
12.1.2 What You Need To Know	131
12.2 IPv4 Firewall	132
12.2.1 IPv4 Firewall – Add Rule	134
12.3 IPv6 Firewall	135
12.3.1 IPv6 Firewall – Add Rule	136
Chapter 13	
System	138
13.1 System Overview	138
13.2 What You Can Do	138
13.3 Status	138
13.4 General Setting	141
13.5 Remote Access	143
13.6 Maintenance Setup	144
13.7 Operating Mode	145
13.8 Logs	146
Part III: Troubleshooting and Appendices	148
Chapter 14	
Troubleshooting	149
14.1 Overview	149
14.2 Power, Hardware Connections, and LEDs	149
14.3 NBG7815 Access and Login	150
14.4 Internet Access	151
14.5 Resetting the NBG7815 to Its Factory Defaults	152
14.6 WiFi Connections	152

14.7 OpenVPN Problems	154
14.8 USB File Sharing Problems	154
Appendix A Customer Support	156
Appendix B Setting Up Your Computer's IP Address.....	161
Appendix C Legal Information	177
Index	183

PART I

User's Guide

CHAPTER 1

Introduction

1.1 NBG7815 Overview

This chapter introduces the main features and applications of the NBG7815, also called ARMOR G5.

The NBG7815 is able to work on both 2.4G and 5G networks. It supports OpenVPN (server and client), firewall for IPv4 and IPv6, and multi-gigabit port.

This table summarizes some of the features that are available at the time of writing.

Table 1 Features Supported

FEATURES	NBG7815
Number of 2.5G/1G WAN port	1
Number of 10G Multi-Gigabit LAN port	1
Number of 1 Gbps Ethernet LAN ports	4
Number of USB port	1
Rubber feet for desktop placement	Yes
Wall-mount	Yes
Operating mode	Router and Bridge
Mobile app	ARMOR
OpenVPN (Server and Client)	Yes (router mode)
WiFi network	IEEE 802.11a/b/g/n/ac/ax compatible
Guest WiFi	Yes (router mode)
Firewall (IPv4 and IPv6)	Yes
NAT and Port Forwarding	Yes (router mode)
ALG (Application Layer Gateway)	Yes (router mode)
VPN (Virtual Private Network) Pass-through	Yes (router mode)
Port Triggering	Yes (router mode)
Dynamic DNS (Domain Name System)	Yes (router mode)
Parental Control	Yes (router mode)
IPv6 support	Yes (router mode)
UPnP (Universal Plug-and-Play)	Yes (router mode)
USB for file sharing (Samba)	Yes
USB file sharing using FTP	Yes
USB media sharing	Yes
Save configuration	Yes

1.2 Applications for the NBG7815

The NBG7815 supports the following applications.

Multi-Gigabit

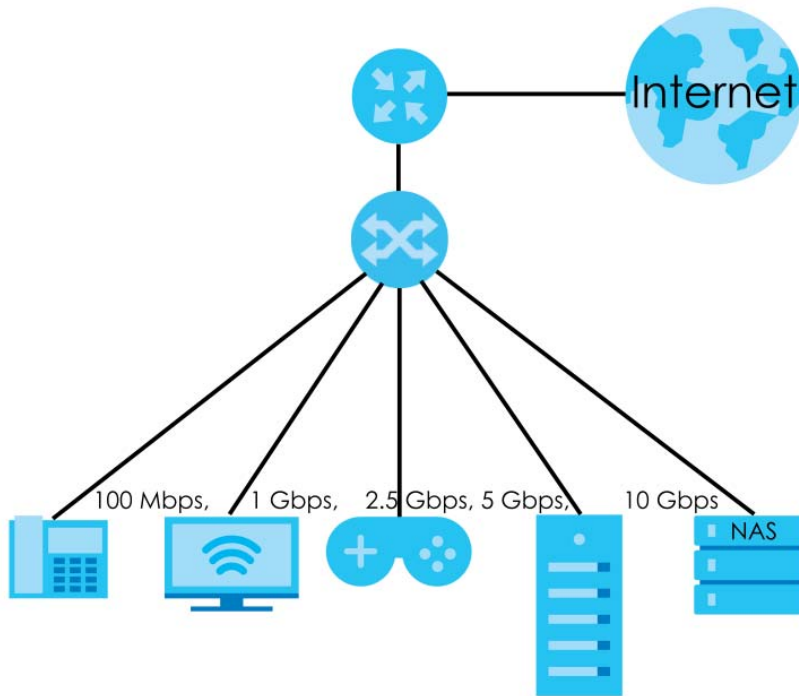
A 10 Gigabit port supports speed of 10 Gbps if the connected device supports 10 Gbps and a Cat 6a (up to 100 m) or Cat 6 cable (up to 50 m) is used. The speed drops to 1G if these criteria are not met; it drops to 100 Mbps if a Cat 5 cable is used (up to 100 m).

If a network device such as a 5G network card, gaming computer, server, Network Attached Storage (NAS) or Access Point (AP) only supports 2.5 Gigabit or 5 Gigabit connectivity, then the maximum speed potential of these devices is never reached.

In addition, at the time of writing, most existing cabling is Cat 5e or Cat 6, further limiting maximum speed or distance potential.

Multi-Gigabit (IEEE 802.3bz) solves these problems by additionally supporting 2.5 Gigabit and 5 Gigabit Ethernet connections over Cat 5e and higher Ethernet cables. Multi-Gigabit ports are also backward compatible with 100 Mbps and 1 Gigabit ports.

Figure 1 Multi-Gigabit Application



See the following table for the cables required and distance limitation to attain the corresponding speed.

Table 2 Ethernet Cable Types

CABLE	TRANSMISSION SPEED	MAXIMUM DISTANCE	BANDWIDTH CAPACITY
Category 5	100 Mbps	100 m	100 MHz
Category 5e	1 Gbps / 2.5 Gbps / 5 Gbps	100 m	100 MHz

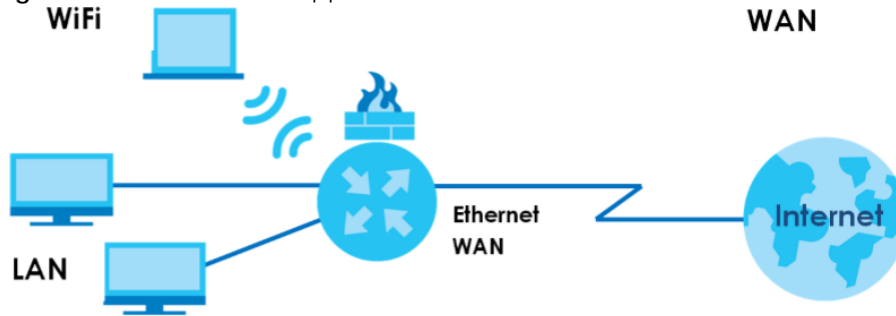
Table 2 Ethernet Cable Types (continued)

CABLE	TRANSMISSION SPEED	MAXIMUM DISTANCE	BANDWIDTH CAPACITY
Category 6	5 Gbps / 10 Gbps	50 m	250 MHz
Category 6a	10 Gbps	100 m	500 MHz
Category 7	10 Gbps	100 m	650 MHz

Internet Access

Your NBG7815 provides shared Internet access by connecting an Ethernet cable provided by the ISP (Internet Service Provider) to the **2.5G/1G** port. Connect network devices through the Ethernet ports of the NBG7815 (or wirelessly) so that they can communicate with each other and access the Internet.

Figure 2 Internet Access Application: Wired Connection

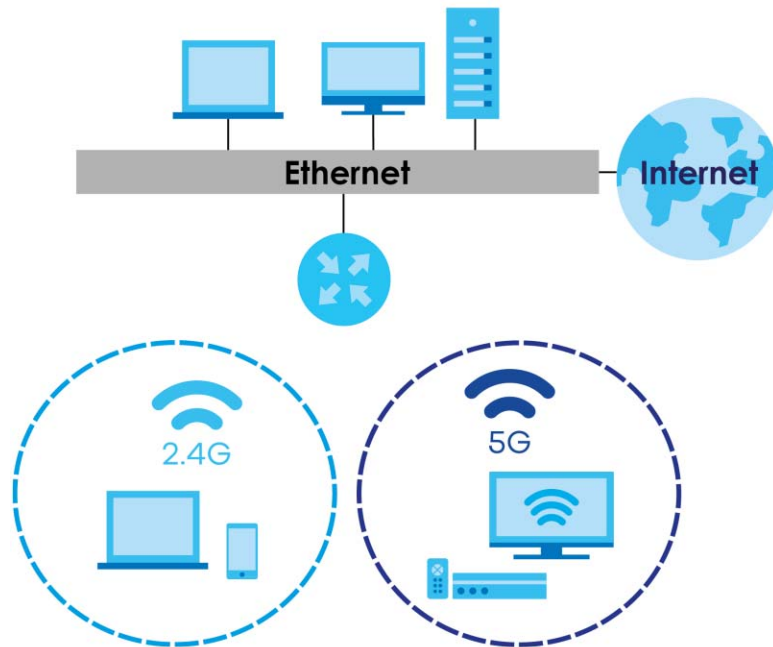


Dual-Band WiFi

IEEE 802.11a/b/g/n/ac/ax compliant clients can wirelessly connect to the NBG7815 to access network resources.

The NBG7815 is a dual-band gateway that can use both 2.4G and 5G networks at the same time. You can use the 2.4 GHz band for regular Internet surfing and downloading while using the 5 GHz band for time sensitive traffic like high-definition video, music, and gaming.

Figure 3 Dual-Band Application



You can use WPS (WiFi Protected Setup) to create an instant WiFi network connection with another WPS-compatible device.

Guest WiFi

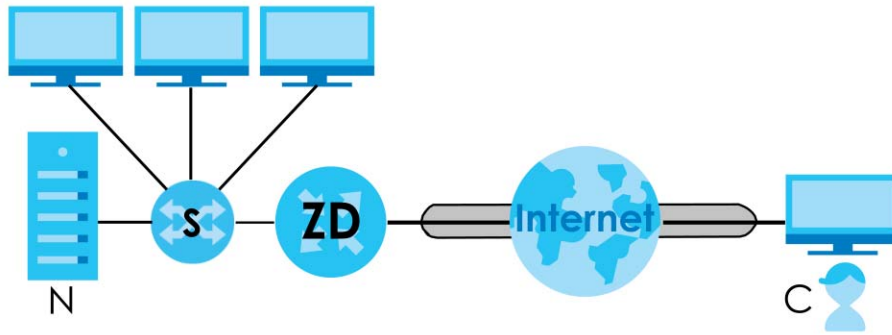
The NBG7815 allows you to set up a guest WiFi network where users can access the Internet through NBG7815, but not to other networks connected to it.

OpenVPN Server/Client

Your NBG7815 supports OpenVPN. OpenVPN is a VPN protocol which is open source and free of charge. It can be used to create a virtual private network or to interconnect local networks. It uses OpenSSL encryption library and SSLv3/TLSv1 protocols. This provides high security and anonymity for all transmitted data. It also provides faster connection speeds than other VPN protocols.

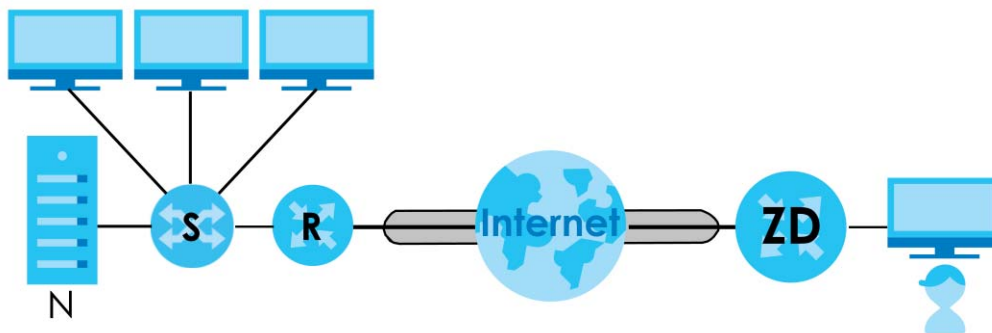
The following figure illustrates the NBG7815 (**ZD**) connected to a server network (**N**) through an Ethernet switch (**S**) function as an OpenVPN Server that transmit data to a client device (**C**) through a secure VPN channel.

Figure 4 OpenVPN Server Application



Alternatively, the following figure illustrates the NBG7815 (ZD) function as an OpenVPN Client to allow a VPN server (R) connected to a server network (N) through an Ethernet switch (S) to transmit data through a secure VPN channel to a client device connected to the NBG7815 (ZD).

Figure 5 OpenVPN Client Application



IPv6 and IPv6 Firewall

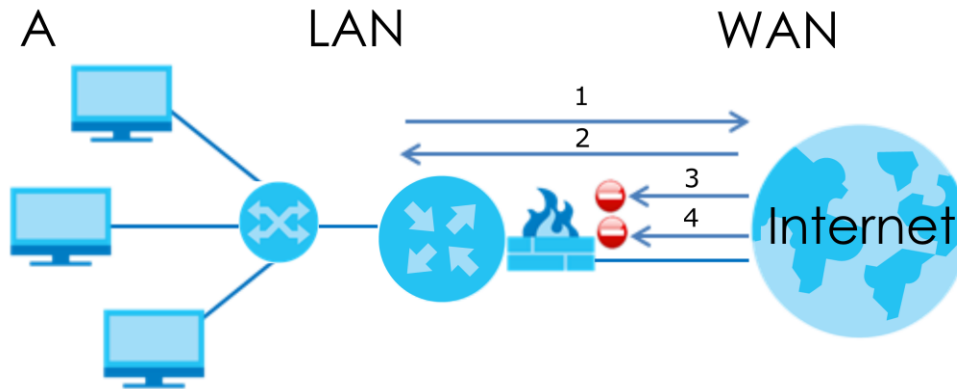
IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{38} IP addresses. The NBG7815 can use IPv4/IPv6 dual stack to connect to IPv4 and IPv6 networks, and support IPv6 rapid deployment (6RD).

Consequently, you can enable and create IPv6 firewall rules to filter IPv6 traffic.

Firewall protects your NBG7815 and network from attacks by hackers on the Internet and control access to it. The firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

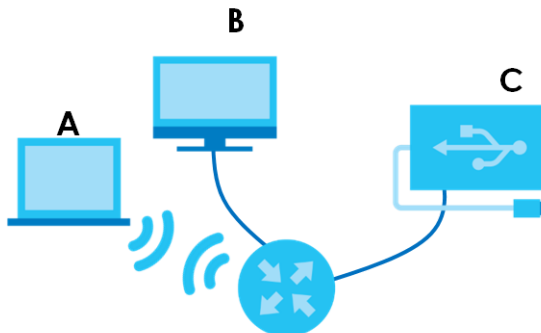
The following figure illustrates the firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

Figure 6 Default Firewall Action

USB File Sharing

Share files on a USB memory stick or hard drive connected to your NBG7815 with users on your network. The NBG7815 also supports file sharing using FTP (file transfer protocol).

The following figure illustrates the NBG7815's file server feature. Computers (A) and (B) can access files on a USB device (C) which is connected to the NBG7815.

Figure 7 File Sharing Overview

USB Media Sharing

The media server feature lets anyone on your network play video, music, and photos from the USB storage device connected to your NBG7815 without having to copy them to another computer. The NBG7815 can function as a DLNA-compliant media server, where the NBG7815 streams files to DLNA-compliant media clients like Windows Media Player.

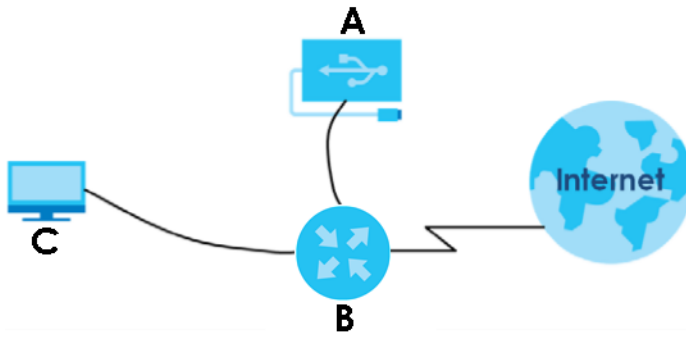
The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network.

The NBG7815 media server enables you to:

- Publish all share folders for everyone to play media files in the USB storage device connected to the NBG7815.
- 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.

Figure 8 Media Server Overview



The figure above illustrates a USB storage device (A) containing media files connected to the NBG7815 (B). A computer (C) with Windows Media Player installed can play the files.

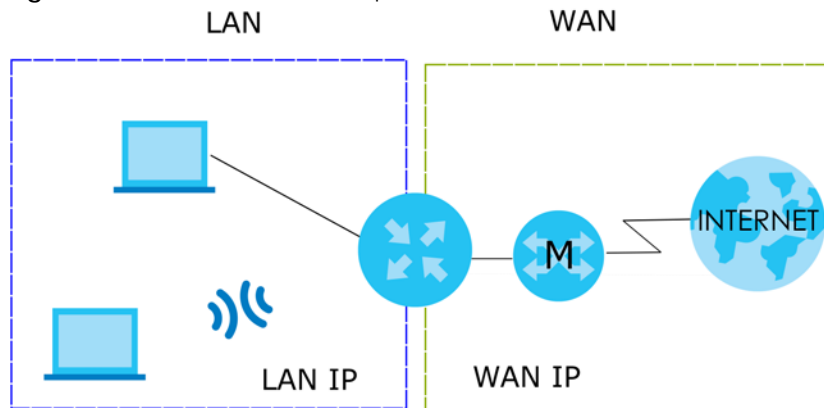
1.3 Operating Modes for the NBG7815

The NBG7815 is available in both Standard (router) mode and bridge mode.

1.3.1 Standard (Router) Mode

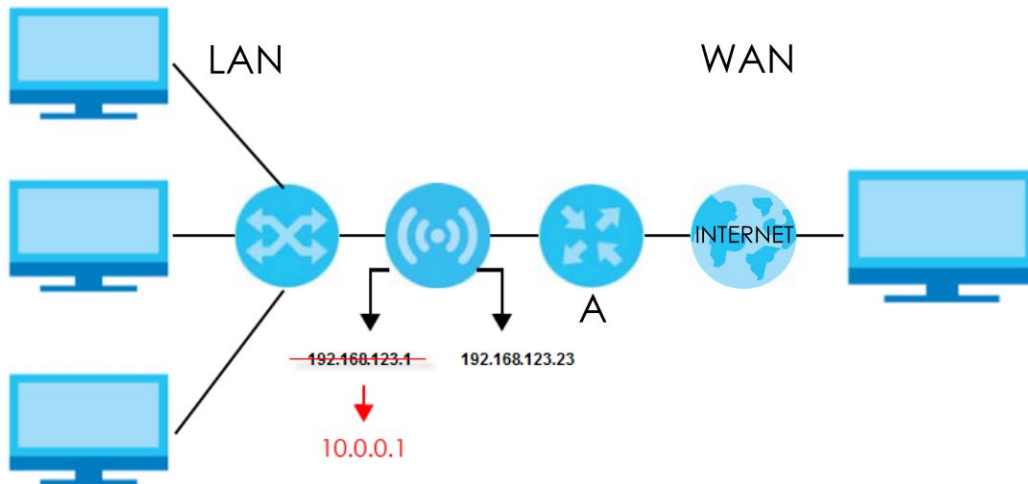
The NBG7815 is set to standard (router) mode by default. The NBG7815 is used to connect the local network to another network (for example, the Internet). In standard mode NBG7815 has two IP addresses, a LAN IP address and a WAN IP address. It also has more routing features. In the example scenario below, NBG7815 connects the local network to the Internet through a modem (M).

Figure 9 Standard Mode Example



Auto-IP Change

When the NBG7815 (A) gets a WAN IP address or a DNS server IP address which is in the same subnet as the LAN IP address 192.168.123.1, Auto-IP Change allows the NBG7815 to change its LAN IP address to 10.0.0.1 automatically. If the NBG7815'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 NBG7815 switches to use 192.168.123.1 as its LAN IP address.

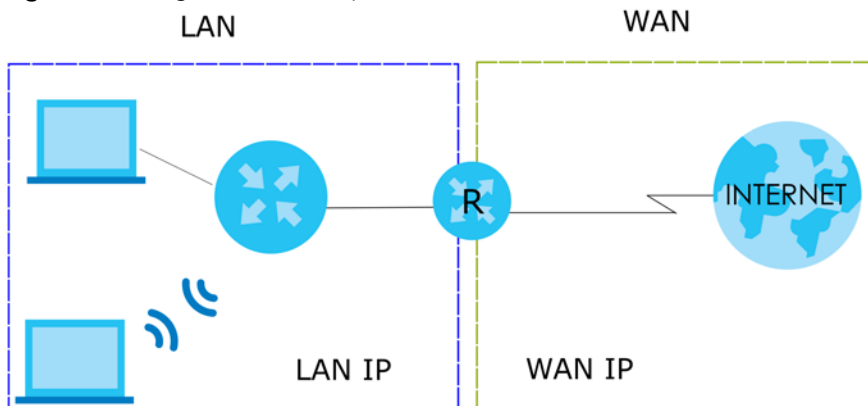
Figure 10 Auto-IP Change Example

Auto-IP Change only works under the following conditions:

- The NBG7815 must be in standard (router) mode for Auto-IP Change to become active.
- The NBG7815 is set to receive a dynamic WAN IP address.

1.3.2 Bridge Mode

Use your NBG7815 as a bridge if you already have a router or gateway on your network. In this mode your NBG7815 bridges a wired network (LAN) and WiFi in the same subnet. In bridge mode, NBG7815 has one IP address and NBG7815 interfaces are bridged together in the same network. In the example scenario below, NBG7815 connects the local network to the Internet through a router (R).

Figure 11 Bridge Mode Example

1.4 Ways to Manage the NBG7815

Use the following method to manage the NBG7815.

- Web Configurator. This is recommended for everyday management of the NBG7815 using a (supported) web browser.

- Zyxel ARMOR mobile app. This is the app you can use to manage the NBG7815 on your cellphone. To install the app, scan the QR code on the QSG.

1.5 Good Habits for Managing the NBG7815

Do the following things regularly to make the NBG7815 more secure and to manage the NBG7815 more effectively.

- Change the password. Use a password that is 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.

CHAPTER 2

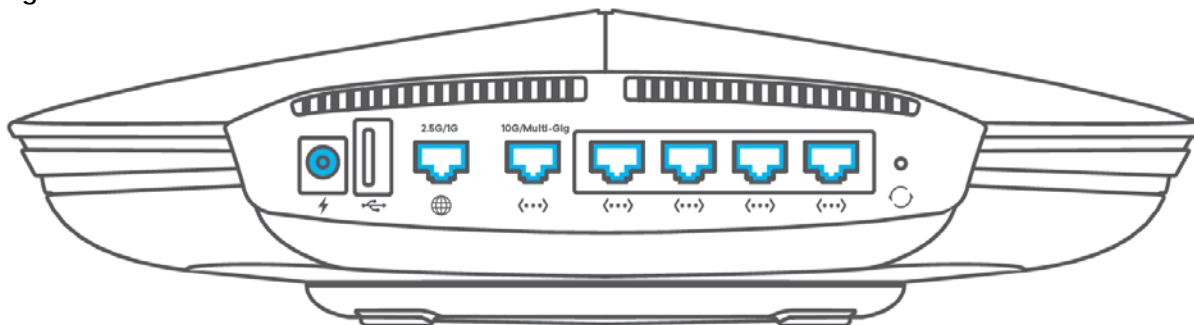
Hardware Installation and Connection

This chapter describes the front panel LED and rear panel of the NBG7815 and shows you how to mount the NBG7815 on the desk or wall.

2.1 Rear Panel

The following figure show the rear panel of the NBG7815. The rear panel contains:

Figure 12 Rear Panel



The following table describes the items on the rear panel.

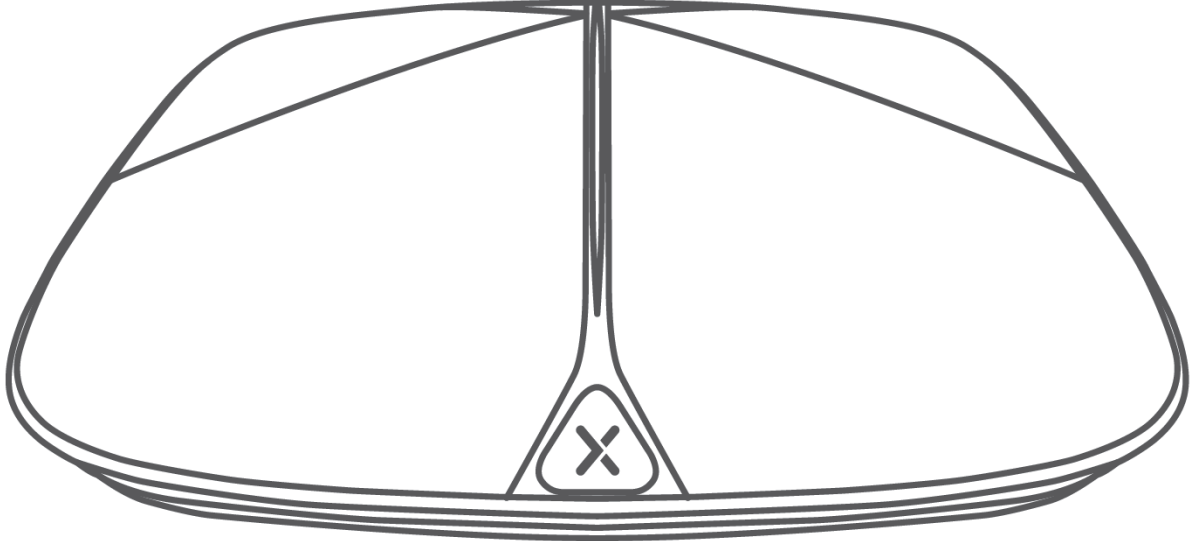
Table 3 Rear Panel Ports

LABEL	DESCRIPTION
Power	Connect the power adapter to start the NBG7815.
USB	The USB port is used for file-sharing and media server.
2.5G/1G	Connect an Ethernet cable to the Ethernet WAN port for Internet access.
10G/Multi-Gig	Connect Multi-Gigabit Ethernet devices to the Ethernet port for high speed Internet access.
LAN1 – LAN4	Connect computers or other Ethernet devices to Ethernet ports for Internet access.
Reset	Press the button for longer than 8 seconds to return the NBG7815 to the factory defaults.

2.2 Front Panel LED

After you connect the power to the NBG7815, view the LEDs to ensure proper functioning of the NBG7815 and as an aid to troubleshooting.

Figure 13 Front Panel LED



The following table describes the front panel LED.

Table 4 Front Panel LED

COLOR	STATUS	DESCRIPTION
White	On	The NBG7815 is receiving power.
	Blinking	The NBG7815 is booting.
Dark Blue	On	Bluetooth is ready.
	Blinking	Bluetooth linking is in process.
Amber	Blinking (Slow)	The NBG7815 is upgrading firmware.
	Blinking (Fast)	The NBG7815 is resetting.
Purple	Blinking	WPS is in process.
Purple and Dark Blue	Blinking	The NBG7815 is receiving power and ready for use.
Red	On	The NBG7815 detects Internet connection problems.

2.3 Mounting

The NBG7815 can be mounted on the wall or placed on the desk.

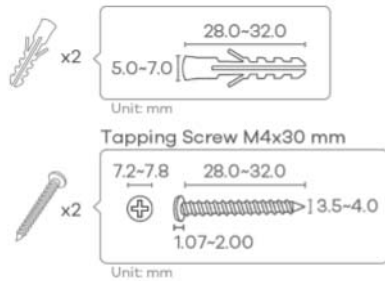
2.3.1 Wall Mounting

You may need screw anchors if mounting the NBG7815 on a concrete or brick wall.

Table 5 Wall Mounting Information

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

Note: See [The WiFi connection is slow or intermittent. on page 153](#) when selecting the mounting location.

Figure 14 Screw Specifications

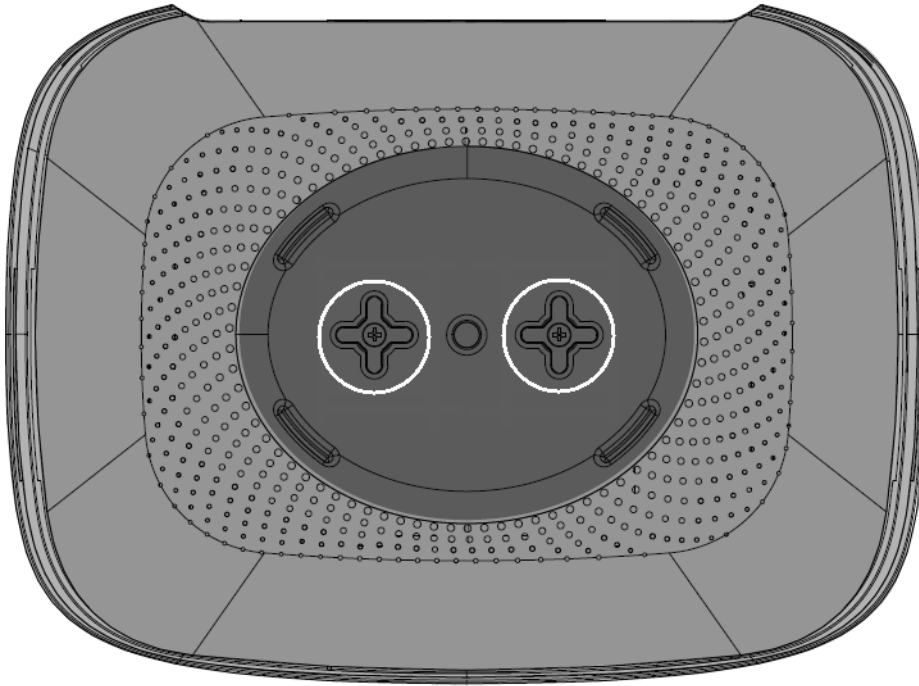
- 1 Select a position free of obstructions on a wall strong enough to hold the weight of the device.
- 2 Mark two holes on the wall at the appropriate distance apart for the screws.

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 NBG7815 with the connection cables.
- 5 Remove the rubber feet.
- 6 Align the holes on the back of the NBG7815 with the screws on the wall. Hang the NBG7815 on the screws.

Figure 15 Wall Mounting – Remove the Rubber Feet

2.3.2 Desk Placement

Place the side of the NBG7815 with the attached rubber feet carefully on the desk. These rubber feet help protect the NBG7815 from shock or vibration and ensure space between the desk and NBG7815.

Cautions:

- Ensure enough clearance around the NBG7815 to allow air circulation for cooling.
- Do NOT remove the rubber feet except when wall mounting as it provides space for air circulation.

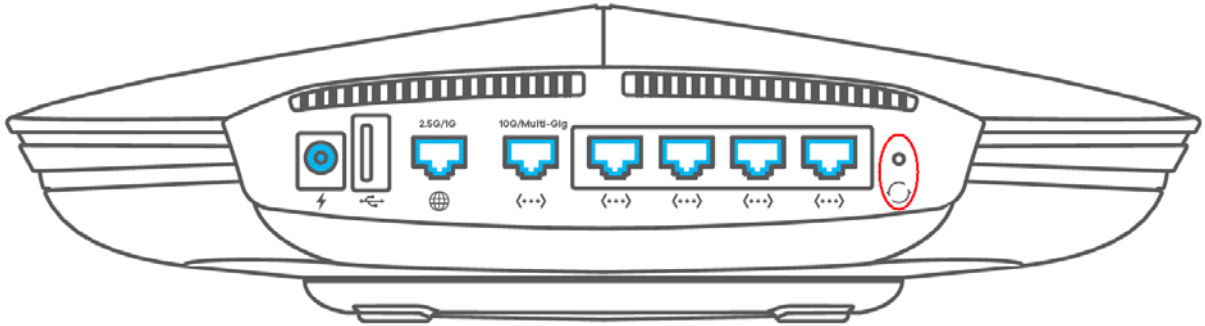
2.4 Resetting the NBG7815

If you forget your password or IP address, or you cannot access the Web Configurator, insert a thin object into the **Reset** hole on the NBG7815 to reload the factory-default configuration file. This means that you will lose all settings that you had previously saved.

2.4.1 How to Use the Reset Button

- 1 Make sure the power LED is on.
- 2 Locate the **Reset** hole.
- 3 Insert a thin object into the **Reset** hole for longer than 8 seconds to reset the NBG7815 back to its factory-default configuration (for example, default Standard (Router) operation mode and login IP address of 192.168.123.1, WiFi SSID and password).

Figure 16 Reset Hole



2.5 WPS Button

Your NBG7815 supports WiFi Protected Setup (WPS), which is an easy way to set up a secure WiFi network.

WPS allows you to quickly set up a WiFi 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 in the Web Configurator of the NBG7815 to activate WPS in order to quickly set up a WiFi network with strong security.

- 1 Make sure the power LED is on (not blinking).
- 2 Open the Web Configurator.
- 3 Click **Settings > WiFi > WPS**, and then press the WPS button.
- 4 Press the WPS button on another WPS-enabled device within range of the NBG7815. See the User's Guide of the other device for details.

Note: You must activate WPS in the NBG7815 and in another WiFi device within 2 minutes of each other.

CHAPTER 3

Wizard

3.1 Wizard Overview

The wizard appears automatically when the NBG7815 is accessed for the first time or when you reset the NBG7815 to its default factory settings. The wizard helps you set up the following:

- 2.4G/5G WiFi name and WiFi password
- Automatically check and update your NBG7815 firmware
- Create a myZykelCloud account to log into the NBG7815
- Authorize the NBG7815 to access your myZykelCloud account
- Create a local password as an alternative for logging into the NBG7815.

In this chapter, you will learn how to:

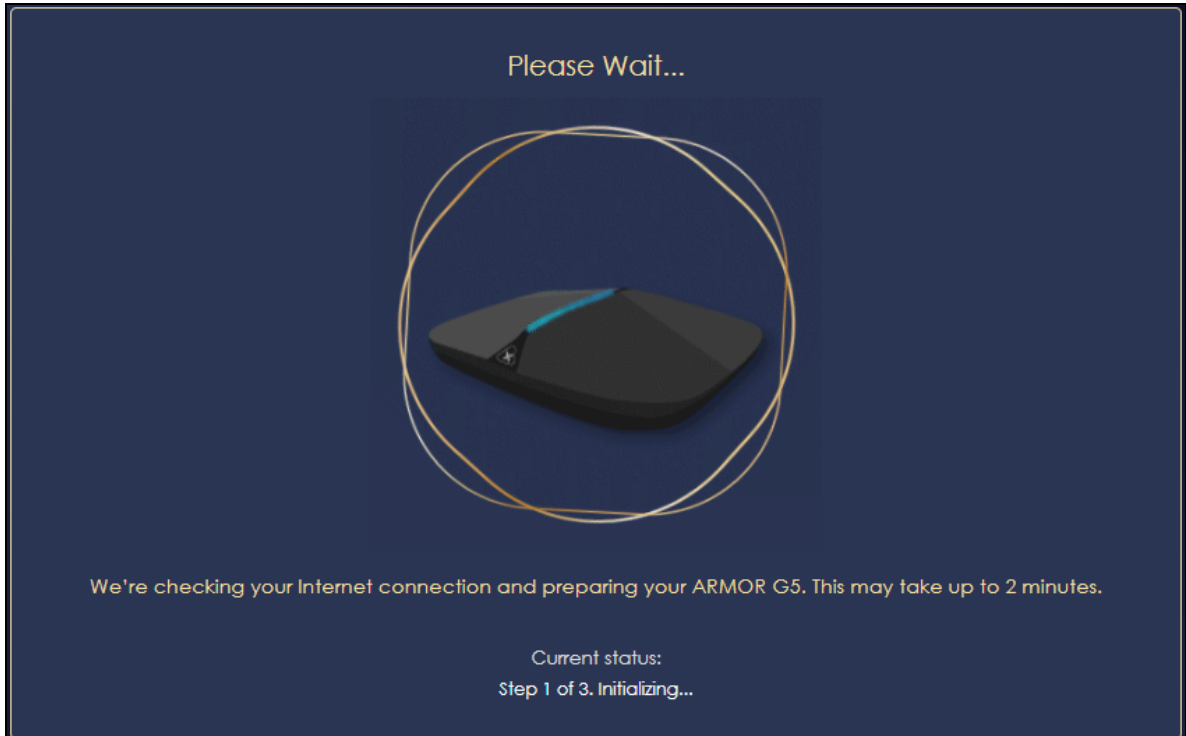
- Go through NBG7815 (ARMOR G5) wizard steps
- Configure basic settings for your WiFi
- Create a myZykel Cloud account.

3.2 Accessing the Wizard

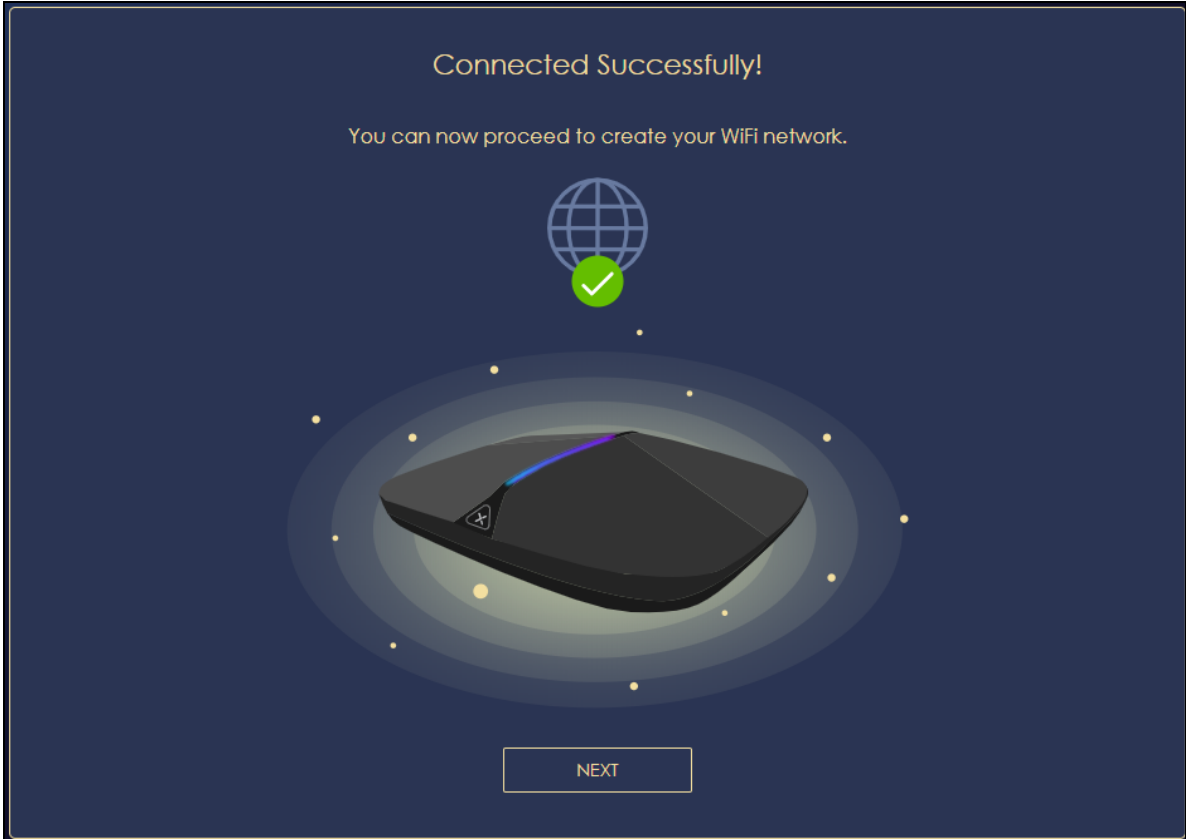
Launch your web browser and enter "http://zyxelwifi.com" or "http://zyxelwifi.net" as the website address.

Note: The wizard appears automatically when the NBG7815 is accessed for the first time or when you reset the NBG7815 to its default factory settings.

- 1 Your NBG7815 will check the status of your Internet connection the first time you log in.

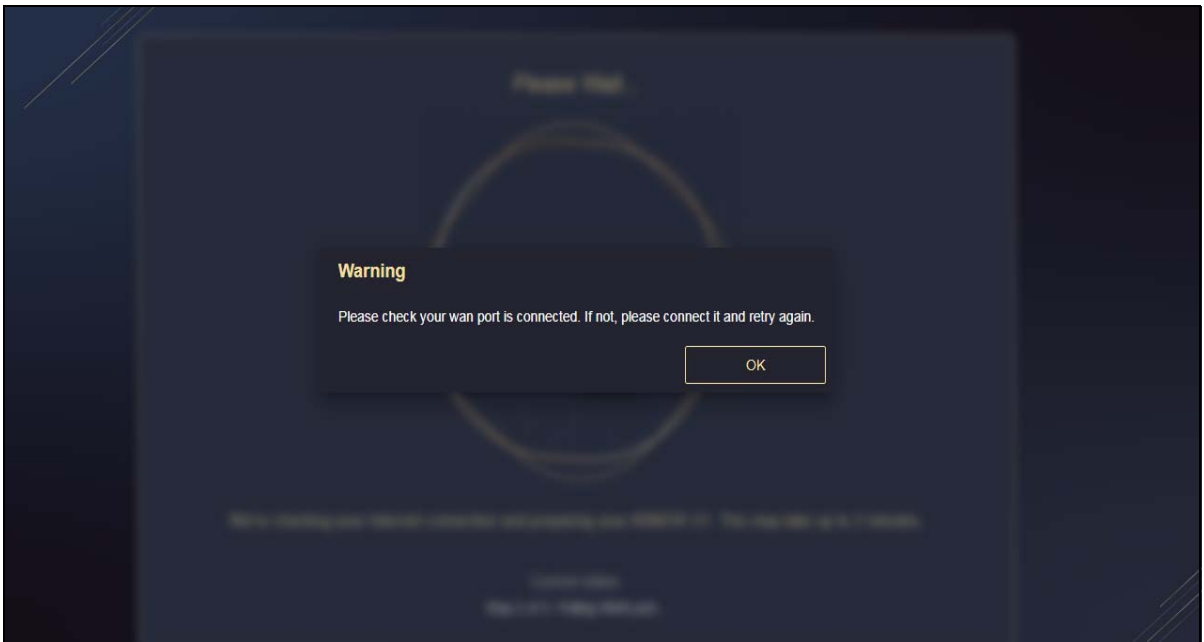


- 2 The following screen shows if you are connected to the Internet. Click **NEXT** to go to the next step in the wizard.



The following screen shows if you are not connected to the Internet.

Note: You may need to turn off your network firewall if access to the Internet from the NBG7815 is blocked. You need to connect to the Internet to access your NBG7815. See [Section 14.4 on page 151](#) if you cannot connect to the Internet.



- 3 Enter 1 – 128 single-byte printable ASCII characters but not ""<>^\$& as your **2.4G/5G WiFi Name** and **WiFi Password**. Select the check box **Keep 2.4G & 5G name the same** if you want to use the same name for your 2.4G and 5G WiFi.

Name Your WiFi

Create a WiFi name that you're going to use for your network.

2.4G WiFi Name

alice

5G WiFi Name

alice

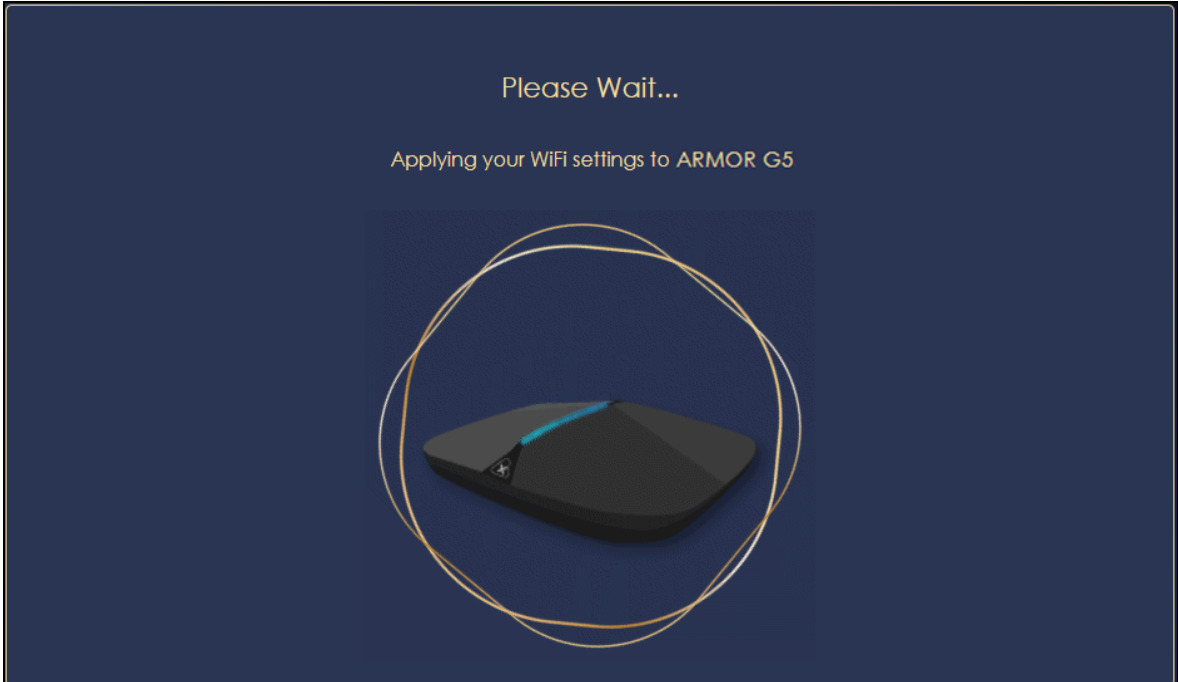
WiFi Password

•••••••

Keep 2.4G & 5G name the same

NEXT

- 4 Wait a moment for your WiFi settings to be applied to your NBG7815.



- 5 The following screen shows if you have set up your WiFi name and password successfully. Click **NEXT** to go to the next step in the wizard.



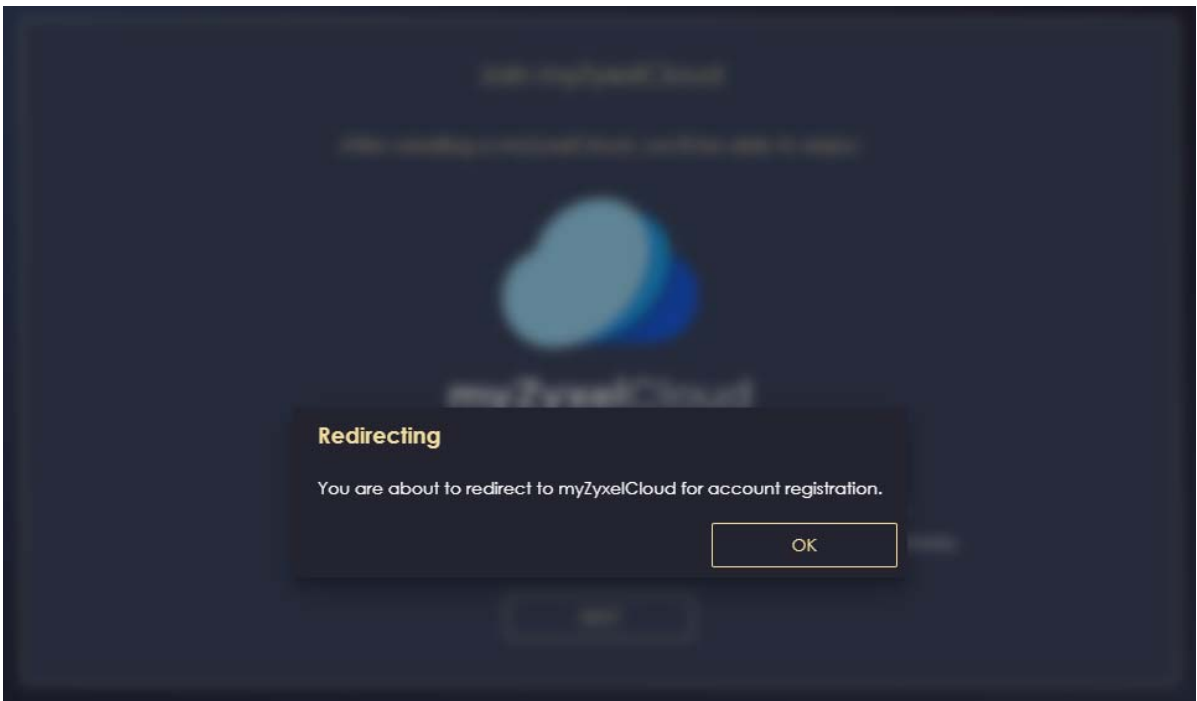
- 6 Wait a moment for the NBG7815 to check if your device is updated with the latest firmware. If not, your NBG7815 will automatically update the firmware.



- 7 You need to create a myZyxeCloud account to log into the NBG7815. The Zyxel cloud service gives you an online management site to configure and view the status of your NBG7815. Click **NEXT** to go to the next step in the wizard.



- 8 A pop-up message shows. Click **OK** to be redirected to the registration website of myZyxeCloud.



- 9 Enter your **Email** and **Password** if you already have a myZyxeCloud account. If not, you can create one by clicking **Sign Up**. You can also click the Facebook or Google icon to create an account with your Facebook or Google account.

Log in with
myZyxeCloud account

Email

Password

Remember me

You need to sign in or sign up before continuing.

SIGN IN

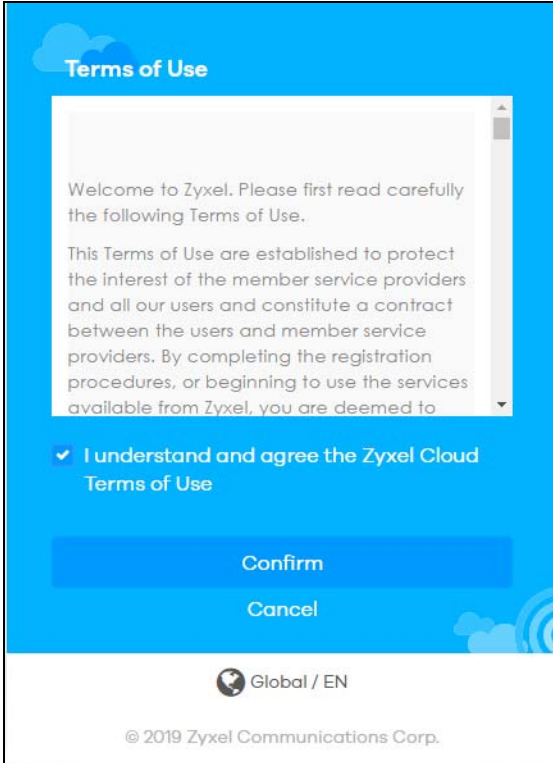
or

[Sign Up](#) / [Forgot Password](#) / [Help](#)

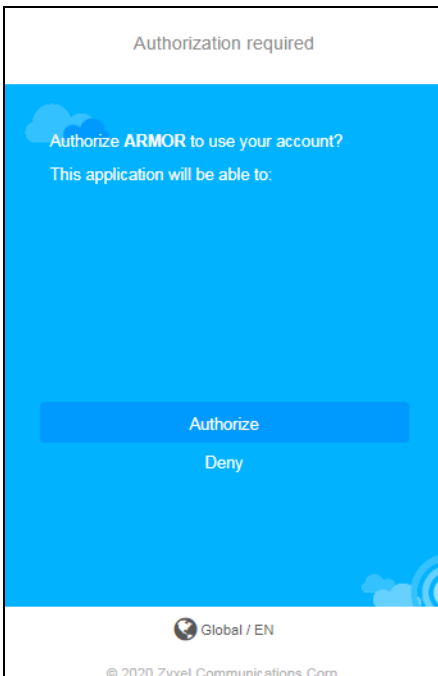
Global / EN

© 2019 Zyxel Communications Corp.

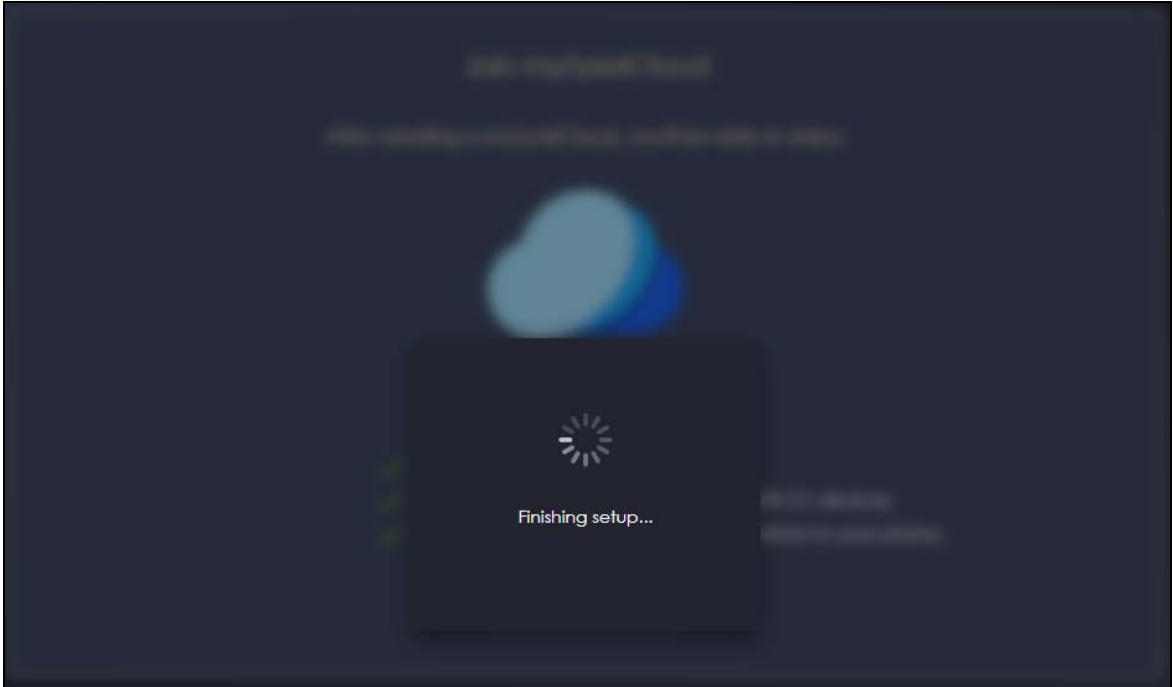
- 10 The legal page shows after you log in. Select the check box **I understand and agree the Zyxel Cloud Terms of Use** and then click **Confirm**.



- 11 The following page asks for your authorization to use your account. Click **Authorize** to finish registering your myZyxelCloud account. You will be directed back to the NBG7815 Web Configurator.



- 12 Wait a moment for your NBG7815 to link to your myZyxelCloud account.



- 13 You can create a local password to access the NBG7815 directly. You can choose to log in with your myZyxecloud account or your local password the next time you log in.

Note: You can change your local password in **System > General Settings**. See [Section 13.4 on page 141](#) for more information.

A screenshot of a dark blue web interface for setting a device login password. The title is "Device Login password" in orange. Below it, the text "Please create your local password for device login" is displayed. There are two input fields: "Password" and "Confirm Password", both with black backgrounds and white text. To the right of each field is a small white eye icon. At the bottom center, there is a white button with the text "APPLY" in black.

CHAPTER 4

Tutorials


4.1 Tutorials Overview

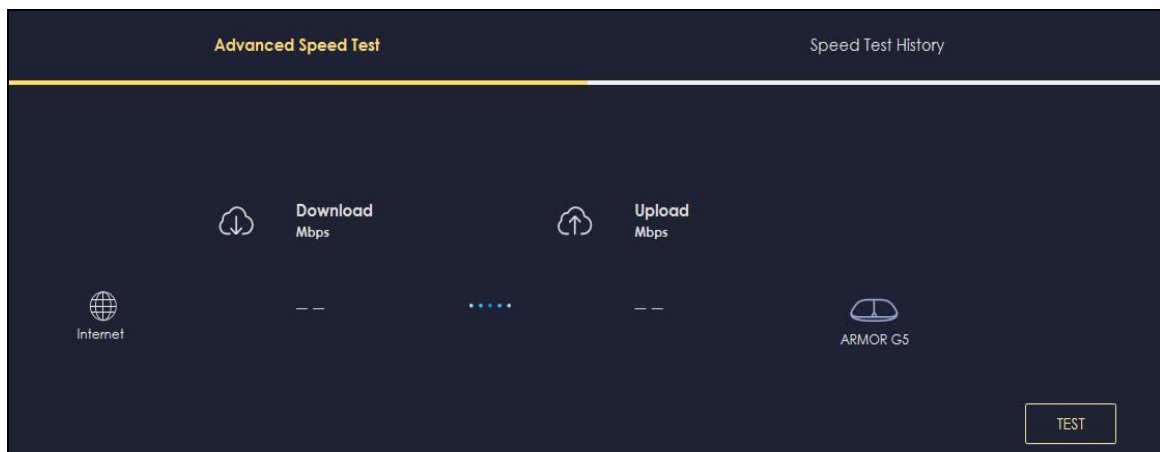
This chapter provides tutorials for setting up your NBG7815.

- [Run a Speed Test](#)
- [Configure the NBG7815's WiFi Networks](#)
- [Enable or Disable a Guest WiFi Network](#)
- [Add Clients to a Profile](#)
- [Configure a Profile's WiFi Schedule](#)
- [Pause or Resume Internet Access on a Profile](#)
- [Turn on or off the NBG7815's LED \(Light\)](#)
- [Change Your NBG7815 Operating Mode](#)
- [Configure a Port Forwarding Rule](#)
- [Configure NBG7815 as an OpenVPN Server](#)
- [Configure NBG7815 as an OpenVPN Client](#)

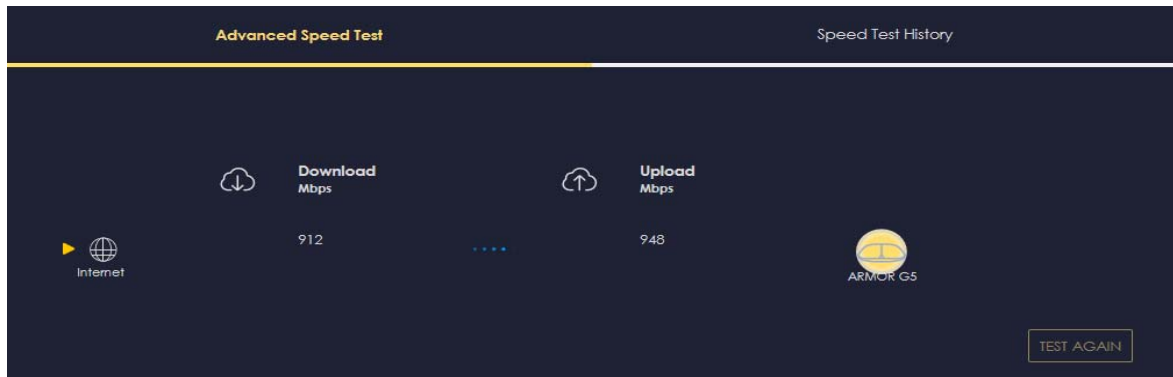
4.2 Run a Speed Test

With the NBG7815 Web Configurator, you can check the speed of the connection between your NBG7815 and the broadband modem/router.

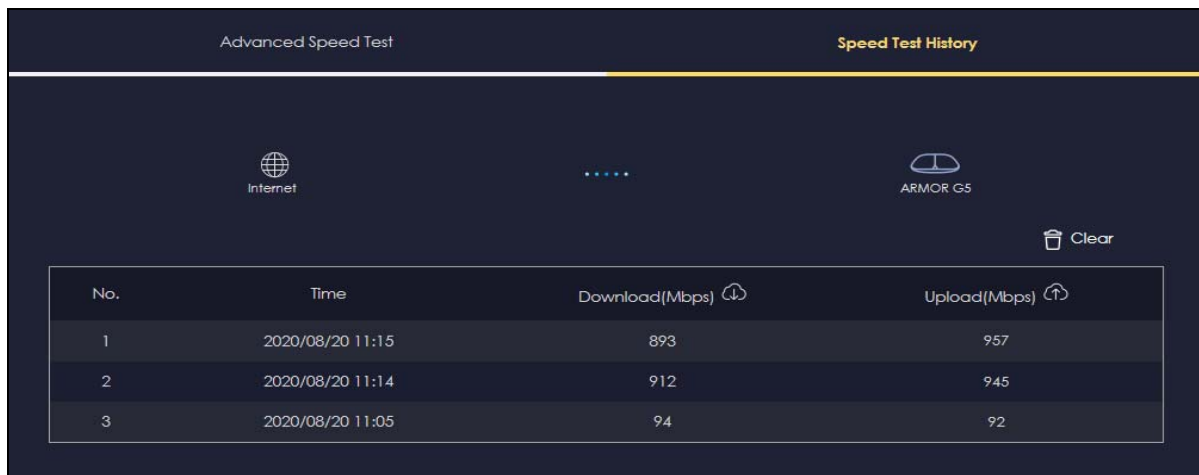
- 1 Click the **Navigation Panel** icon on the top-left corner () and click **Diagnose** to open the **Advanced Speed Test** screen. Use this screen to view all the available connections in your NBG7815 system.



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



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




4.3 Configure the NBG7815's WiFi Networks

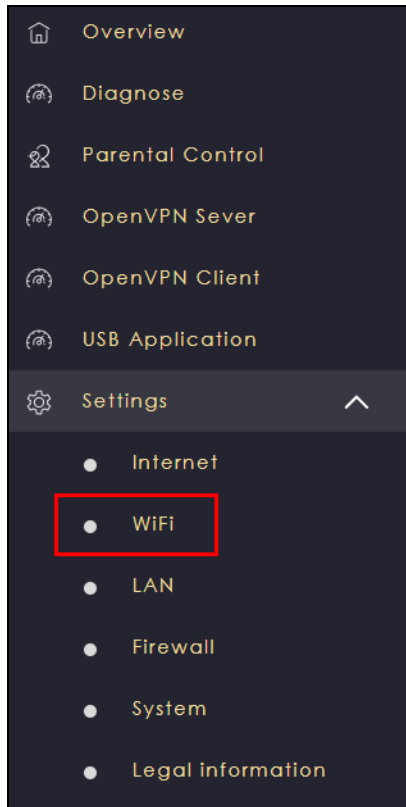
In the NBG7815 you can configure independent WiFi networks with different privileges. Clients can associate only with the network for which they have security settings (SSID and password). The following table describes the different NBG7815's profile networks and their privileges.

Table 6 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

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

- 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 (SSID)** 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. Select the WiFi security mode, bandwidth, and channel for the 2.4 GHz and 5 GHz networks. Click **APPLY** to save your changes.

Main WiFi

Enable Main WiFi Enable Disable

Name(SSID)

Keep 2.4G & 5G name the same

Security Mode WPA2-PSK WPA3-PSK WPA3-PSK Mix

Password

Region

2.4G Bandwidth

2.4G Channel Channel : 9

5G Bandwidth

5G Channel

Advanced Settings

2.4G WiFi

OBSS Enable Disable

MU-MIMO

Down Link Enable Disable

Up Link Enable Disable

OFDMA

Down Link Enable Disable

Up Link Enable Disable

5G WiFi

MU-MIMO

Down Link Enable Disable

Up Link Enable Disable

OFDMA

Down Link Enable Disable

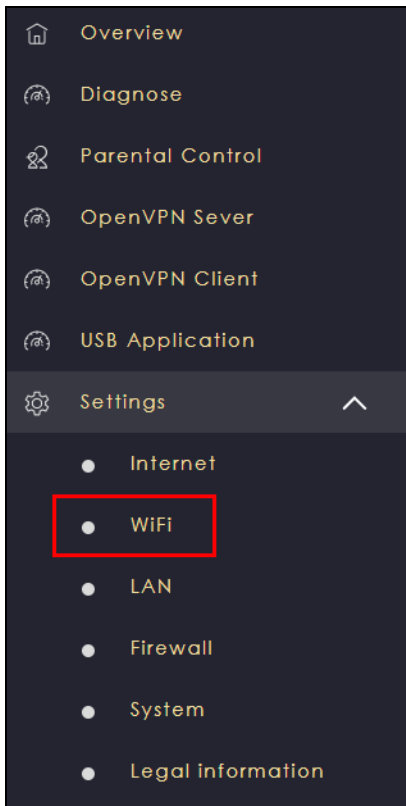
Up Link Enable Disable

4.4 Enable or Disable a Guest WiFi Network

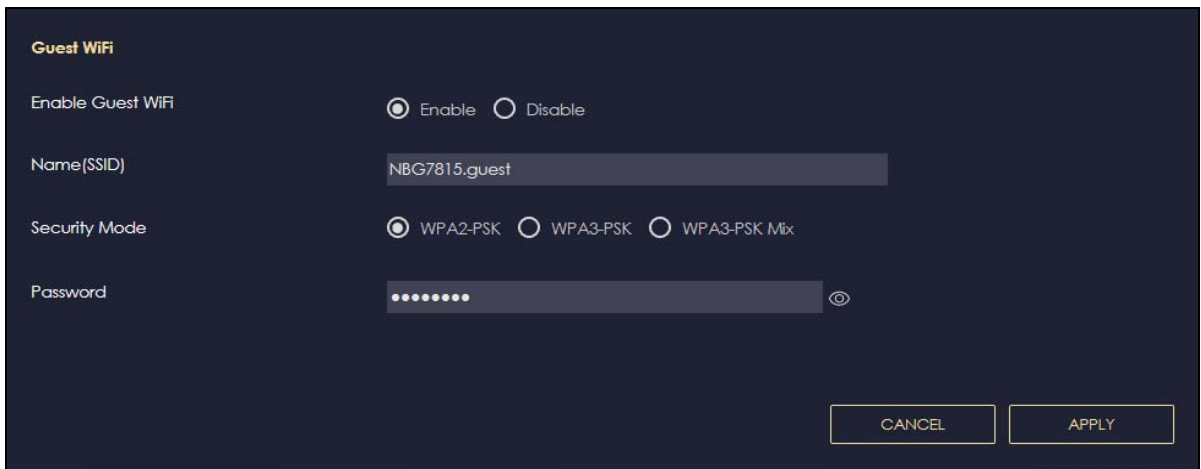
After the NBG7815 is set up, you can use separate WiFi networks for your clients. The WiFi settings will be applied to all clients in the same network.

Note: This is not available if you are using bridge mode.

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




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

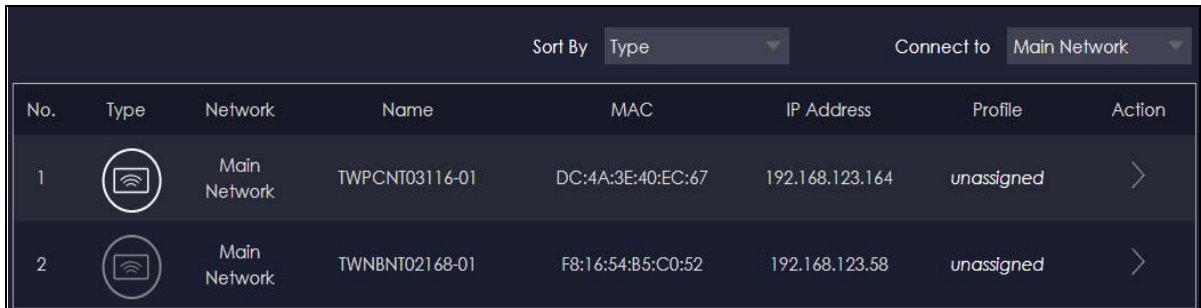






4.5 Add Clients to a Profile


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

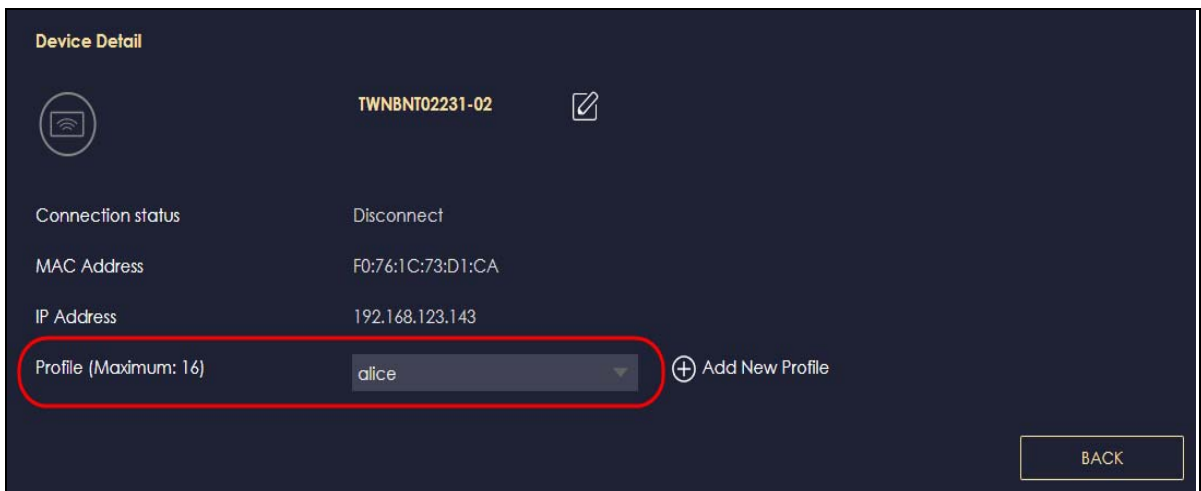
Note: This is not available if you are using bridge mode.

- 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 clients connected to your NBG7815.





No.	Type	Network	Name	MAC	IP Address	Profile	Action
1		Main Network	TWPCNT03116-01	DC:4A:3E:40:EC:67	192.168.123.164	unassigned	
2		Main Network	TWNBNT02168-01	F8:16:54:B5:C0:52	192.168.123.58	unassigned	

- 2 Click the icon under **Action** () to view the user information. In **Device Detail**, select a predefined profile and click **BACK**.




Device Detail

 **TWNBNT02231-02** 

Connection status: Disconnect

MAC Address: F0:76:1C:73:D1:CA

IP Address: 192.168.123.143


Profile (Maximum: 16):  Add New Profile

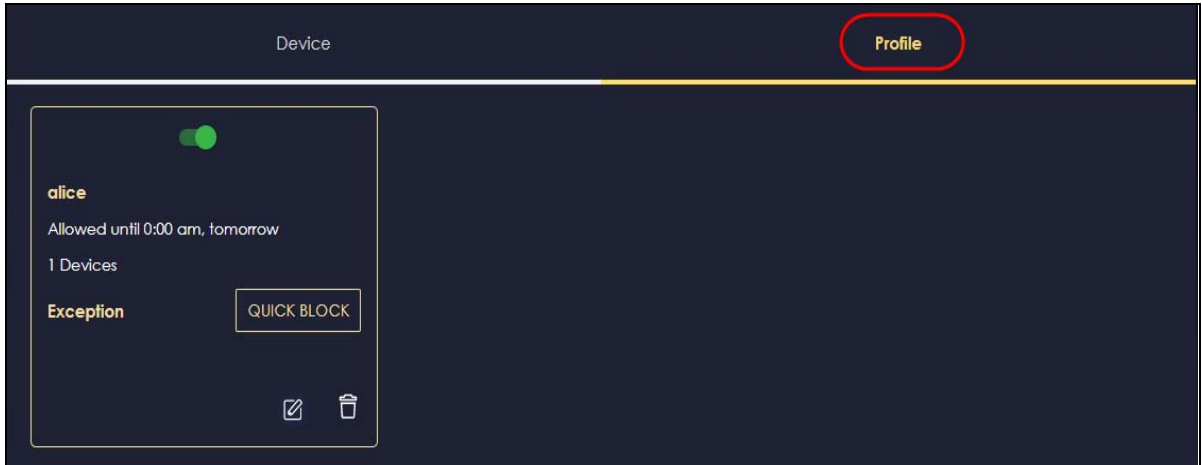
BACK

4.6 Configure a Profile's WiFi Schedule

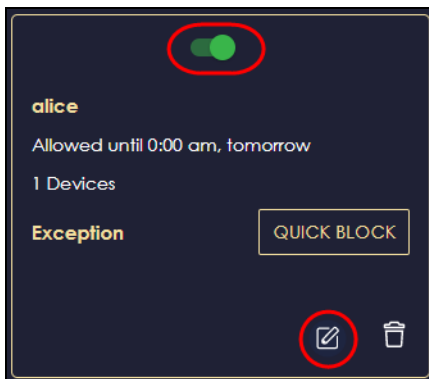
When you create or edit a profile, you can schedule the NBG7815 to automatically disable or enable WiFi access during a certain period of time for clients in that profile.

Note: This is not available if you are using bridge mode.

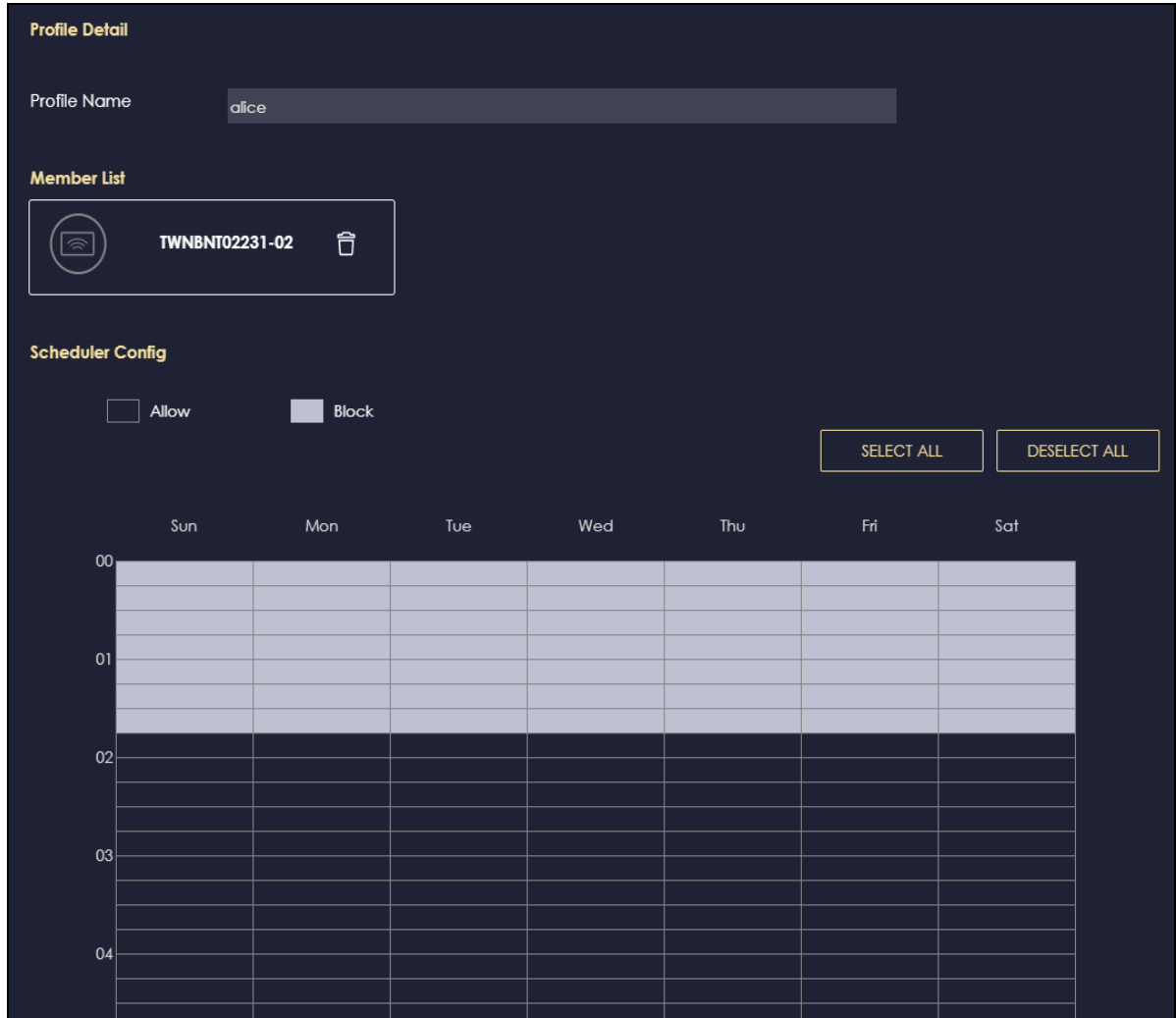
- 1 Click the **Navigation Panel** icon on the top-left corner () and click **Parental Control**, and click the **Profile** tab. Use the **Profile** screen to display the profiles created in the NBG7815.



- 2 Click the switch to activate the profile's Internet schedule. Click the **Edit** icon (✎) to modify a profile's Internet schedule.




- 3 Click the start time cell and drag down to the end time to set up your schedule.

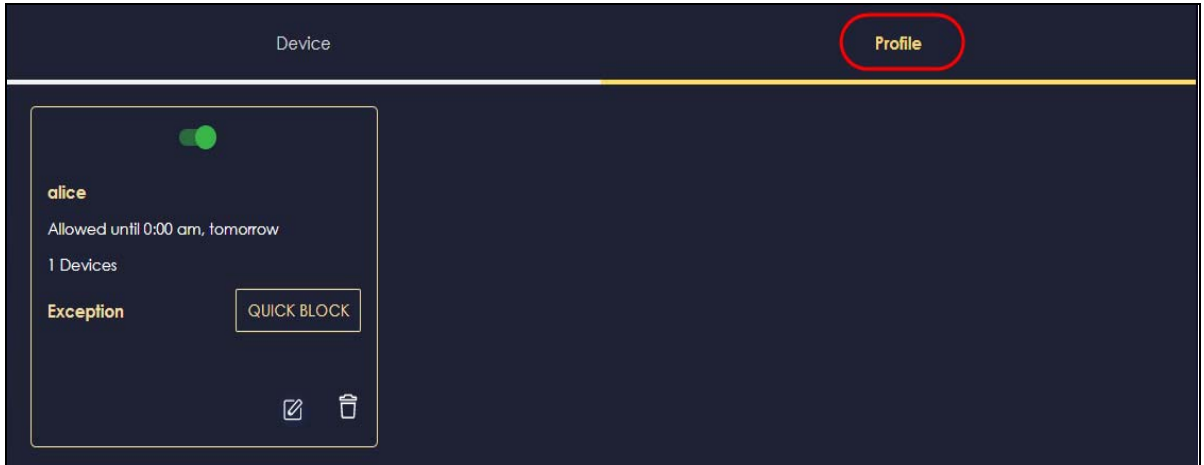


4.7 Pause or Resume Internet Access on a Profile

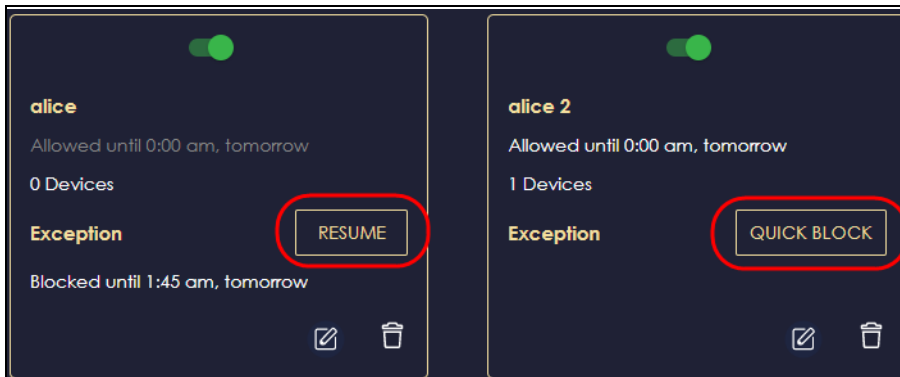
You may want to manually block client devices from accessing the Internet immediately and resume it later.

Note: This is not available if you are using bridge mode.

- 1 Click the **Navigation Panel** icon on the top-left corner () . Select **Parental Control**, and click the **Profile** tab. Use the **Profile** screen to display the profiles created in the NBG7815.

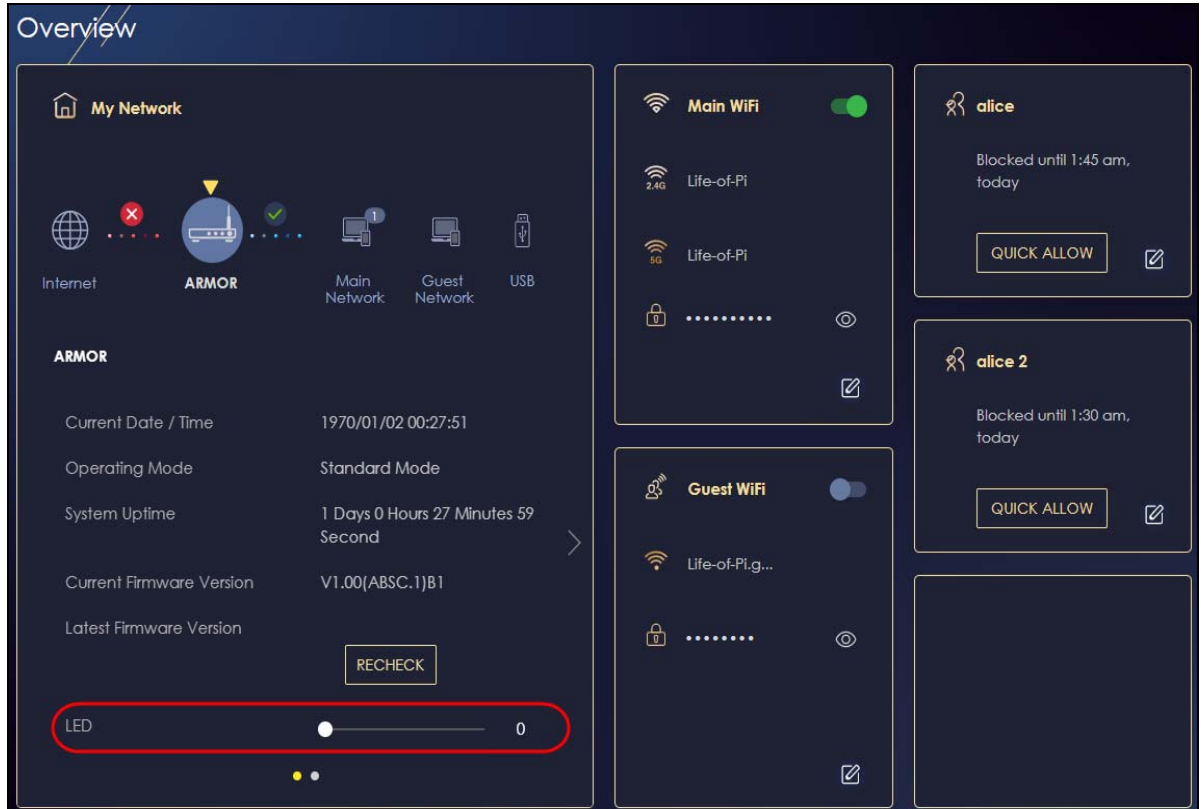


- 2 Click a profile's **RESUME** button to resume network access at once, or click the **QUICK BLOCK** button to pause Internet access for that specific profile.



4.8 Turn on or off the NBG7815's LED (Light)

In the **Overview** screen, find the **LED** field and drag the button of the slider to increase the brightness or turn off the NBG7815's LED.



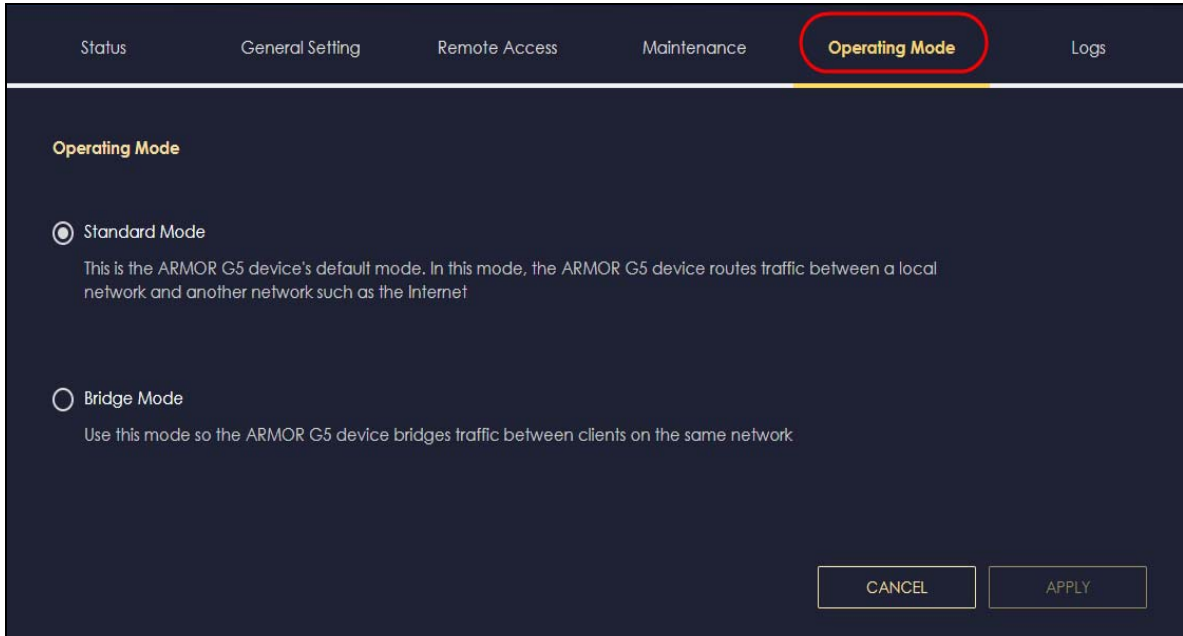
4.9 Change Your NBG7815 Operating Mode

The operating mode refers to how the NBG7815 is being used in the network. The NBG7815 has the following operating modes:

- **Standard:** This is the NBG7815's default mode. In this mode, the NBG7815 routes traffic between a local network and another network such as the Internet.
- **Bridge:** Use this mode so the NBG7815 bridges traffic between clients on the same network.

Note: Features such as parental control, UPnP, port forwarding are not available in bridge mode.


- 1 Click the **Navigation Panel** icon on the top-left corner (☰).
- 2 From the **Settings** drop-down list, click **System**, then click the **Operating Mode** tab.
- 3 Select the operating mode and select **APPLY** to save your changes. Changing the NBG7815's operating mode may take up to 2 minutes.



4.10 Configure a Port Forwarding Rule

If you want to forward incoming packets to a computer on the LAN using ports, create a port forwarding rule.

Note: This is not available if you are using bridge mode.

- 1 Click the **Navigation Panel** icon on the top-left corner (). From the **Settings** drop-down list, select **Internet**, and click the **NAT & Port Forwarding** tab.

Internet Connection **NAT & Port Forwarding** Passthrough Port Trigger Dynamic DNS UPnP

NAT & Port Forwarding

Network Address Translation (NAT) Enable Disable

Server Setup Default Server - 192.168.123.1
 Change to Server
TWNBNT02231-02

Port Forwarding Rule (The maximum number of rules is 32.)

Enable Port Forwarding Enable Disable + Add Rule

No.	Name	Protocol	External Port	Server IP Address	Internal Port	Actions
-----	------	----------	---------------	-------------------	---------------	---------

CANCEL APPLY

- 2 Select **Enable** in the **Enable Port Forwarding** field.

Port Forwarding Rule (The maximum number of rules is 32.)

Enable Port Forwarding Enable Disable

- 3 Click **Add Rule** to create a port forwarding rule. Add a service name, a port number or a range of ports to define the service to be forwarded, specify the transport layer protocol used for the service, and the IP address of a computer on your LAN that will receive the packets from the ports.

Add Port Forwarding Rule

Service Name: User-Define

Protocol: TCP/UDP

External Port: Ex: 10 or 10-20

Device List: TWNBNT02231-02 (192.168.123.143)

Internal Port: Ex: 1-65535

CANCEL APPLY

4.11 Configure NBG7815 as an OpenVPN Server

Create an OpenVPN server account to allow the NBG7815 to transmit data to client devices through a secure VPN channel.

Note: This is NOT available if you are using bridge mode.

- 1 Enable DDNS (Dynamic DNS) in **Settings > Internet > Dynamic DNS**. Click **APPLY**.

Dynamic DNS

Dynamic DNS Enable Disable


Service Provider

Host Name .zyxel.me

User Name

Password

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, Dynamic DNS (DDNS) maps a domain name to a dynamic IP address. With DDNS, you can use a domain name to access your ZyxEL device and home network regardless of the device's current (dynamic) IP address. The ZyxEL device must have a public WAN IP address to use Dynamic DNS.

- Click the **Navigation Panel** icon on the top-left corner (). Select **OpenVPN Server**, and click the **OpenVPN Server** tab. Configure the OpenVPN Server account.

OpenVPN Server

Dynamic DNS Enable

Host Name

Configuration

Status Enable Disable

Protocol TCP UDP

Server Port

VPN Subnet / Netmask /

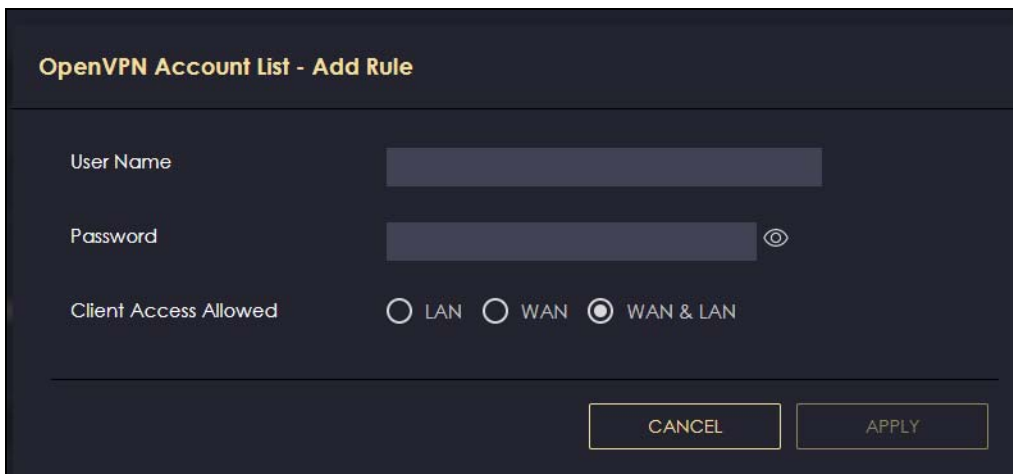
Advertise DNS to Clients Enable Disable

Key Setting

- Click the **OpenVPN Account** tab.



- 4 Click **Add Rule** to create up to 5 OpenVPN account rules. Add a user name, set the password, and select the interfaces through which the clients are allowed to connect to the account.

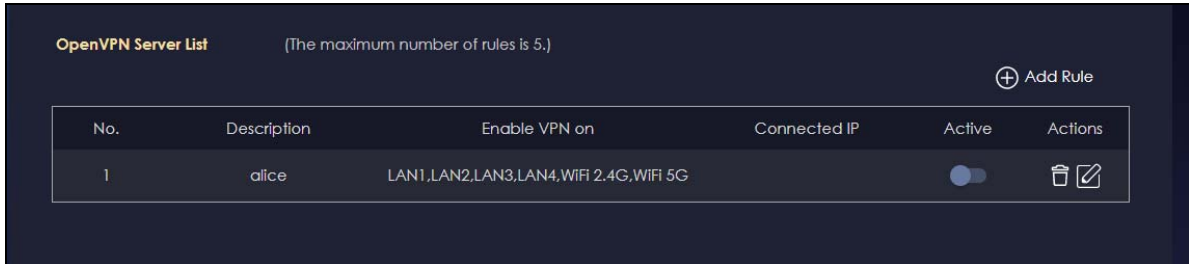


4.12 Configure NBG7815 as an OpenVPN Client

Use OpenVPN Client to allow a VPN server to transmit data through a secure VPN channel to the NBG7815 client device.

Note: Do NOT activate OpenVPN Server and OpenVPN Client at the same time. The NBG7815 can only connect to one server at a time.

- 1 Click the **Navigation Panel** icon on the top-left corner () . Select **OpenVPN Client**.



- 2 Click **Add Rule** to create up to 5 OpenVPN account rules. Add a description, user name and password of the OpenVPN Server, import an `.ovpn` file that you get from the OpenVPN Server that you want to connect to, and select the interfaces that are allowed by the OpenVPN Server account.

The screenshot shows the 'OpenVPN Server List - Add Rule' form. It has the following fields and options:

- Description:
- User Name:
- Password:
- Import `.ovpn` file: No file chosen
- Enable VPN on: All
- LAN1 LAN2 LAN3 LAN4
- WiFi 2.4G WiFi 5G

At the bottom, there are two buttons: and .

CHAPTER 5

Web Configurator

5.1 Web Configurator Overview

This chapter describes how to access the NBG7815 Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy system setup and management through Internet browser. Use a browser that supports HTML5, such as Microsoft Edge, Internet Explorer 11, Mozilla Firefox, or Google Chrome. The minimum 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 computer
- JavaScript (enabled by default)
- Java permissions (enabled by default).

5.2 Accessing the Web Configurator

- 1 Make sure your NBG7815 hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 If the NBG7815 is in **Standard Mode** (the default mode), enter "http://zyxelwifi.com" in the browser's address bar.

To see the standard mode features, go to [Table 7 on page 54](#).

If the NBG7815 is in **Bridge Mode**, enter "http://" (DHCP-assigned IP)" in the browser's address bar.

To see the bridge mode features, go to [Table 8 on page 56](#).

- 4 On the displayed login screen, log in using your myZyxelCloud user name and password or the local password.

Note: If this is the first time you are accessing the Web Configurator or if the device has been reset, you must complete the setup wizard, see [Chapter 3 on page 25](#).

Note: For setting and changing the local password, see [Section 13.4 on page 141](#).

Figure 17 LOG IN



- 5 The NBG7815 **Overview** screen displays allowing you to monitor your NBG7815. It shows if the NBG7815 is online, and how many WiFi clients are currently connected to your NBG7815, as well as their upstream/downstream data rates.

Figure 18 Overview (Standard Mode)

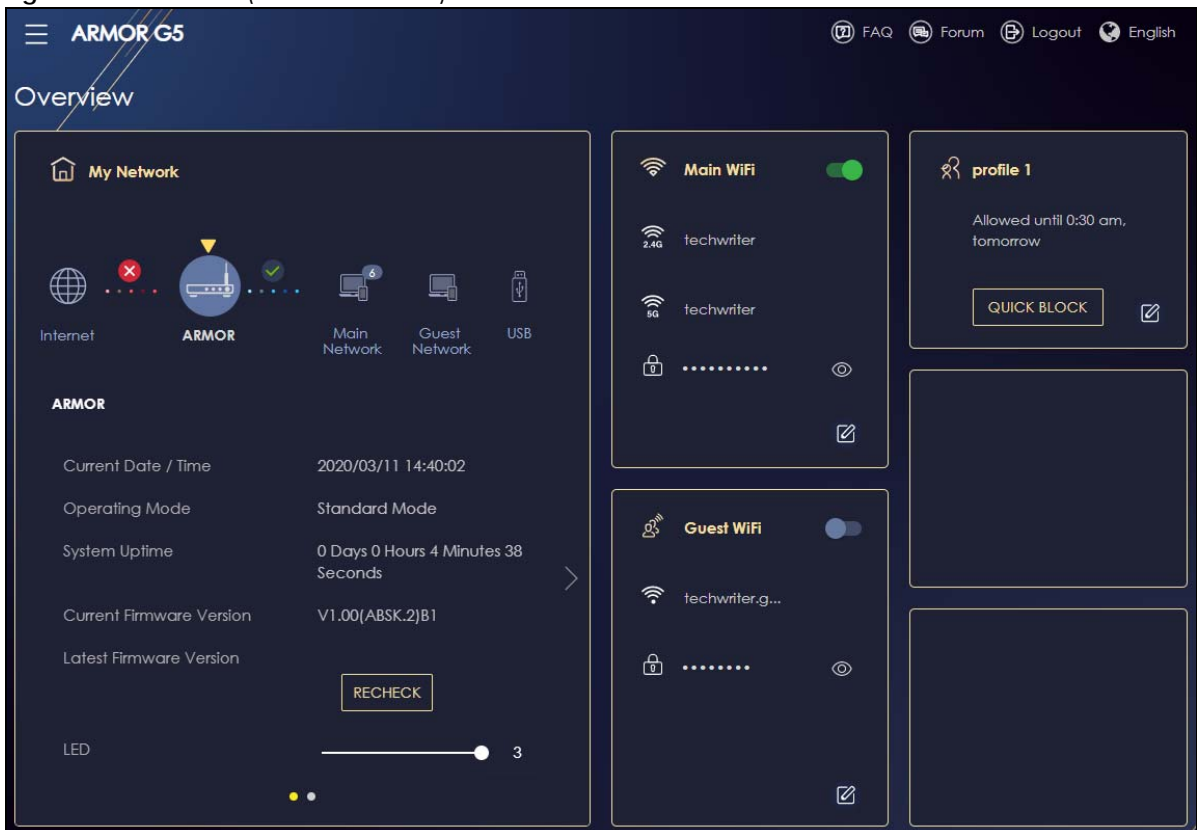
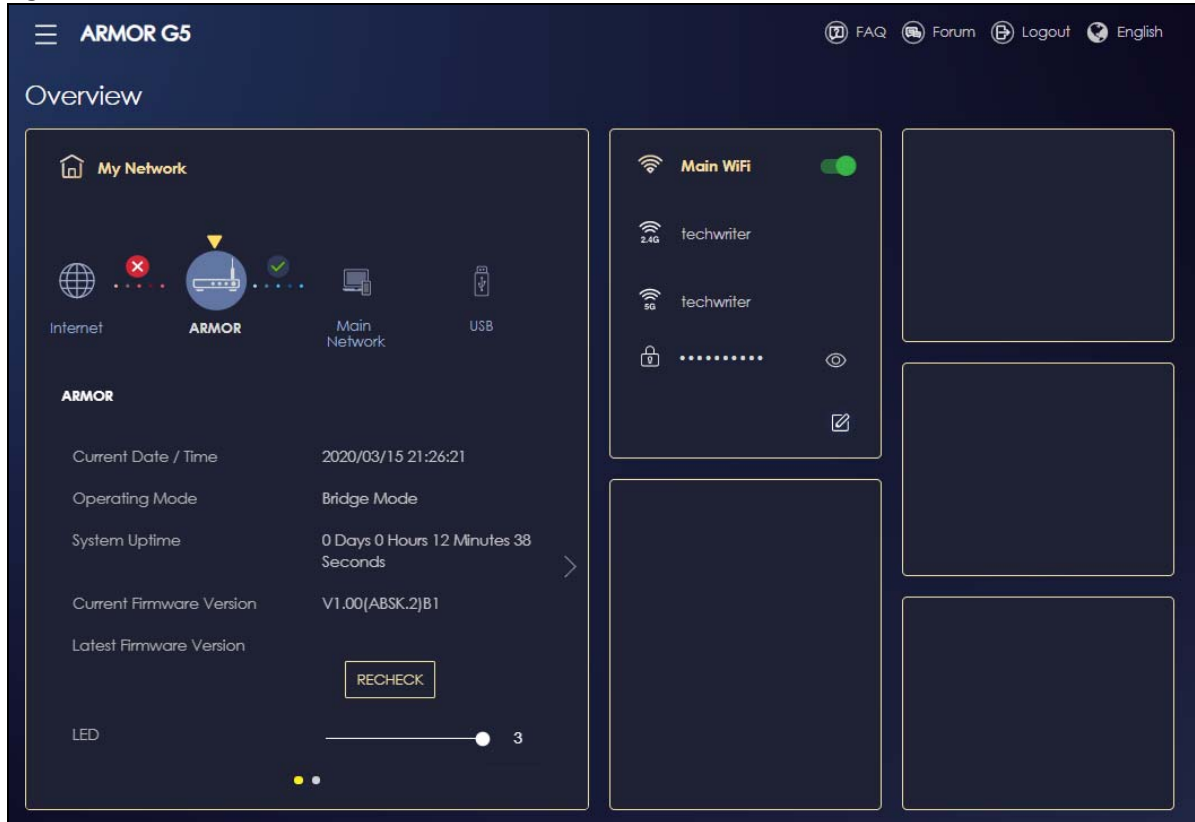


Figure 19 Overview (Bridge Mode)

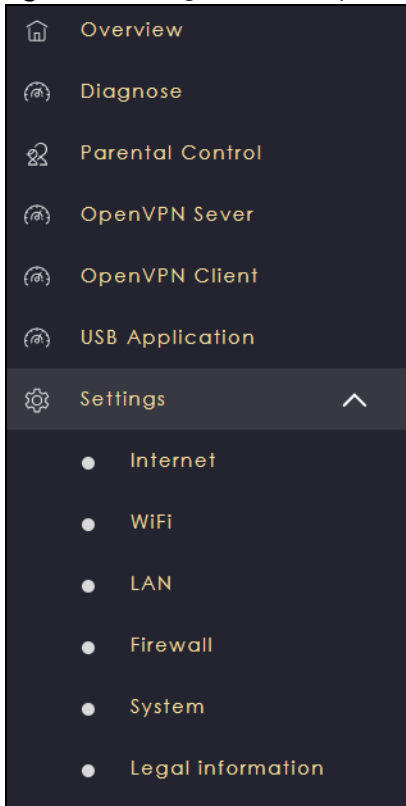


5.3 Navigation Panel

Use the sub-menus on the navigation panel to configure NBG7815 features. Your navigation panel varies depending on the operating mode of your NBG7815. See [Section 1.3 on page 17](#) for more information on standard (router) mode and bridge mode.

5.3.1 Standard Mode Navigation Panel

Figure 20 Navigation Panel (Standard Mode)



The following table describes the sub-menus.

Table 7 Navigation Panel (Standard Mode)

LINK	TAB	FUNCTION
Overview		Use this screen to: <ul style="list-style-type: none"> View read-only information about your NBG7815 Configure WiFi settings Change the brightness of your NBG7815's LED
Diagnose	Advanced Speed Test	Use this screen to check the speed of the connection between your NBG7815 and the broadband modem/router.
	Speed Test History	Use this screen to view a summary of previous speed tests.
Parental Control	Device	Use this screen to: <ul style="list-style-type: none"> View devices information Add and configure parental control rules or schedules
	Profile	Use this screen to enable or configure existing parental control rules.
OpenVPN Server	OpenVPN Server	Use this screen to create and configure an OpenVPN server account.
	OpenVPN Account	Use this screen to: <ul style="list-style-type: none"> View basic information about NBG7815 OpenVPN server View basic information about clients that are connected to the NBG7815 OpenVPN server

Table 7 Navigation Panel (Standard Mode) (continued)

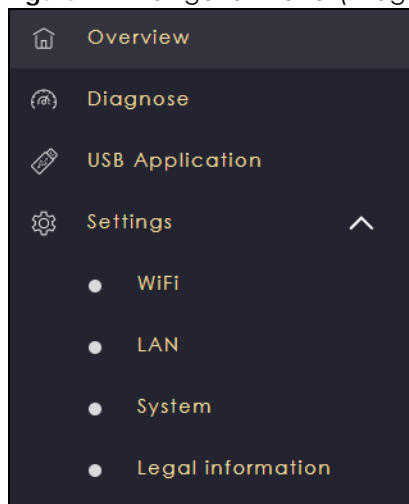
LINK	TAB	FUNCTION
OpenVPN Client		Use this screen to: <ul style="list-style-type: none"> View basic information about OpenVPN Server accounts that you are connected to Add an OpenVPN Server Account you want your NBG7815 to connect to when the NBG7815 functions as an OpenVPN client
USB Application	SAMBA	Use this screen to: <ul style="list-style-type: none"> Set up file-sharing through the NBG7815 using File Explorer or the workgroup name Configure the workgroup name and create file-sharing user accounts
	FTP	Use this screen to set up file sharing through the NBG7815 using FTP and create user accounts.
	USB Media Sharing	Use this screen to configure settings for media sharing.
Internet	Internet Connection	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address.
	NAT & Port Forwarding	Use this screen to enable NAT. Use this screen to configure servers behind the NBG7815 and forward incoming service requests to the servers on your local network.
	Passthrough	Use this screen to change your NBG7815's port triggering settings.
	Port Trigger	Use this screen to configure ALGs (Application Layer Gateway) and VPN pass-through settings.
	Dynamic DNS	Use this screen to configure dynamic DNS.
	UPnP	Use this screen to enable UPnP on the NBG7815.
WiFi	Main WiFi	Use this screen to enable WiFi and configure WiFi and WiFi security settings.
	Guest WiFi	Use this screen to configure multiple BSSs on the NBG7815.
	MAC Filter	Use the MAC filter screen to configure the NBG7815 to block access to devices or block the devices from accessing the NBG7815.
	WPS	Use this screen to configure WPS.
	Scheduling	Use this screen to schedule the times WiFi is enabled.
LAN	LAN IP	Use this screen to configure the NBG7815's LAN IP address and subnet mask. Use this screen to enable the NBG7815's DHCP server.
	IPv6 LAN	Use this screen to configure the IPv6 address for your NBG7815 on the LAN.
Firewall	IPv4 Firewall	Use this screen to configure IPv4 firewall rules.
	IPv6 Firewall	Use this screen to configure IPv6 firewall rules.

Table 7 Navigation Panel (Standard Mode) (continued)

LINK	TAB	FUNCTION
System	Status	Use this screen to view the basic information of the NBG7815.
	General Setting	Use this screen to change password or to set the timeout period of the management session.
	Remote Access	Use this screen to configure the interfaces from which the NBG7815 can be managed remotely and specify a secure client that can manage the NBG7815.
	Maintenance	Use this screen to upload firmware, reboot the NBG7815 without turning the power off or reset the NBG7815 to factory default.
	Operating Mode	Use this screen to select whether your NBG7815 acts as a router, or a bridge.
	Logs	Use this screen to view the list of activities recorded by your NBG7815.
Legal Information	Legal Information	Use this screen to view the legal and regulatory information of the NBG7815.

5.3.2 Bridge Mode Navigation Panel

Figure 21 Navigation Panel (Bridge Mode)



The following table describes the sub-menus.

Table 8 Navigation Panel (Bridge Mode)

LINK	TAB	FUNCTION
Overview		Use this screen to: <ul style="list-style-type: none"> View read-only information about your NBG7815 Configure WiFi settings Change the brightness of your NBG7815's LED
Diagnose	Advanced Speed Test	Use this screen to check the speed of the connection between your NBG7815 and the broadband modem/router.
	Speed Test History	Use this screen to view a summary of previous speed tests.

Table 8 Navigation Panel (Bridge Mode) (continued)

LINK	TAB	FUNCTION
USB Application	SAMBA	Use this screen to <ul style="list-style-type: none"> • Set up file-sharing through the NBG7815 using File Explorer or the workgroup name • Configure the workgroup name and create file-sharing user accounts
	FTP	Use this screen to set up file sharing through the NBG7815 using FTP and create user accounts.
	USB Media Sharing	Use this screen to configure settings for media sharing.
WiFi	Main WiFi	Use this screen to enable WiFi and configure WiFi and WiFi security settings.
	MAC Filter	Use the MAC filter screen to configure the NBG7815 to block access to client devices or block the client devices from accessing the NBG7815.
	WPS	Use this screen to configure WPS.
	Scheduling	Use this screen to schedule the times WiFi is enabled.
LAN	LAN IP	Use this screen to configure the NBG7815's LAN IP address and subnet mask.
		Use this screen to configure the IPv6 address for the NBG7815 on the LAN.
		Use this screen to enable the NBG7815's DHCP server.
System	Status	Use this screen to view the basic information of the NBG7815.
	General Setting	Use this screen to change password or to set the timeout period of the management session.
	Maintenance	Use this screen to upload firmware, reboot the NBG7815 without turning the power off or reset the NBG7815 to factory default.
	Operating Mode	Use this screen to select whether your NBG7815 acts as a router, or a bridge.
	Logs	Use this screen to view the list of activities recorded by your NBG7815.
Legal Information	Legal Information	Use this screen to view the legal and regulatory information of the NBG7815.

CHAPTER 6

Standard Mode Status

6.1 Standard Mode Overview

Use the **Status** screen to view read-only information about your NBG7815 in standard (router) mode.

6.2 Standard Mode Status

Click **Settings > System > Status** to open the status screen.

Figure 22 Settings > System > Status (Standard Mode)

System	
Model Name	NBG7815
Firmware Version	V1.00(ABSK.2)B1
System Operation Mode	Standard Mode
Enable IPv4 Firewall	Enable
Enable IPv6 Simple Security	Enable
System Uptime	0 Days 0 Hours 24 Minutes 45 Seconds
WAN Information	
MAC Address	BC:CF:4F:B7:53:61
IP Address	
IP Subnet Mask	
Gateway	
IPv6 Address	
LAN Information	
MAC Address	BC:CF:4F:B7:53:60
IP Address	10.0.0.1
IP Subnet Mask	255.255.255.0
DHCP Server	Enable
IPv6 Address	

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

Table 9 Settings > System > Status (Standard Mode)

LABEL	DESCRIPTION
System	
Model Name	This is the model name of your NBG7815.
Firmware Version	This is the firmware version.
System Operation Mode	This is the device mode to which the NBG7815 is set, see Section 13.7 on page 145 for more information.
Enable IPv4 Firewall	This shows if the IPv4 firewall is enabled on the NBG7815.
Enable IPv6 Simple Security	This shows if the IPv6 firewall is enabled on the NBG7815.
System Uptime	This is the total time the NBG7815 has been on.
WAN Information	
MAC Address	This shows the WAN Ethernet adapter MAC address of your NBG7815.

Table 9 Settings > System > Status (Standard Mode) (continued)

LABEL	DESCRIPTION
IP Address	This shows the WAN port's IP address.
IP Subnet Mask	This shows the WAN port's subnet mask.
Gateway	This shows the WAN port's gateway IP address.
IPv6 Address	This shows the current IPv6 address of the NBG7815.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC address of your NBG7815.
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 NBG7815 in the LAN.

CHAPTER 7

Bridge Mode Status

7.1 Bridge Mode Overview

Many screens that are available in **Standard Mode** are not available in **Bridge Mode**, such as port forwarding and firewall. See [Section 5.3 on page 53](#) for more information.

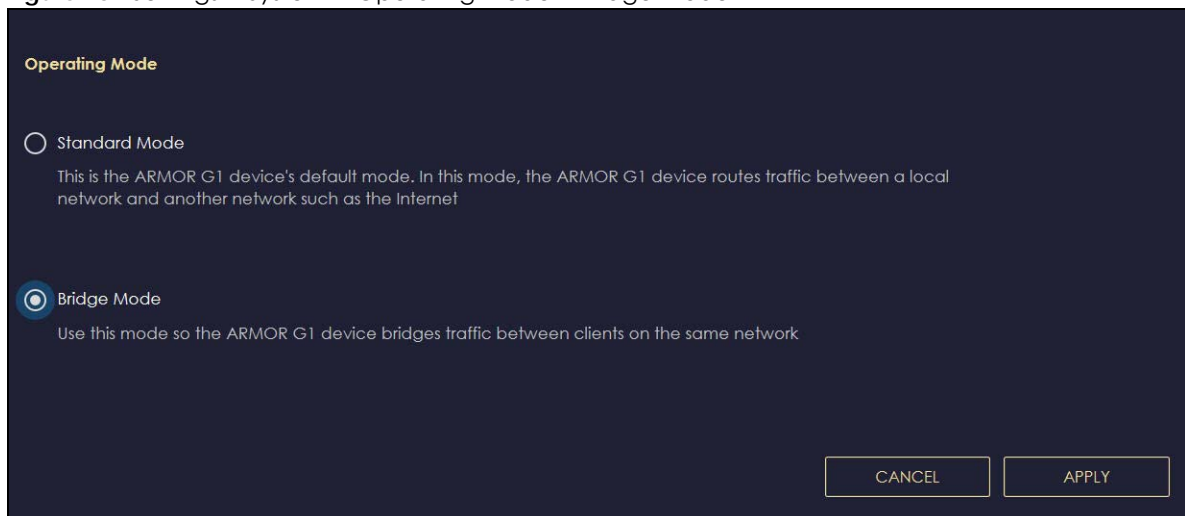
7.2 What You Can Do

- Set up a network with the NBG7815 as a bridge ([Section 7.3 on page 61](#)).
- Use the **Status** screen to view read-only information about your NBG7815 ([Section 7.4 on page 62](#)).

7.3 Setting your NBG7815 to Bridge Mode

- 1 Log into the Web Configurator if you have not already. See the Quick Start Guide for instructions on how to do this.
- 2 To use your NBG7815 as a bridge, go to **Settings > System > Operating Mode** and select **Bridge Mode**.

Figure 23 Settings > System > Operating Mode > Bridge Mode



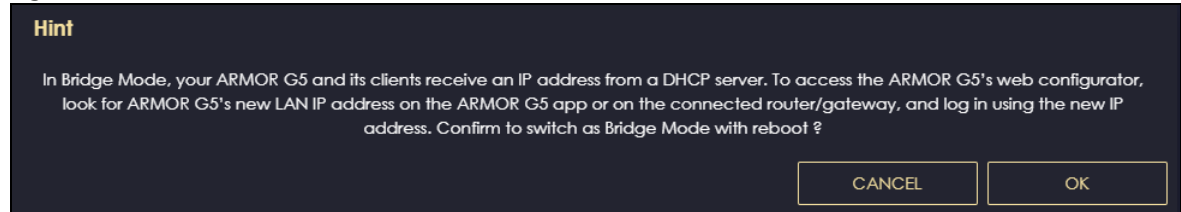
Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your NBG7815 is already in bridge mode.

Note: Choose your NBG7815 operating mode carefully to avoid having to change it later.

When changing to another mode, the IP address of the NBG7815 changes (192.168.123.1 in standard (router) mode to 192.168.123.2 in bridge mode and vice versa). The running applications and services of the network devices connected to the NBG7815 may be interrupted.

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

Figure 24 Pop-up for Bridge Mode



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

7.3.1 Accessing the Web Configurator in Bridge Mode

To log in to the Web Configurator in bridge mode, do the following:

- 1 Log into the Web Configurator. See the Quick Start Guide for instructions on how to do this.
- 2 Connect your computer to one of the LAN port of the NBG7815.
- 3 Connect a modem/router to the other LAN port of the NBG7815 using an Ethernet cable.
- 4 If the NBG7815 is not connected to a router or DHCP server, the NBG7815 cannot assign your computer an IP address.
- 5 After you have set your computer's IP address, open a web browser such as Google Chrome and enter "http://(DHCP-assigned IP)" as the web address in your web browser.

7.4 Bridge Mode Status

Click **Settings > System > Status** to open the status screen.

Figure 25 Settings > System > Status (Bridge Mode)

System	
Model Name	NBG7815
Firmware Version	V1.00(ABSK.2)B1
System Operation Mode	Bridge Mode
Enable IPv4 Firewall	Enable
Enable IPv6 Simple Security	Enable
System Uptime	0 Days 0 Hours 19 Minutes 20 Seconds
LAN Information	
MAC Address	BC:CF:4F:87:53:60
IP Address	192.168.1.34
IP Subnet Mask	255.255.255.0
DHCP Server	Enable
IPv6 Address	

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

Table 10 Settings > System > Status (Bridge Mode)

LABEL	DESCRIPTION
System	
Model Name	This is the model name of your NBG7815.
Firmware Version	This is the firmware version.
System Operation Mode	This is the device mode to which the NBG7815 is set, see Section 13.7 on page 145 for more information.
Enable IPv4 Firewall	This shows if the IPv4 firewall is enabled on the NBG7815.
Enable IPv6 Simple Security	This shows if the IPv6 firewall is enabled on the NBG7815.
System Uptime	This is the total time the NBG7815 has been on.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC address of your NBG7815.
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 NBG7815 in the LAN.

PART II

Technical Reference

CHAPTER 8

Applications

8.1 Applications Overview

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

8.1.1 What You Can Do

- Use the **Parental Control** screens to enable parental control, configure the parental control rules and schedules, and send email notifications. ([Section 8.2 on page 66](#)).
- Use the **OpenVPN Server** screen to create or configure your NBG7815 when it functions as an OpenVPN Server ([Section 8.3.1 on page 70](#)).
- Use the **OpenVPN Client** screen to add an OpenVPN Server Account you want your NBG7815 to connect to ([Section 8.3.3 on page 73](#)).
- Use the **USB Application** screen to allow file sharing or to set up your NBG7815 to act as a media server ([Section 8.4 on page 75](#)).

8.1.2 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 NBG7815 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 NBG7815 supports New Technology File System (NTFS), File Allocation Table (FAT) and FAT32 file systems.

Windows/CIFS

Common Internet File System (CIFS) is a standard protocol supported by most operating systems in order to share files across the network.

CIFS runs over TCP/IP but uses the SMB (Server Message Block) protocol found in Microsoft Windows for file and printer access; therefore, CIFS will allow all applications, not just Web browsers, to open and share files across the Internet.

The NBG7815 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 NBG7815. 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 (FTP)

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

VPN

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

8.1.3 Before You Begin

Make sure the NBG7815 is connected to your network and turned on.

- 1 Connect the USB device to the NBG7815's USB port.
- 2 The NBG7815 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 NBG7815, see the troubleshooting for suggestions.

8.2 Parental Control

Parental Control allows you to block specific URLs. You can also define time periods and days during which the NBG7815 performs parental control on a specific user.

Note: This is not available if you are using bridge mode.

8.2.1 Device Setup

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


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

Figure 26 Parental Control > Device

No.	Type	Network	Name	MAC	IP Address	Profile	Action
1		Main Network	TWPCNT03116-01	DC:4A:3E:40:EC:67	192.168.123.164	unassigned	
2		Main Network	TWNBNT02168-01	F8:16:54:B5:C0:52	192.168.123.58	unassigned	

The following table describes the fields in this screen.

Table 11 Parental Control > Device

LABEL	DESCRIPTION
Sort By	Choose to sort the order of your client devices by Type or Name .
Connect to	Choose whether you want to show client devices that are connected to Main Network or client devices that are connected to Guest Network . Choose All if you want to show all client devices.
No.	This shows the index number of the rule.
Type	This shows the type of client device to which this rule applies.
Network	This shows the type of network the client devices are connected to.
Name	This shows the name of the user to which this rule applies.
MAC	This field shows the MAC address of the client device with the name in the Name field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a client 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 client device. If no rule exists, unassigned is showed in this field.
Action	Click the Action icon () to configure a rule for the client device.

8.2.1.1 Edit Device Detail



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

Figure 27 Parental Control > Device: Edit

Table 12 Parental Control > Device: Edit

LABEL	DESCRIPTION
Device Name	Enter a name for the client device to which this rule applies.
Device Type	Choose the type of client device to which this rule applies.
APPLY	Click APPLY to save your settings back to the NBG7815.
CANCEL	Click CANCEL to exit the screen without saving.

8.2.1.2 Add New Profile

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

Figure 28 Parental Control > Device: Add New Profile

The following table describes the fields in this screen.

Table 13 Parental Control > Device: Add New Profile

LABEL	DESCRIPTION
Profile Name	Enter a name for this rule.
Scheduler Config	Click to Allow or Block WiFi access to client devices.
SELECT ALL	Click SELECT ALL then de-select the blocks you do not want or click on blocks separately to specify days and times to turn WiFi on or off.
DESELECT ALL	Click DESELECT ALL to remove all WiFi scheduling.

8.2.1.3 Profile Screen




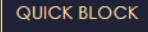


Use this screen to edit or delete an existing rule. Click **Parental Control > Profile** to show the following screen.

Figure 29 Parental Control > Profile



The following table describes the fields in this screen.

Table 14 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 	Click QUICK BLOCK to activate the profile.
Edit 	Click the Edit icon to edit an existing rule.
Delete 	Click the Delete icon to delete an existing rule.

8.3 OpenVPN Server/Client

Note: We do not recommend activating OpenVPN Server and OpenVPN Client at the same time on your NBG7815.

Note: This is not available if you are using bridge mode.

8.3.1 OpenVPN Server

Use this screen to create an OpenVPN server account. Click the **Navigation Panel** icon on the top-left corner (). Select **OpenVPN Server**, and click the **OpenVPN Server** tab.

Figure 30 Example of NBG7815 Acting As VPN Server



The NBG7815 (A) transmits data through a secure VPN channel (B) to the client device (C).

Note: You have to enable DDNS in **Settings > Internet > Dynamic DNS** screen before you can create an OpenVPN account. See [Section 9.8 on page 104](#) for more information on Dynamic DNS.

Figure 31 OpenVPN Server > OpenVPN Server

The screenshot shows the 'OpenVPN Server' configuration page. It is divided into several sections:

- Dynamic DNS:** A toggle switch set to 'Enable'.
- Host Name:** A text field containing 'alice.yin'.
- Configuration:**
 - Status:** Radio buttons for 'Enable' (selected) and 'Disable'.
 - Protocol:** Radio buttons for 'TCP' (selected) and 'UDP'.
 - Server Port:** A text field containing '1194'.
 - VPN Subnet / Netmask:** Two text fields containing '10.8.0.0' and '255.255.255.0' respectively, separated by a slash.
 - Advertise DNS to Clients:** Radio buttons for 'Enable' (selected) and 'Disable'.
 - Key Setting:** A button labeled 'CHANGE KEY'.
- Bottom Buttons:** Three buttons labeled 'EXPORT CONFIG', 'CANCEL', and 'APPLY'.

The following table describes the fields in this screen.

Table 15 OpenVPN Server > OpenVPN Server

LABEL	DESCRIPTION
OpenVPN Server	
Dynamic DNS	This field shows the status of your Dynamic DNS . Make sure it shows Enable before you create an OpenVPN account.
Host Name	This field shows the Host Name of your Dynamic DNS account.
Configuration	
Status	Select Enable to activate your OpenVPN Server account.
Protocol	Select the protocol you want to apply to your OpenVPN Server account.
Server Port	The default server port number is 1194. You can change it if needed. However, clients connected to this OpenVPN Server account will have to use the same port number in order to access the server account.
VPN Subnet / Netmask	The fields define the network from which OpenVPN clients can connect to the NBG7815 OpenVPN server. Enter an IPv4 address and subnet mask.
Advertise DNS to Clients	Select Enable if you want the NBG7815 to broadcast its OpenVPN server to OpenVPN clients in its VPN network defined previously.

Table 15 OpenVPN Server > OpenVPN Server (continued)

LABEL	DESCRIPTION
Key Setting	Click the CHANGE KEY button if you want to change the key your clients use to access to your OpenVPN Server account. You do not need to click CHANGE KEY the first time to configure this screen. Periodically changing the key is recommended, but you must export the new .ovpn configuration file and send it to all OpenVPN clients so that they can they use the new key.
EXPORT CONFIG	Click EXPORT CONFIG to export your configuration to an .ovpn file that OpenVPN clients need to connect to the NBG7815 OpenVPN server.
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to begin configuring this screen afresh.

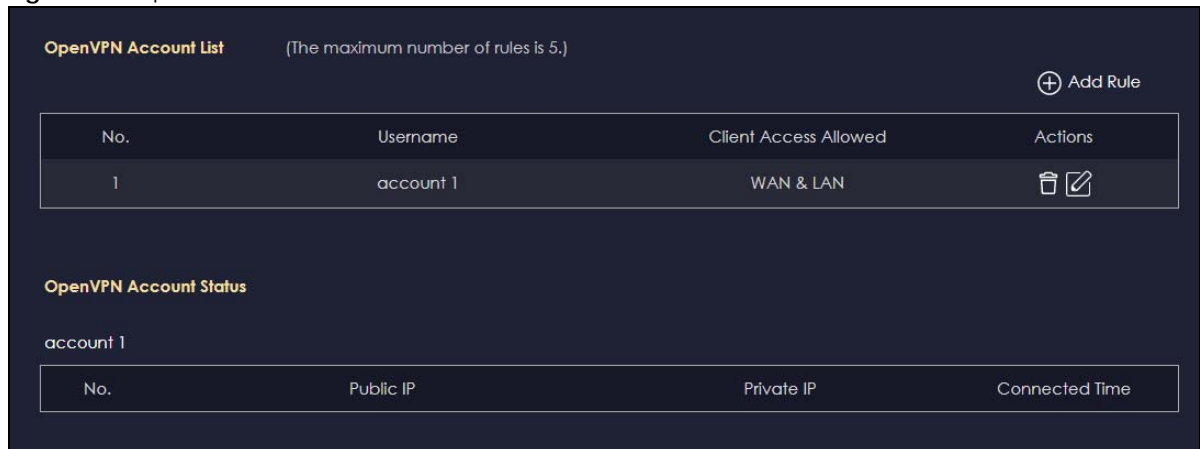
8.3.2 OpenVPN Account

Use the **OpenVPN Account List** screen to view the basic information of the NBG7815 OpenVPN server.

Use the **OpenVPN Account Status** screen to view the basic information of clients that are connected to the NBG7815 OpenVPN server.

Note: At the time of writing, up to 16 OpenVPN clients can connect to the NBG7815 OpenVPN server at the same time.

Figure 32 OpenVPN Account





The following table describes the fields in this screen.

Table 16 OpenVPN Account

LABEL	DESCRIPTION
OpenVPN Account List	
No.	This is the rule index number.
Username	This field displays a name to identify this rule.
Password	This field displays a combination of characters and numbers clients need to connect to an account.
Client Access Allowed	This field displays the interfaces through which the clients are allowed to connect to an account.

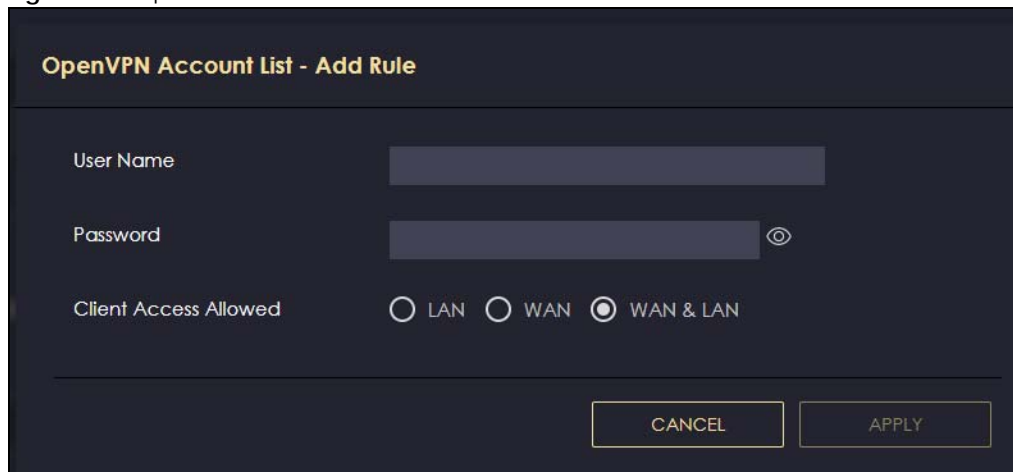
Table 16 OpenVPN Account (continued)

LABEL	DESCRIPTION
Actions	Click the icons under Actions to delete or edit an existing OpenVPN account settings. Click  to delete an existing OpenVPN account. Click  to edit an existing OpenVPN account.
OpenVPN Account Status	
No.	This is the number used to identify a client.
Public IP	This field displays the public IP of a client.
Private IP	This field displays the private IP of a client.
Connected Time	This field displays how long a client is connected.

8.3.2.1 OpenVPN Account List – Add Rule

Use this screen to configure your OpenVPN account settings.

Figure 33 OpenVPN Account List – Add Rule



The following table describes the fields in this screen.

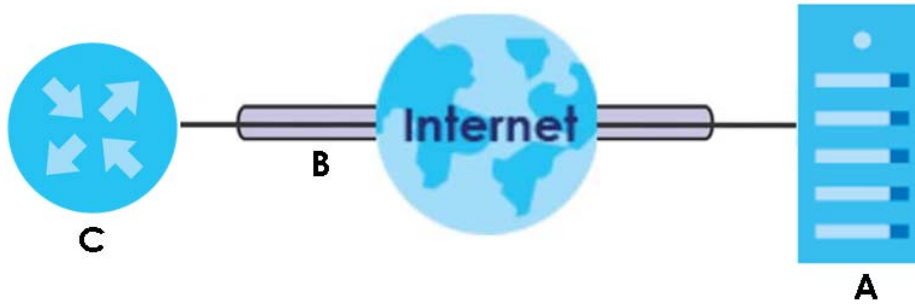
Table 17 OpenVPN Account List – Add Rule

LABEL	DESCRIPTION
User Name	Enter 1 – 32 single-byte printable ASCII characters, but <>^\$& are not allowed.
Password	Enter 1 – 32 single-byte printable ASCII characters, but <>^\$& are not allowed.
Client Access Allowed	Select the interfaces through which the clients are allowed to connect to your account.
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to exit this screen without saving.

8.3.3 OpenVPN Client

Use the **OpenVPN Server List** in this screen to view the basic information of the OpenVPN Server accounts that you are connected to when the NBG7815 functions as an OpenVPN client.

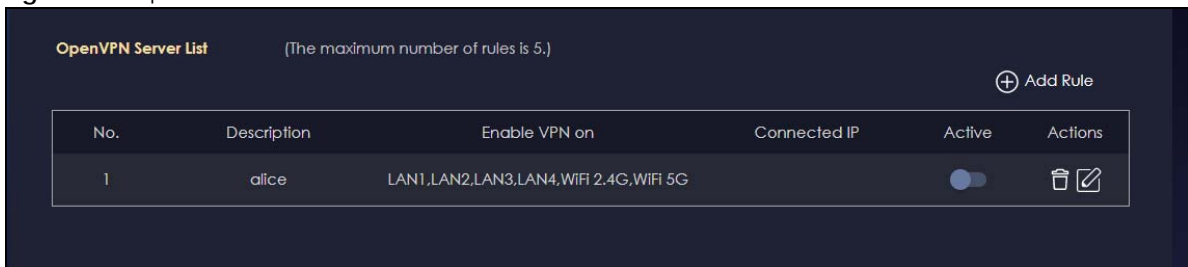
Figure 34 Example of NBG7815 Acting As VPN Client



The VPN server (A) transmits data through a secure VPN channel (B) to the NBG7815 (C) client device.




Note: You can only connect to one server at a time.

Figure 35 OpenVPN Client



The following table describes the fields in this screen.

Table 18 OpenVPN Client

LABEL	DESCRIPTION
No.	This is the rule index number.
Description	This field displays a name to identify this rule.
Enable VPN on	This field displays the interfaces through which your NBG7815 are allowed to connect to an OpenVPN Server account.
Connected IP	This field displays the IP address of the OpenVPN Server account your NBG7815 is connected to.
Active	Slide the switch to the right () to activate your connection to an OpenVPN Server account.
Actions	Click the icons under Actions to delete or edit an existing OpenVPN Server account settings. Click  to delete an existing OpenVPN Server account. Click  to edit an existing OpenVPN Server account.

8.3.3.1 OpenVPN Server List – Add Rule

Use this screen to add an OpenVPN Server Account that you want your NBG7815 to connect to.

Figure 36 OpenVPN Server List – Add Rule

OpenVPN Server List - Add Rule

Description

User Name

Password

Import .ovpn file No file chosen

Enable VPN on All

LAN1 LAN2 LAN3 LAN4

WiFi 2.4G WiFi 5G

The following table describes the fields in this screen.

Table 19 OpenVPN Server List – Add Rule

LABEL	DESCRIPTION
Description	Enter 1 – 32 single-byte printable ASCII characters, but <>^\$& are not allowed.
User Name	Enter the User Name of the OpenVPN Server account you want to connect to.
Password	Enter the Password of the OpenVPN Server account you want to connect to.
Import .ovpn file	Import an .ovpn file that you get from the OpenVPN Server that you want to connect to. Note: Do NOT import the .ovpn file you get from your NBG7815's OpenVPN Server.
Enable VPN on	Select the interfaces that are allowed by the OpenVPN Server account you want to connect to.
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to exit this screen without saving.

8.4 USB Application

Configure file sharing through File Explorer / FTP with users on your network using a USB memory stick or hard drive connected to your NBG7815. You can also configure your NBG7815 to function as a DLNA-compliant media server.

8.4.1 SAMBA Server

Use this screen to set up file-sharing through the NBG7815 using File 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 37 USB Application > SAMBA

The following table describes the labels in this screen.

Table 20 USB Application > SAMBA

LABEL	DESCRIPTION
SAMBA Setup	
Enable SAMBA	Select this to enable file sharing through the NBG7815 using File Explorer or by browsing to your work group.
Name	Specify the name to identify the NBG7815 in a work group.
Work Group	You can add the NBG7815 to an existing or a new work group on your network. Enter the name of the work group which your NBG7815 automatically joins. You can set the NBG7815's work group name to be exactly the same as the work group name to which your computer belongs to. Note: The NBG7815 will not be able to join the work group if your local area network has restrictions set up that do not allow devices to join a work group. In this case, contact your network administrator.
Description	Enter the description of the NBG7815 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.

Table 20 USB Application > SAMBA (continued)

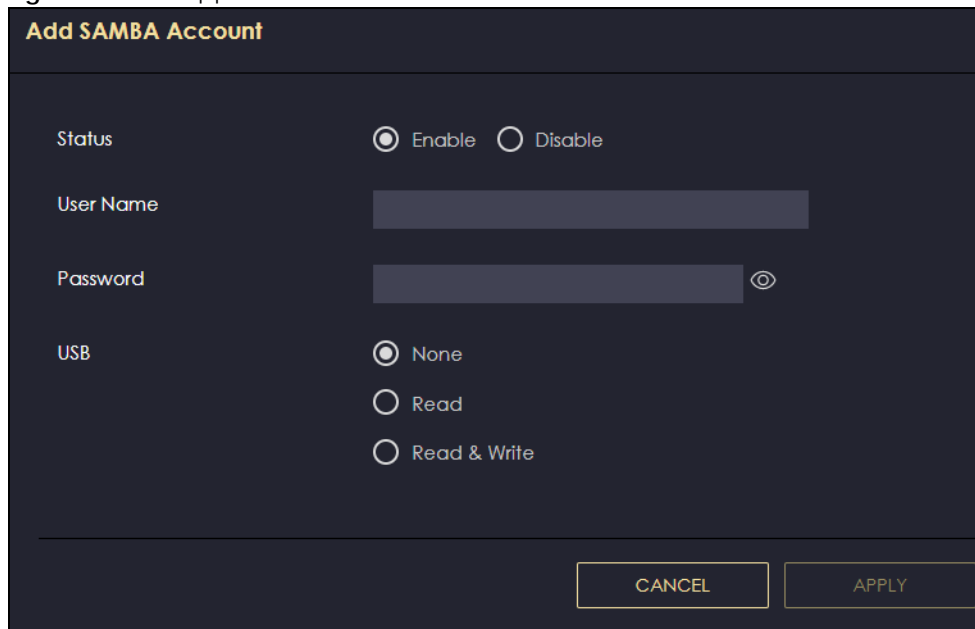
LABEL	DESCRIPTION
User Name	This field displays the user name that will be allowed to access the shared files.
USB	This field displays the user's access rights to the USB storage device which is connected to the NBG7815's USB port.
Actions	Click the icons under Actions to delete or edit a port forwarding rule. Click  to delete a port forwarding rule. Click  to edit an existing port forwarding rule.
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to begin configuring this screen afresh.

8.4.1.1 Add SAMBA Account

Use this screen to configure settings for a SAMBA account.

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

Figure 38 USB Application > SAMBA > Add SAMBA Rule



The following table describes the labels in this screen.

Table 21 USB Application > SAMBA > Add SAMBA 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 are 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 21 USB Application > SAMBA > Add SAMBA Rule (continued)

LABEL	DESCRIPTION
USB	Specify the user's access rights to the USB storage device which is connected to the NBG7815'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 cannot create or edit the files on the connected USB device. None – The user cannot access the files on the USB devices connected to the USB port.
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to exit the screen without saving.

8.4.2 FTP Server

Use this screen to set up file sharing through the NBG7815 using FTP and create user accounts.

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



Figure 39 USB Application > FTP

The following table describes the labels in this screen.

Table 22 USB Application > FTP

LABEL	DESCRIPTION
Enable FTP	Select this to enable the FTP server on the NBG7815 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.
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.

Table 22 USB Application > FTP (continued)

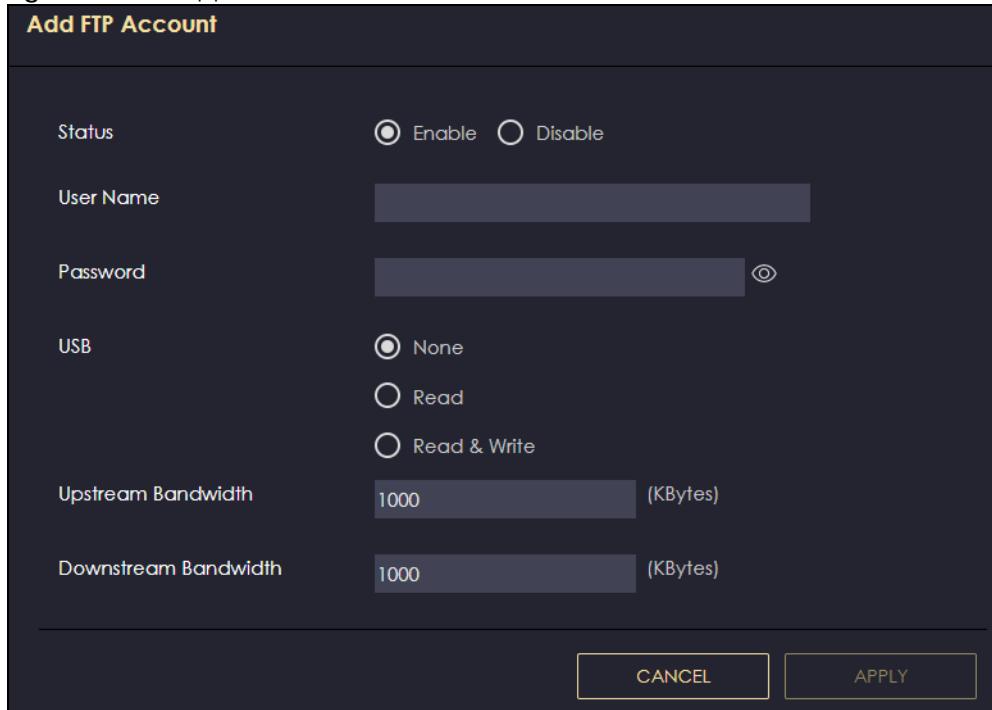
LABEL	DESCRIPTION
USB	This field displays the user's access rights to the USB storage device which is connected to the NBG7815's USB port.
Upstream Bandwidth	This field shows the maximum bandwidth (in Kbps) allowed for incoming FTP traffic.
Downstream Bandwidth	This field shows the maximum bandwidth (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 port forwarding rule. Click  to edit an existing port forwarding rule.
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to begin configuring this screen afresh.

8.4.2.1 Add FTP Account

Use this screen to configure settings for a FTP account.

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


Figure 40 USB Application > FTP > Add FTP Account



Add FTP Account

Status Enable Disable

User Name

Password 

USB None Read Read & Write

Upstream Bandwidth (KBytes)

Downstream Bandwidth (KBytes)

CANCEL **APPLY**

The following table describes the labels in this screen.

Table 23 USB Application > FTP > Add FTP Account

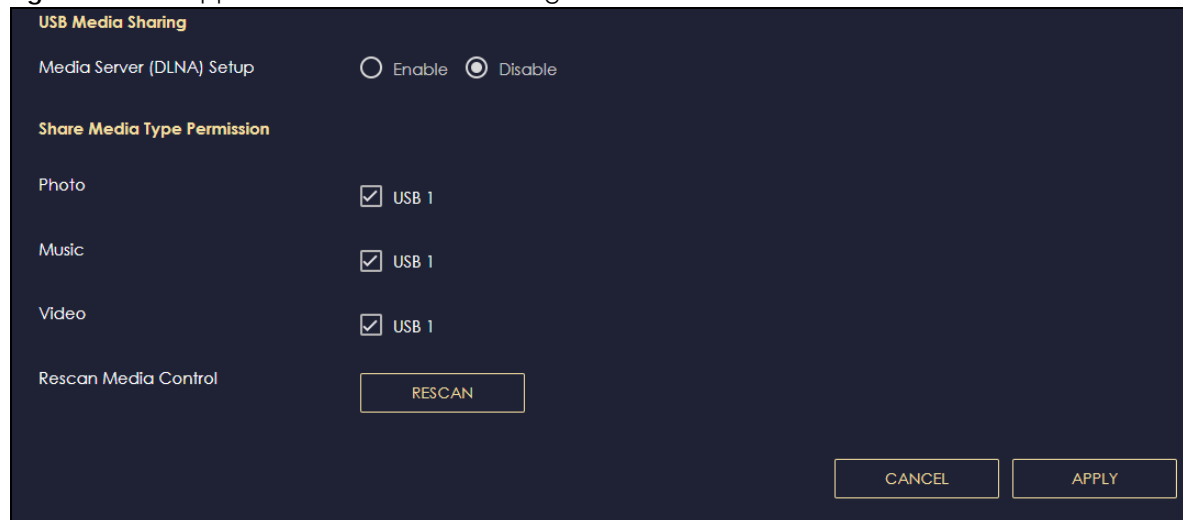
LABEL	DESCRIPTION
Status	Select Enable to enable the account. Select Disable to disable the account.
User Name	Enter a user name that will be allowed to access the shared files. You can enter up to 20 characters. Only letters and numbers allowed.
Password	Enter the password used to access the shared 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 NBG7815'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 cannot create or edit the files on the connected USB device. None – The user cannot access the files on the USB devices 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 NBG7815.
CANCEL	Click CANCEL to exit the screen without saving.

8.4.3 USB Media Sharing

Use this screen to configure settings for media sharing.

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

Figure 41 USB Application > USB Media Sharing



The following table describes the labels in this screen.

Table 24 USB Application > USB Media Sharing

LABEL	DESCRIPTION
USB Media Sharing	
Media Server (DLNA) Setup	Choose Enable to have the NBG7815 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 NBG7815's USB port.
Rescan Media Control	
RESCAN	Click this button to have the NBG7815 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 NBG7815.
CANCEL	Click CANCEL to begin configuring this screen afresh.

8.5 Access Your Shared Files From a Computer

This section shows you how to access shared files from a computer using File Explorer or through FTP.

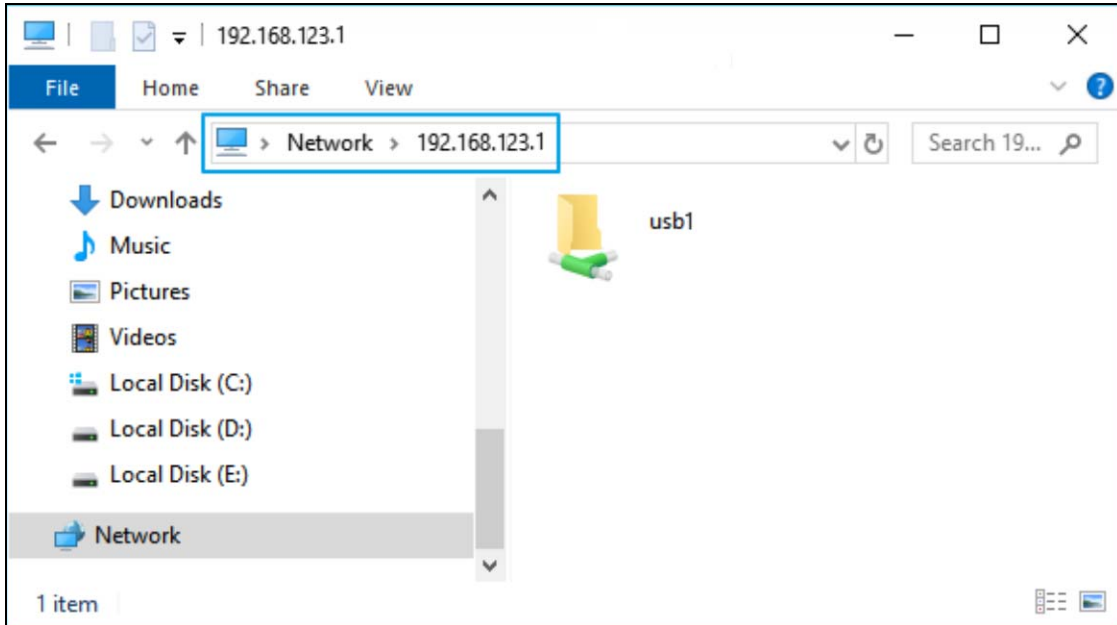
8.5.1 Using File Explorer

You can use File Explorer to access the file storage devices connected to the NBG7815.

Note: The examples in this User's Guide show you how to use Microsoft's Windows 10 to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

Open File Explorer to access **usb1** using the File Explorer browser.

In the File Explorer's address bar type a double backslash "\\\" followed by the IP address of the NBG7815 (the default IP address of the NBG7815 is 192.168.123.1) and press [ENTER]. The share folder **usb1** is available.



Once you access **usb1** through your NBG7815, you do not have to re-login unless you restart your computer.

8.5.2 Using an FTP Program

Here is how to use an FTP program to access a file storage device connected to the NBG7815's USB port.

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

- 1 Download FileZilla and install the FTP software to your computer.
- 2 Go to **USB Application > FTP**. On the **FTP Setup** screen, click **Add Rule** to go to the **Add FTP Account** screen. You can use this screen to create a set of **User Name** and **Password**, and USB rules for file sharing. (See more information at [Section 8.4.2.1 on page 79](#).) Click **Apply** to save the changes.

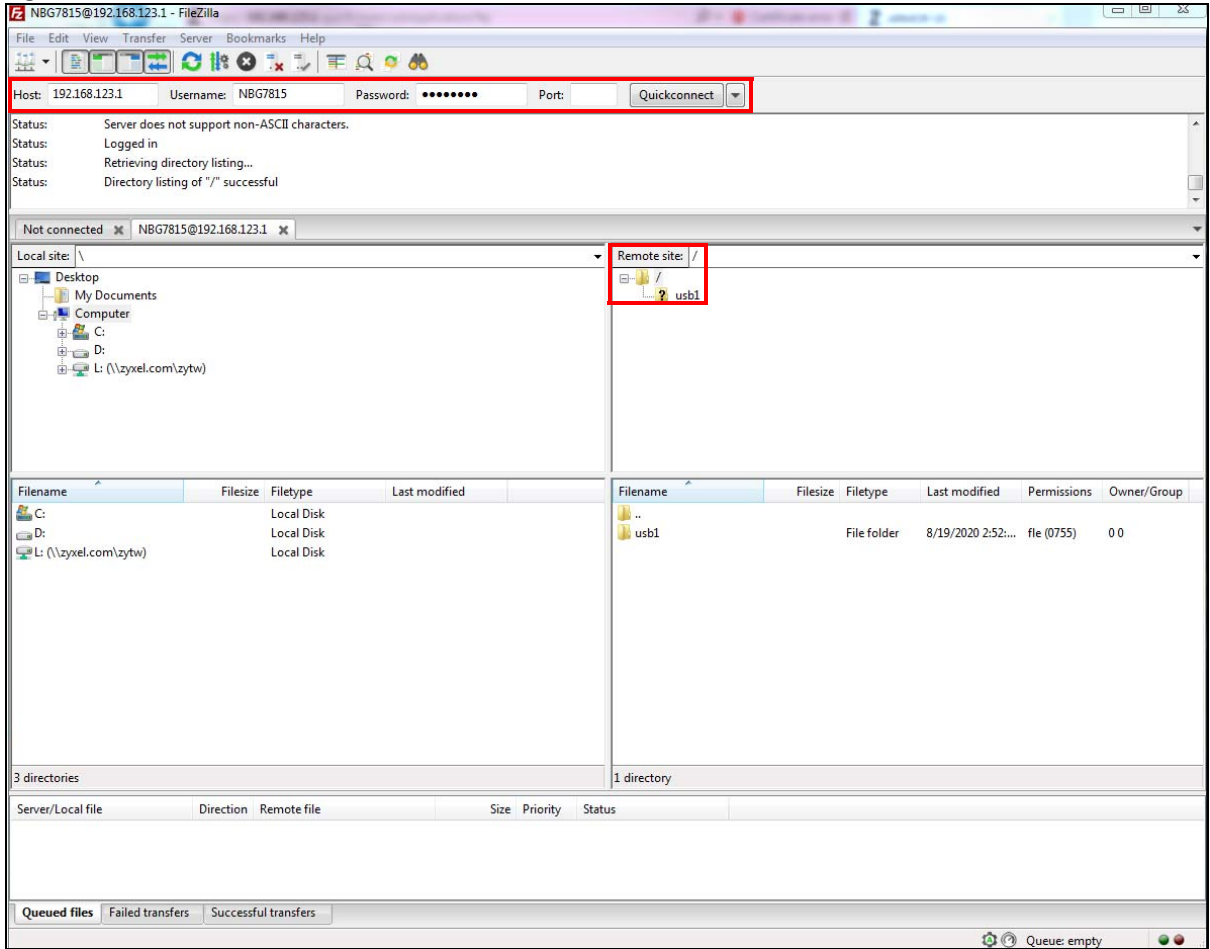
Figure 42 USB Application > FTP : Add FTP Account

- 3 You can click the **Edit** or **Delete** icon to edit or delete the rules.

Figure 43 USB Application > FTP: Edit

- 4 Open FileZilla, enter the **Host** IP address of the NBG7815 (the default IP address is 192.168.123.1), the **Username** and **Password**, and the **port** number 21, and then click **Quickconnect**. A screen asking for password authentication appears.

Figure 44 IFile Sharing through FTP



- 5 Once you log in the USB device displays in the usb1 folder.

CHAPTER 9

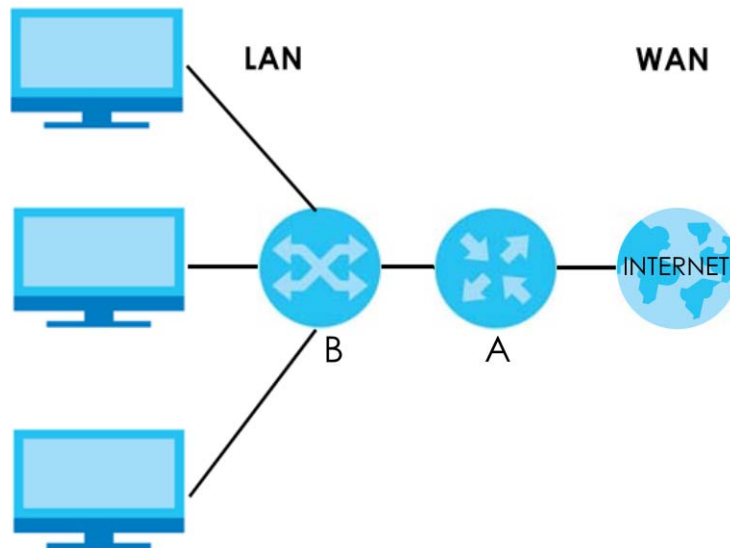
WAN

9.1 WAN (Wide Area Network) Overview

This chapter discusses the NBG7815's **WAN** screens. Use these screens to configure your NBG7815 for Internet access.

A WAN 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. A computer in one location can communicate with computers connected through a Switch (**B**) in other locations through the NBG7815 (**A**).

Figure 45 LAN and WAN



Note: Features in this chapter are not available if you are using bridge mode.

9.2 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 9.4 on page 88](#)).
- Use the **NAT & Port Forwarding** screen to enable NAT, set a default server and change your NBG7815's port forwarding settings ([Section 9.5 on page 97](#)).
- Use the **Passthrough** screen to configure your NBG7815's ALGs and VPN pass-through settings ([Section 9.6 on page 100](#)).
- Use the **Port Trigger** screen to configure your NBG7815's port trigger settings ([Section 9.7 on page 102](#)).
- Use the **Dynamic DNS** screen to change your NBG7815's DDNS settings ([Section 9.8 on page 104](#)).

- Use the **UPnP** screen to enable UPnP on your NBG7815 ([Section 9.9 on page 105](#)).

9.3 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 NBG7815.

9.3.1 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 user name and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the NBG7815, which makes it accessible from an outside network. It is used by the NBG7815 to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the NBG7815 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 addresses (and a gateway IP address if you use the Ethernet).

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 NBG7815 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 NBG7815'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.

IPv6 Addressing

The 128-bit IPv6 address is written as eight 16-bit hexadecimal blocks separated by colons (:). This is an example IPv6 address `2001:0db8:1a2b:0015:0000:0000:1a2f:0000`.

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So `2001:0db8:1a2b:0015:0000:0000:1a2f:0000` can be written as `2001:db8:1a2b:15:0:0:1a2f:0`.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So `2001:0db8:0000:0000:1a2f:0000:0000:0015` can be written as `2001:0db8::1a2f:0000:0000:0015`, `2001:0db8:0000:0000:1a2f::0015`, `2001:db8::1a2f:0:0:15` or `2001:db8:0:0:1a2f::15`.

IPv6 Prefix and Prefix Length

Similar to an IPv4 subnet mask, IPv6 uses an address prefix to represent the network address. An IPv6 prefix length specifies how many most significant bits (start from the left) in the address compose the network address. The prefix length is written as "/x" where x is a number. For example,

```
2001:db8:1a2b:15::1a2f:0/32
```

means that the first 32 bits (`2001:db8`) is the subnet prefix.

IPv6 Subnet Masking

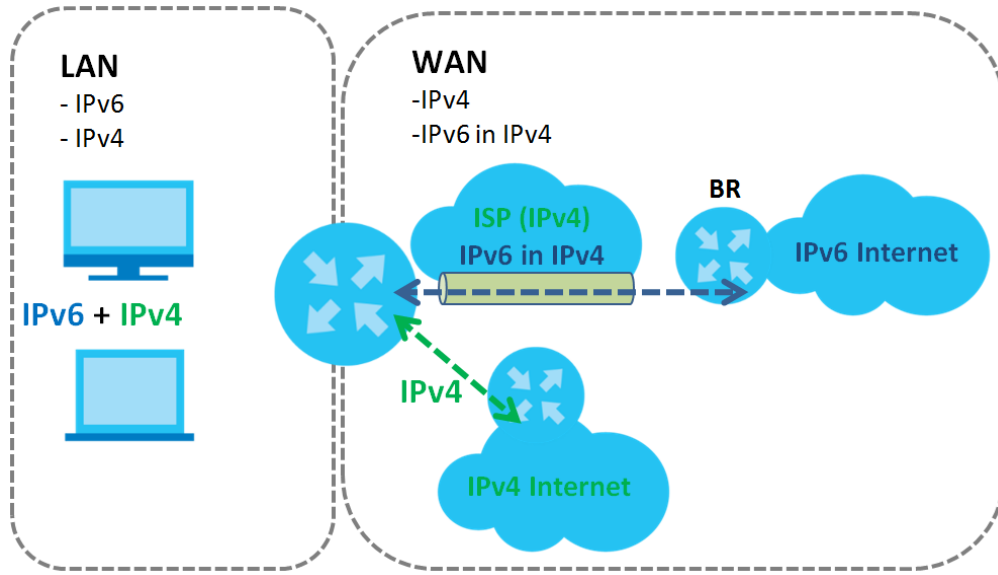
Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 – 10, A – F). Each block's 16 bits are then represented by four hexadecimal characters. For example, `FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000`.

IPv6 Rapid Deployment

Use IPv6 Rapid Deployment (6rd) when the local network uses IPv6 and the ISP has an IPv4 network. When the NBG7815 has an IPv4 WAN address and you set **IPv6/IPv4 Mode** to **IPv4 Only**, you can enable 6rd to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network.

The NBG7815 generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router (BR in the figure) to connect to the native IPv6 Internet. The local network can also use IPv4 services. The NBG7815 uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

Figure 46 IPv6 Rapid Deployment



9.4 Internet Connection

Use this screen to change your NBG7815's Internet access settings. The screen varies depending on the encapsulation method you select. Click **Settings > Internet > Internet Connection**.

9.4.1 IpoE Encapsulation

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

Figure 47 Settings > Internet > Internet Connection: IPoE (IPv4 Only)

The following table describes the labels in this screen.

Table 25 Network > WAN > Internet Connection: IPoE

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 NBG7815 to run IPv4 only. Select Dual Stack to allow the NBG7815 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.

Table 25 Network > WAN > Internet Connection: IPoE (continued)

LABEL	DESCRIPTION
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 NBG7815 divides it into smaller fragments.
DNS Server	
First 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.
Second DNS Server	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.
Third DNS Server	
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 NBG7815 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 NBG7815 change its LAN IP address to 10.0.0.1 or 192.168.123.1 accordingly when the NBG7815 gets a dynamic WAN IP address in the same subnet as the LAN IP address. See Section 9.3.1 on page 86 for more information. The NAT, DHCP server and firewall functions on the NBG7815 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. <ul style="list-style-type: none"> Select DUID-LL (Default) to have the NBG7815 use DUID-LL (DUID Based on Link-layer Address) for identification when exchanging DHCPv6 messages. Select DUID-LLT to have the NBG7815 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	Select User-Defined and enter the IPv6 DNS server address assigned by the ISP to have the NBG7815 use the IPv6 DNS server addresses you configure manually.
Second DNS Server	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.
Third DNS Server	

Table 25 Network > WAN > Internet Connection: IPoE (continued)

LABEL	DESCRIPTION
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to begin configuring this screen afresh.

9.4.2 PPPoE Encapsulation

The NBG7815 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, WiFi, and so on) 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 NBG7815 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG7815 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 48 Settings > Internet > Internet Connection: PPPoE (IPv4 Only)

Internet Connection

Internet Service Provider Type: IPoE PPPoE PPTP

IPv4 / IPv6: IPv4 Only

PPPoE Username: [Input Field]

PPPoE Password: [Input Field] [Eye Icon]

MTU Size: 1492

Service Name: [Input Field]

WAN IP Address Assignment

Obtained From ISP

Fixed IP

IP Address: [Input Field]

DNS Server

First DNS Server: Obtained From ISP 0.0.0.0

Second DNS Server: Obtained From ISP 0.0.0.0

Third DNS Server: Obtained From ISP 0.0.0.0

WAN MAC

Factory Default

Clone My Computer's MAC Address

Set WAN MAC Address

LAN & WAN Subnet Conflict

Automatically change the LAN IP: Enable Disable

CANCEL APPLY

The following table describes the labels in this screen.

Table 26 Network > WAN > Internet Connection: PPPoE

LABEL	DESCRIPTION
Internet Connection	
Internet Service Provider Type	Select PPPoE if you connect to your Internet through dial-up.
IPv4 / IPv6	Select IPv4 Only if you want the NBG7815 to run IPv4 only. Select Dual Stack to allow the NBG7815 to run IPv4 and IPv6 at the same time.
PPPoE Username	Enter the user name given to you by your ISP.

Table 26 Network > WAN > Internet Connection: PPPoE (continued)

LABEL	DESCRIPTION
Password	Enter 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 NBG7815 can receive and process.
Service Name	Enter the PPPoE service name specified in the ISP account.
DNS Server	
First 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.
Second DNS Server	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.
Third DNS Server	
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 NBG7815'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 address 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. <ul style="list-style-type: none"> Select DUID-LL (Default) to have the NBG7815 use DUID-LL (DUID Based on Link-layer Address) for identification when exchanging DHCPv6 messages. Select DUID-LLT to have the NBG7815 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	Select User-Defined and enter the IPv6 DNS server address assigned by the ISP to have the NBG7815 use the IPv6 DNS server addresses you configure manually.
Second DNS Server	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.
Third DNS Server	
LAN & WAN Subnet Conflict	

Table 26 Network > WAN > Internet Connection: PPPoE (continued)

LABEL	DESCRIPTION
Automatically change the LAN IP	Select this option to have the NBG7815 change its LAN IP address to 10.0.0.1 or 192.168.123.1 accordingly when the NBG7815 gets a dynamic WAN IP address in the same subnet as the LAN IP address. See Section 9.3.1 on page 86 for more information. The NAT, DHCP server and firewall functions on the NBG7815 are still available in this mode.
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to begin configuring this screen afresh.

9.4.3 PPTP Encapsulation

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

Figure 49 Settings > Internet > Internet Connection: PPTP (IPv4 Only)

The following table describes the labels in this screen.

Table 27 Network > WAN > Internet Connection: PPTP

LABEL	DESCRIPTION
Internet Connection	
Internet Service Provider Type	Select PPTP if you want to connect the Internet through point to point tunneling protocol.

Table 27 Network > WAN > Internet Connection: PPTP (continued)

LABEL	DESCRIPTION
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 MPPE.
MTU Size	Enter the MTU (Maximum Transmission Unit) size for each packet. If a larger packet arrives, the NBG7815 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	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.
Second DNS Server	
Third DNS Server	
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 Fixed IP .
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 NBG7815 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 address 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 NBG7815 change its LAN IP address to 10.0.0.1 or 192.168.123.1 accordingly when the NBG7815 gets a dynamic WAN IP address in the same subnet as the LAN IP address. See Section 9.3.1 on page 86 for more information. The NAT, DHCP server and firewall functions on the NBG7815 are still available in this mode.
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to begin configuring this screen afresh.

9.5 NAT and Port Forwarding

Use Port Forwarding to forward incoming service requests from the Internet to the servers on your local network. Port forwarding is commonly used when you want to host online gaming, P2P file sharing, or other servers on your network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, DNS service is on port 53 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service, it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

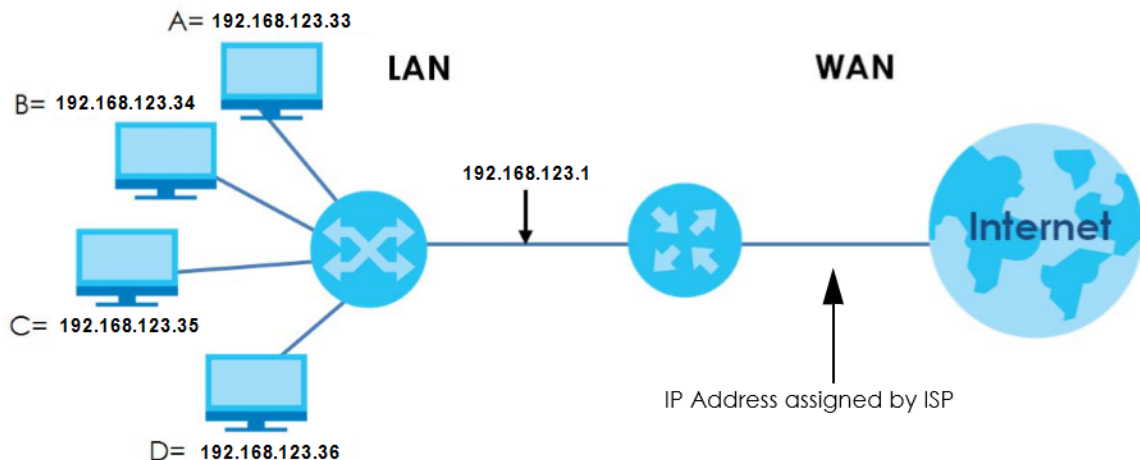
Note: TCP port 80, 443, 8008, 8099, and 8443 are reserved ports and can not be used for NAT and firewall rules.

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

Configuring Servers Behind Port Forwarding (Example)

Let us say you want to assign ports 21 – 25 to one FTP, Telnet and SMTP server (**A** in the example), port 60 to another (**B** in the example) and assign a default server IP address of 192.168.123.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 50 Multiple Servers Behind NAT Example



Use this screen to enable NAT, set a default server and view the summary table of your NBG7815's port forwarding settings. Click **Settings > Internet > NAT & Port Forwarding** to show the following screen.

Figure 51 Settings > Internet > NAT & Port Forwarding

NAT & Port Forwarding

Network Address Translation (NAT) Enable Disable

Server Setup Default Server - 192.168.123.1
 Change to Server
 TWNBNT02231-02

Port Forwarding Rule (The maximum number of rules is 32.)

Enable Port Forwarding Enable Disable + Add Rule



No.	Name	Protocol	External Port	Server IP Address	Internal Port	Actions
1	WWW	TCP/UDP	10	192.168.123.143	3	

The following table describes the labels in this screen.

Table 28 Settings > Internet > NAT & Port Forwarding

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	
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 number uniquely identifies the port forwarding rule.
Name	This field displays a name to identify this rule.
Protocol	This is the transport layer protocol used for the service.
External Port	This is the port number used to connect to this service using the router's external IP address on the WAN.

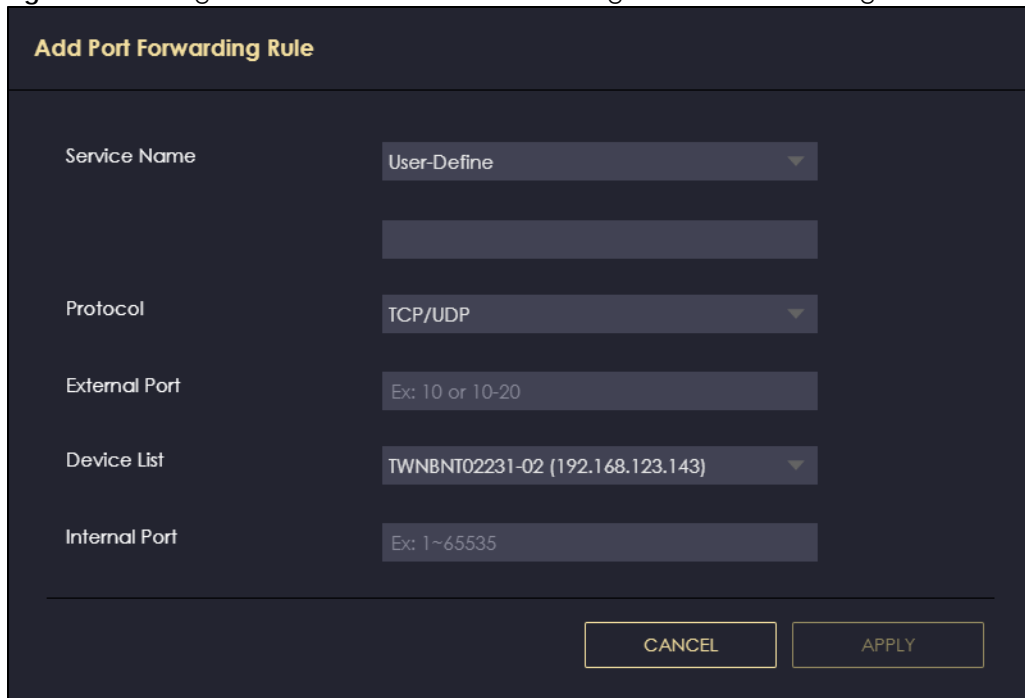
Table 28 Settings > Internet > NAT & Port Forwarding (continued)

LABEL	DESCRIPTION
Server IP Address	This field displays the internal IP address of the server.
Internal Port	This is the port number used to connect to this service using the server's internal IP address on the LAN.
Actions	Click the icons under Actions to delete or edit a port forwarding rule. Click  to delete the rule. Click  to edit the rule.
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to begin configuring this screen afresh.

9.5.1 Add Port Forwarding Rule

Use this screen to configure your NBG7815's port forwarding settings to forward incoming service requests to the servers on your local network. Click **Settings > Internet > NAT & Port Forwarding > Add Rule** to show the following screen.

Figure 52 Settings > Internet > NAT & Port Forwarding: Add Port Forwarding Rule



Add Port Forwarding Rule

Service Name: User-Define

Protocol: TCP/UDP

External Port: Ex: 10 or 10-20

Device List: TWNBNT02231-02 (192.168.123.143)

Internal Port: Ex: 1~65535

CANCEL APPLY

The following table describes the labels in this screen.

Table 29 Settings > Internet > NAT & Port Forwarding: Add Port Forwarding Rule

LABEL	DESCRIPTION
Service Name	Select a pre-defined service from the drop-down list box. The pre-defined service port numbers 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 used to connect to this service using the router's external IP address on the WAN. If you select User-Define in the Service Name field, enter the port numbers manually.
Device List	Select the internal IP address of the virtual server.
Internal Port	This shows the port number used to connect to this service using the server's internal IP address on the LAN. 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 exit this screen without saving.

9.6 Passthrough

Use this screen to change your NBG7815'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 NBG7815'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 NBG7815's NAT.

Figure 53 Settings > Internet > Passthrough

ALG Setup

FTP Enable Disable

H.323 Enable Disable

SIP Enable Disable

SNMP Enable Disable

RTSP Enable Disable

IRC Enable Disable

VPN Passthrough

PPTP Enable Disable

L2TP Enable Disable

IPSEC Enable Disable

CANCEL APPLY

The following table describes the labels in this screen.

Table 30 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.
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 NBG7815 through the network through SNMP.
RTSP	Select Enable to have the NBG7815 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 NBG7815 and the NBG7815 will drop the request. When PPTP is enabled, the NBG7815 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 NBG7815 and the NBG7815 will drop the request. When L2TP is enabled, the NBG7815 will forward the reply from the VPN server to the client that initiated the request, and the connection will establish successfully.

Table 30 Settings > Internet > Passthrough (continued)

LABEL	DESCRIPTION
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 NBG7815 and the NBG7815 will drop the request. When IPSEC is enabled, the NBG7815 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 NBG7815.
CANCEL	Click CANCEL to begin configuring this screen afresh.

9.7 Port Trigger

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding, you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

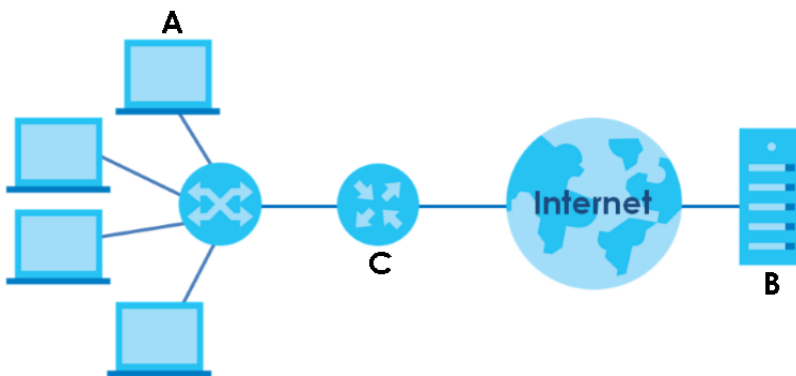
Port trigger addresses this problem. Port trigger allows computers on the LAN to dynamically take turns using the service. The NBG7815 records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the NBG7815's WAN port receives a response with a specific port number and protocol ("open" port), the NBG7815 forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

Note: TCP port 7547 is reserved for system use.

Note: The maximum number of port triggers for a single rule or all rules is 999.

Note: The maximum number of open ports for a single rule or all rules is 999.

Figure 54 Port Trigger Process: Example



- 1 Jane (A) requests a file from the Real Audio server (B, port 7070).

- 2 Port 7070 is a "trigger" port and causes the NBG7815 (C) to record Jane's computer IP address. The NBG7815 associates Jane's computer IP address with the "open" port range of 6970 – 7170.
- 3 The Real Audio server responds using a port number ranging between 6970 – 7170.
- 4 The NBG7815 forwards the traffic to Jane's computer IP address. Only Jane can connect to the Real Audio server until the connection is closed or times out. The NBG7815 times out in 3 minutes with UDP (User Datagram Protocol) or 2 hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Use this screen to view the summary table of your NBG7815's port trigger settings. Click **Settings > Internet > NAT & Port Trigger** to show the following screen.

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

Figure 55 Settings > Internet > NAT & Port Trigger

No.	Name	Incoming Port	End Port	Trigger Port	End Port	Actions
1	A	3	5	4	6	

The following table describes the labels in this screen.

Table 31 Settings > Internet > 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.
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 final port number in a range of port numbers.
Trigger Port	This field displays a port number that causes the NBG7815 to record the IP address of the LAN computer that sent then traffic to a server on the WAN.
End Port	This field displays a port number or the ending port number in a range of port numbers.
Actions	Click the icons under Actions to delete or edit an existing port trigger settings. Click to delete the rule. Click to edit the rule.

9.7.1 Add Port Trigger Rule

Use this screen to configure your NBG7815's port trigger settings. Click **Expert Mode > WAN > NAT > Port Trigger > Add Rule** to show the following screen.

Figure 56 Settings > Internet > NAT & Port Trigger: Add Port Trigger Rule

The following table describes the labels in this screen.

Table 32 Settings > Internet > NAT & Port Trigger: Add Port Trigger Rule

LABEL	DESCRIPTION
Name	Enter 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 NBG7815 forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Enter a port number or the starting port number in a range of port numbers.
End Port	Enter 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 NBG7815 to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Enter a port number or the starting port number in a range of port numbers.
End Port	Enter a port number or the ending port number in a range of port numbers.
APPLY	Click APPLY to save your changes.
CANCEL	Click CANCEL to exit this screen without saving.

9.8 Dynamic DNS

Use this screen to change your NBG7815's DDNS settings. Click **Settings > Internet > Dynamic DNS** to show the following screen.

Note: You can register at <https://mycloud.zyxel.com/> to get a free accessible-from-anywhere DDNS account.

Figure 57 Settings > Internet > Dynamic DNS

Dynamic DNS

Dynamic DNS Enable Disable

Service Provider mycloud.zyxel.com

Host Name _____ .zyxel.me

User Name _____

Password _____

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, Dynamic DNS (DDNS) maps a domain name to a dynamic IP address. With DDNS, you can use a domain name to access your ZyXEL device and home network regardless of the device's current (dynamic) IP address. The ZyXEL device must have a public WAN IP address to use Dynamic DNS.

CANCEL APPLY

The following table describes the labels in this screen.

Table 33 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 name in the field provided. You can specify up to two host names in the field separated by a comma (",").
Username	Enter your user name.
Password	Enter the password assigned to you.
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to begin configuring this screen afresh.

9.9 UPnP

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 9.9.1 on page 106](#) and [Section 9.9.1 on page 106](#) for more information on UPnP.

Use this screen to enable UPnP on your NBG7815. Click **Settings > Internet > UPnP** to display the following screen.

Figure 58 Settings > Internet > UPnP

The following table describes the labels in this screen.

Table 34 Settings > Internet > UPnP

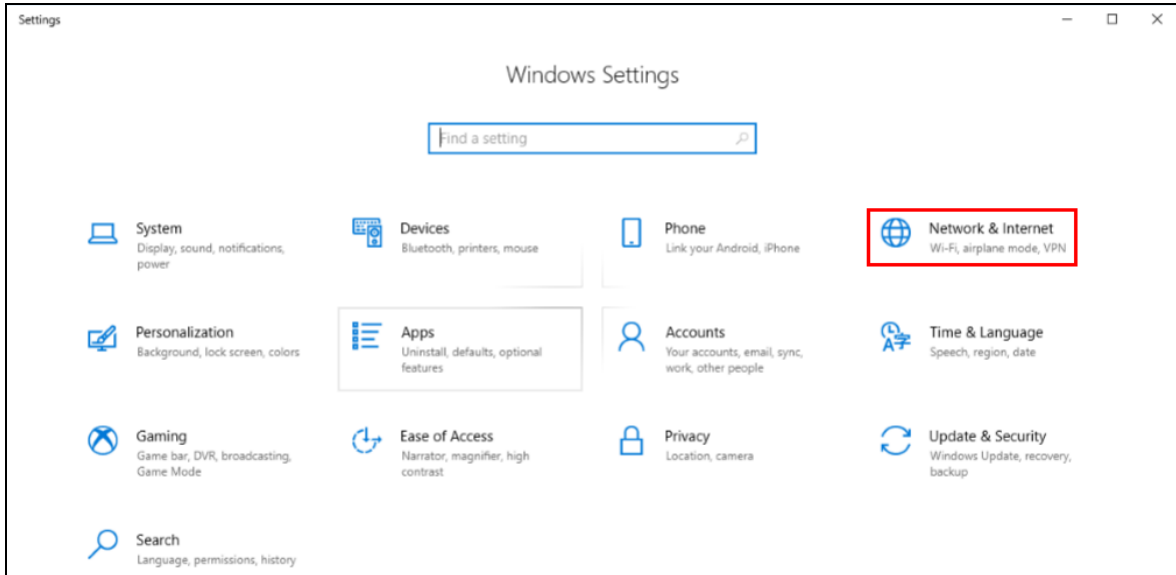
LABEL	DESCRIPTION
UPnP Setup	
Enable UPnP	Select Enable to activate UPnP. Be aware that anyone could use a UPnP application to open the Web Configurator's login screen without entering the NBG7815's IP address (although you must still enter the password to access the Web Configurator).
UPnP Setup Rule	
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 InPort . This field displays the port number of the UPnP entry.
IP Address	This field displays the IP address of this UPnP entry.
APPLY	Click APPLY to save your settings.
CANCEL	Click CANCEL to return to the previously saved settings.

9.9.1 Turning on UPnP in Windows 10 Example

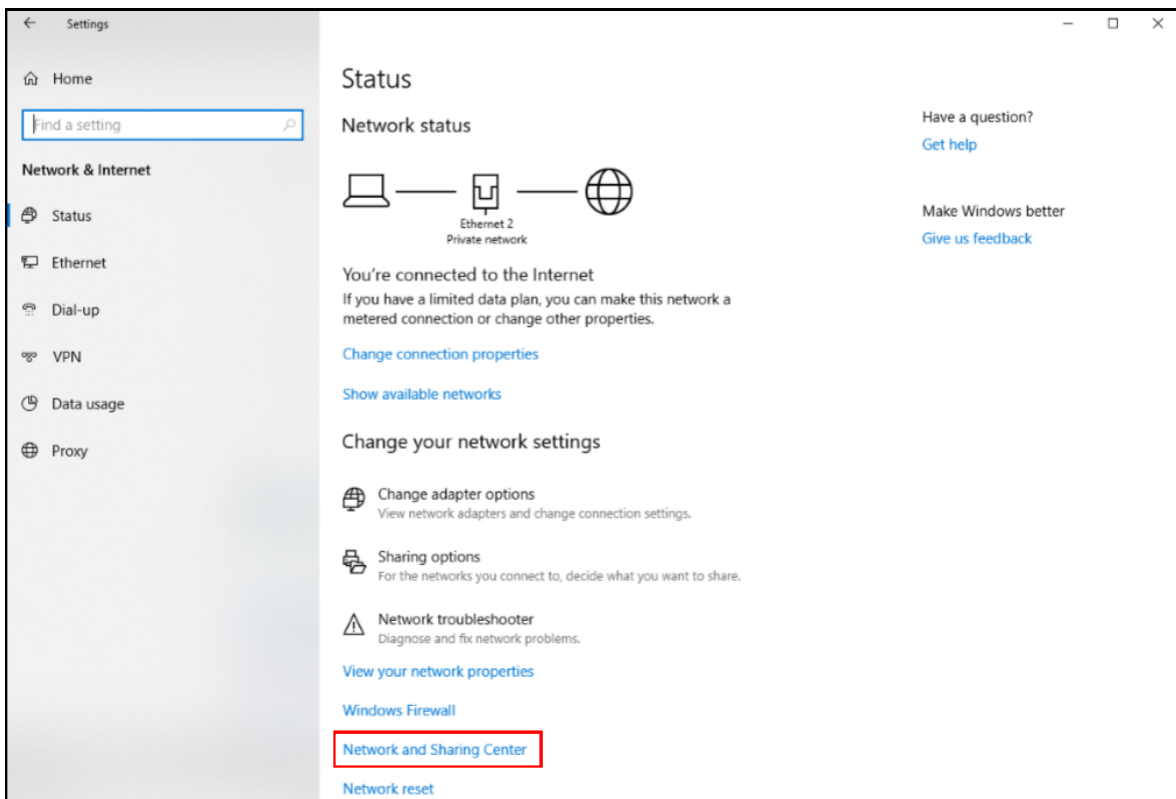
This section shows you how to use the UPnP feature in Windows 10. UPnP server is installed in Windows 10. Activate UPnP on the NBG7815 in **Settings > Internet > UPnP**.

Make sure the computer is connected to the LAN port of the NBG7815. Turn on your computer and the NBG7815.

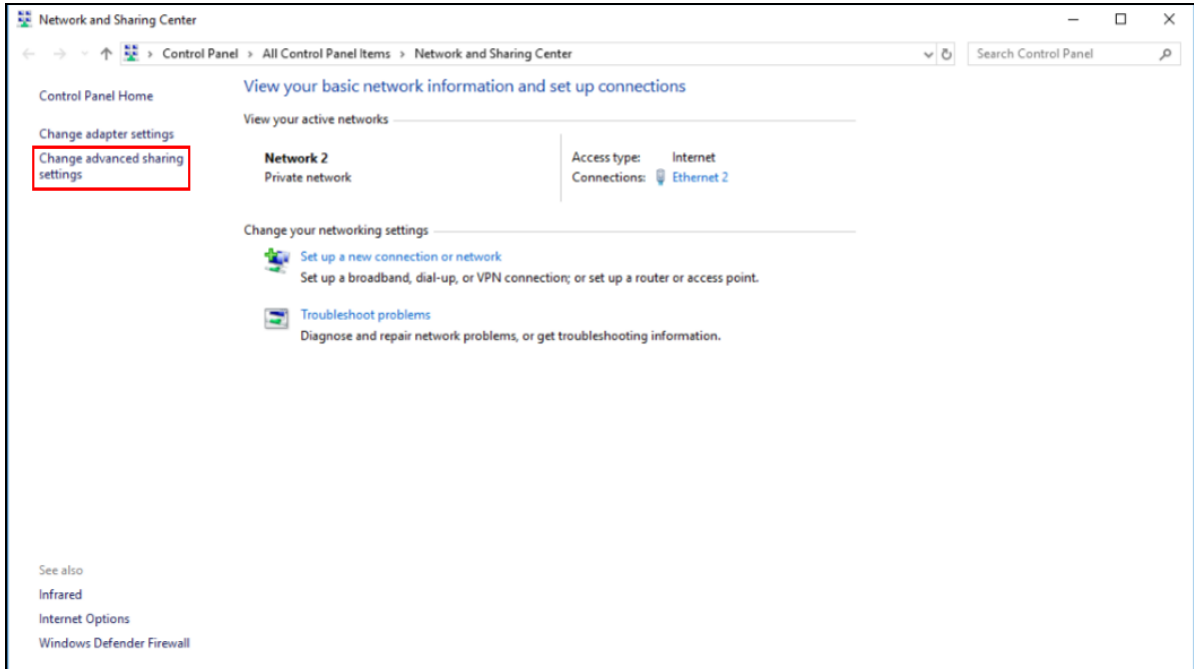
- 1 Click the start icon, **Settings** and then **Network & Internet**.



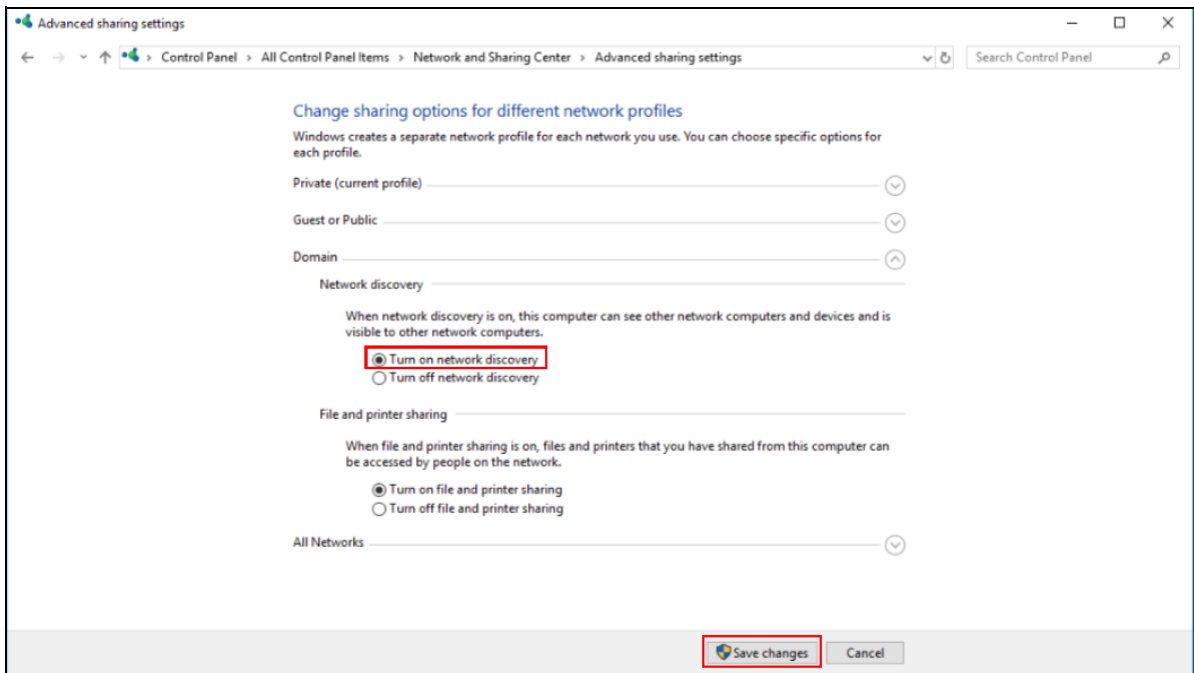
2 Click **Network and Sharing Center**.



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 10

Wireless LAN

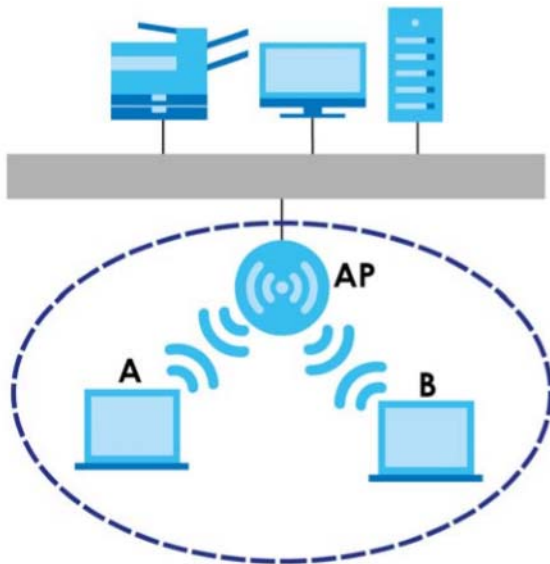
10.1 Wireless LAN Overview

This chapter discusses how to configure the WiFi network settings in your NBG7815. The NBG7815 can service both 2.4G and 5G networks at the same time. You can have different WiFi setup and settings for 2.4G and 5G WiFi. Click **Settings > WiFi** to configure **wireless LAN 2.4G** or **wireless LAN 5G**.

See the appendices for more detailed information about WiFi networks.

The following figure provides an example of a WiFi network.

Figure 59 Example of a WiFi Network



The WiFi network in the figure is encircled in blue. In this WiFi network, devices **A** and **B** are called WiFi clients. The WiFi clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your NBG7815 is the AP.

10.1.1 What You Can Do

- Use the **Main WiFi** screen to enable or disable the 2.4G or 5G WiFi, set up WiFi security between the NBG7815 and the WiFi clients, and make other basic configuration changes ([Section 10.2 on page 113](#)).
- Use the **Guest WiFi** screen to set up multiple WiFi networks on your NBG7815 ([Section 10.3 on page 116](#)).
- Use the **MAC Filter** screen to allow or deny WiFi stations from connecting to the NBG7815 based on their MAC address ([Section 10.4 on page 117](#)).

- Use the **WPS** screen to quickly set up a WiFi network with strong security without having to configure security settings manually ([Section 10.5 on page 118](#)).
- Use the **Scheduling** screen to set the times your WiFi is turned on and off ([Section 10.6 on page 120](#)).

10.1.2 What You Should Know

Every WiFi network must follow these basic guidelines.

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

WiFi Security Overview

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

MAC Address Filter

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

You can use the MAC address filter to tell the AP which WiFi clients are allowed or not allowed to use the WiFi network. If a WiFi client is allowed to use the WiFi network, it still has to have the correct settings (SSID, channel, and security). If a WiFi client is not allowed to use the WiFi 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 WiFi network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized WiFi client. Then, they can use that MAC address to use the WiFi network.

1. Some WiFi devices, such as scanners, can detect WiFi networks but cannot use WiFi networks. These kinds of WiFi 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 WiFi network before they can use it. This is called user authentication. However, every WiFi client in the WiFi network has to support IEEE 802.1x to do this.

For WiFi 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 WiFi network, even if they cannot use the WiFi network. Furthermore, there are ways for unauthorized WiFi users to get a valid user name and password. Then, they can use that user name and password to use the WiFi network.

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

Encryption

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

The WPA-PSK (WiFi Protected Access-Pre-Shared Key) security mode provides both improved data encryption and user authentication over WEP. Using a pre-shared key, both the NBG7815 and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be. The WPA3-SAE (Simultaneous Authentication of Equals handshake) is the newer security mode that protects against dictionary attacks by implementing a new key exchange protocol.

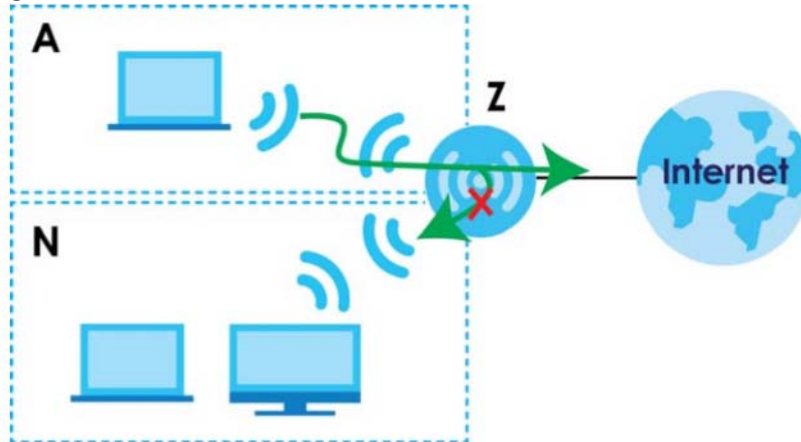
Guest WiFi

Guest WiFi allows you to set up a WiFi network where users can access to Internet through the NBG7815 (Z), but not other networks connected to it. In the following figure, a guest user can access the Internet from the guest WiFi network **A** through **Z** but not the home or company network **N**.

Note: The home or company network **N** and guest WiFi network are independent networks.

Note: Only standard (router) mode supports guest WiFi.

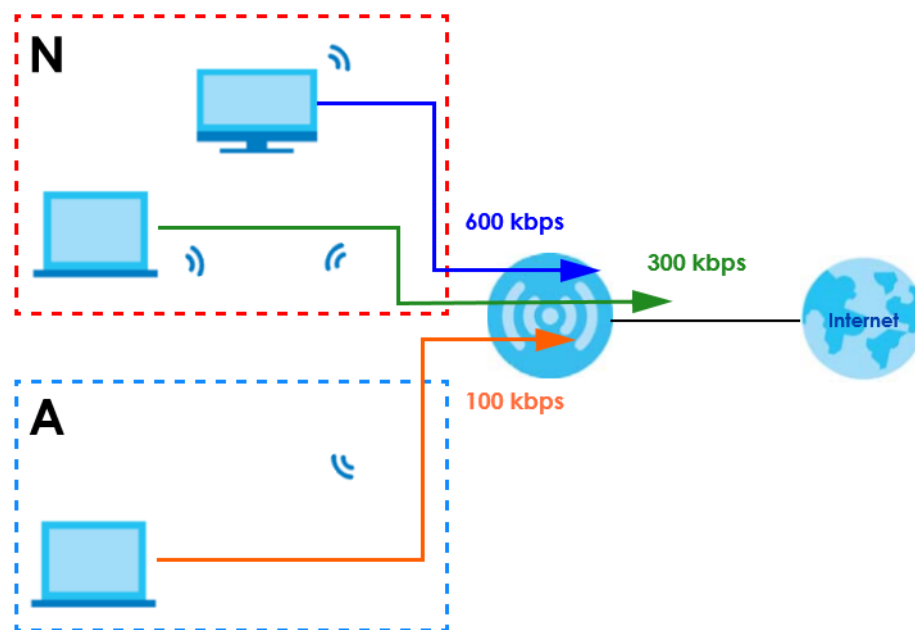
Figure 60 Guest WiFi Network



Guest WiFi Bandwidth

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

Figure 61 Example: Bandwidth for Different Networks



WPS

WiFi Protected Setup (WPS) is an industry standard specification defined by the WiFi Alliance. WPS allows you to set up a WiFi network with strong security without having to configure security settings manually. Depending on the client devices in your network, you can either press a button (on the client device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the client devices. They then connect and set up a secure network by themselves. See how to set up a secure WiFi network using WPS in [Section 4.2 on page 35](#).

10.2 Main WiFi

Use this screen to configure the SSID and WiFi security of the NBG7815's default WiFi.

Note: If you are configuring the NBG7815 from a computer connected to the WiFi and you change the NBG7815's SSID, channel or security settings, you will lose your WiFi connection when you press **Apply** to confirm. You must then change the WiFi settings of your computer to match the NBG7815's new settings.

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

Figure 62 Settings > WiFi > Main WiFi

Main WiFi

Enable Main WiFi Enable Disable

Name(SSID)

Keep 2.4G & 5G name the same

Security Mode WPA2-PSK WPA3-PSK WPA3-PSK Mix

Password

Region

2.4G Bandwidth

2.4G Channel Channel : 9

5G Bandwidth

5G Channel

Advanced Settings ^

2.4G WiFi

OBSS Enable Disable

MU-MIMO

Down Link Enable Disable

Up Link Enable Disable

OFDMA

Down Link Enable Disable

Up Link Enable Disable

5G WiFi

MU-MIMO

Down Link Enable Disable

Up Link Enable Disable

OFDMA

Down Link Enable Disable

Up Link Enable Disable

The following table describes the labels in this screen.

Table 35 Settings > WiFi > Main WiFi



LABEL	DESCRIPTION
Main WiFi	
Enable Main WiFi	Select Enable to activate the 2.4G and/or 5G WiFi. Select Disable to turn it off.
2.4G/5G Name (SSID)	The Service Set Identity (SSID) identifies the WiFi with which a WiFi client is associated. Enter a name (up to 32 printable characters found on a typical English language keyboard) for the WiFi. Click the Keep 2.4G & 5G name the same check box to use the same SSID for 2.4G and 5G WiFi network.
Security Mode	Select the security mode you want to apply to the NBG7815. See Encryption on page 111 for more information on security mode.
Password	The password has two uses: <ul style="list-style-type: none"> Manual: Manually enter the same password on the NBG7815 and the client. Enter 8 – 63 ASCII characters or exactly 64 hexadecimal ('0 – 9', 'a – f') characters. WPS: When using WPS, the NBG7815 sends this password to the client. Click the eye icon  to show or hide the password of your WiFi network. When the eye icon is slashed  , you will 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.
Advanced Settings	
Note: Please check if your device supports these features before enabling them.	
OBSS	Select Enable to have the NBG7815 automatically change the 2.4G bandwidth from 40 MHz to 20 MHz if it detects interference from other 2.4G access points. The NBG7815 automatically changes the 2.4G bandwidth back to 40 MHz when it detects the interference is gone. Note: This setting only takes effect if 2.4G Bandwidth is set to 40 MHz.
MU-MIMO	
Multi-User Multiple-Input, Multiple-Output (MU-MIMO) allows an AP to transmit to multiple groups of MU-MIMO-enabled WiFi clients at the same time, using a technology called RF multipath. WiFi clients in the same group can also co-ordinate in order to transmit to the AP at the same time. MU-MIMO helps decrease client waiting time and increase network throughput. Note: WiFi6 (802.11ax) can support more client groups than WiFi5 (802.11ac). Clients are grouped based on each client's distance and direction from the AP.	
Down Link	Select Enable to allow down link MU-MIMO on the NBG7815. The NBG7815 can then transmit data to several clients simultaneously without a decrease in connection speed.
Up Link	Select Enable to allow up link MU-MIMO on the NBG7815. Several clients can then transmit data to the NBG7815 simultaneously without a decrease in connection speed.
OFDAM	
Orthogonal Frequency-Division Multiple Access (OFDMA) allows an AP to transmit data to multiple OFDMA-enabled WiFi clients at the same time, by dividing channel bandwidth into smaller resource units (RUs). OFDMA-enabled WiFi clients can also co-ordinate in order to transmit to the AP at the same time. OFDMA helps improve efficiency and increase network throughput, especially when WiFi clients are transmitting a large number of small data packets.	
Down Link	Select Enable to allow down link OFDAM on the NBG7815. The NBG7815 can then transmit data to several clients simultaneously without a decrease in connection speed.
Up Link	Select Enable to allow up link OFDAM on the NBG7815. Several clients can then transmit data to the NBG7815 simultaneously without a decrease in connection speed.

Table 35 Settings > WiFi > Main WiFi (continued)

LABEL	DESCRIPTION
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to reload the previous configuration for this screen.

10.3 Guest WiFi

This screen allows you to enable and configure guest WiFi network settings on the NBG7815.

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

Note: This is not available if you are using bridge mode.

Figure 63 Settings > WiFi > Guest WiFi

The following table describes the labels in this screen.

Table 36 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 NBG7815's BSSs. The SSID (Service Set Identifier) identifies the Service Set with which a WiFi device is associated. This field displays the name of the WiFi profile on the network. When a WiFi client scans for an AP to associate with, this is the name that is broadcast and seen in the WiFi client utility.
Security Mode	Select the security mode you want to apply to the NBG7815. See Encryption on page 111 for more information on security mode.
Password	The password has two uses. <ul style="list-style-type: none"> Manual: Manually enter the same password on the NBG7815 and the client. Enter 8 – 63 ASCII characters or exactly 64 hexadecimal ('0 – 9', 'a – f') characters. WPS: When using WPS, the NBG7815 sends this password to the client. Click the Eye icon  to show or hide the password of your WiFi network. When the Eye icon is slashed  , you will see the password in plain text. Otherwise, it is hidden.

Table 36 Settings > WiFi > Guest WiFi (continued)

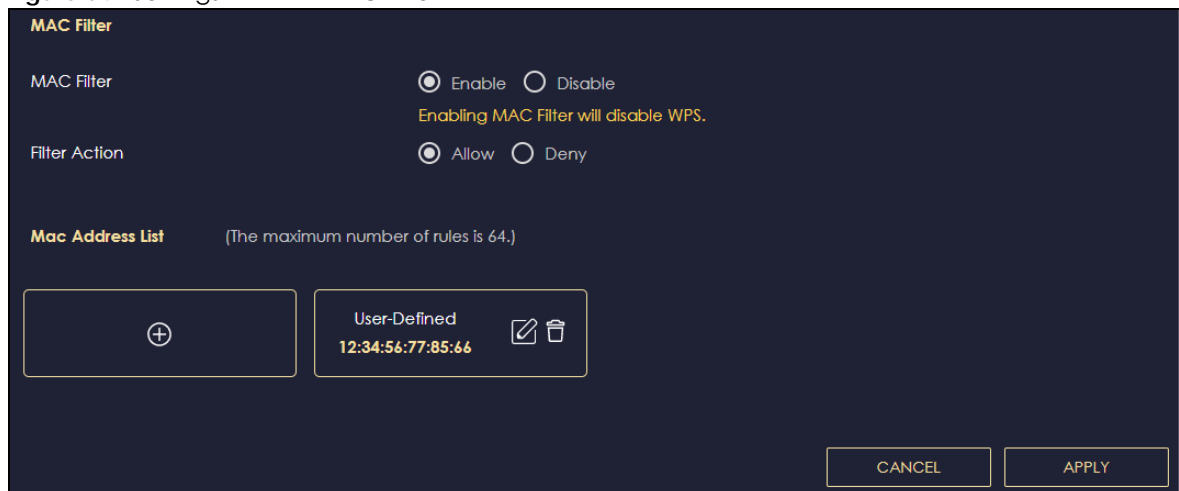
LABEL	DESCRIPTION
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to reload the previous configuration for this screen.

10.4 MAC Filter

The MAC filter screen allows you to give exclusive access to devices (**Allow**) or exclude devices from accessing the NBG7815 (**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 NBG7815's MAC filter settings. Click **Settings > WiFi > MAC Filter** to show following screen.

Figure 64 Settings > WiFi > MAC Filter



The following table describes the labels in this screen.

Table 37 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 NBG7815. MAC addresses not listed will be denied access to the NBG7815. Select Deny to block access to the NBG7815. MAC addresses not listed will be allowed to access the NBG7815.
MAC Address List (Maximum Limit: 64)	
	This field displays the MAC address of the WiFi station you want to filter. Click  to configure the MAC address. Click  to delete the MAC address.

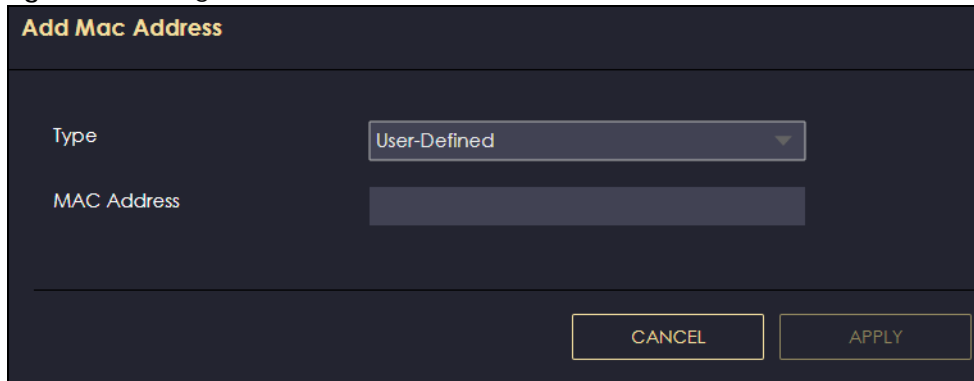
Table 37 Settings > WiFi > MAC Filter (continued)

LABEL	DESCRIPTION
Add	Click  to add a rule in the MAC Address List .
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to reload the previous configuration for this screen.

10.4.1 Add MAC Address

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 65 Settings > WiFi > MAC Filter > Add



The following table describes the labels in this screen.

Table 38 Settings > WiFi > MAC Filter > Add

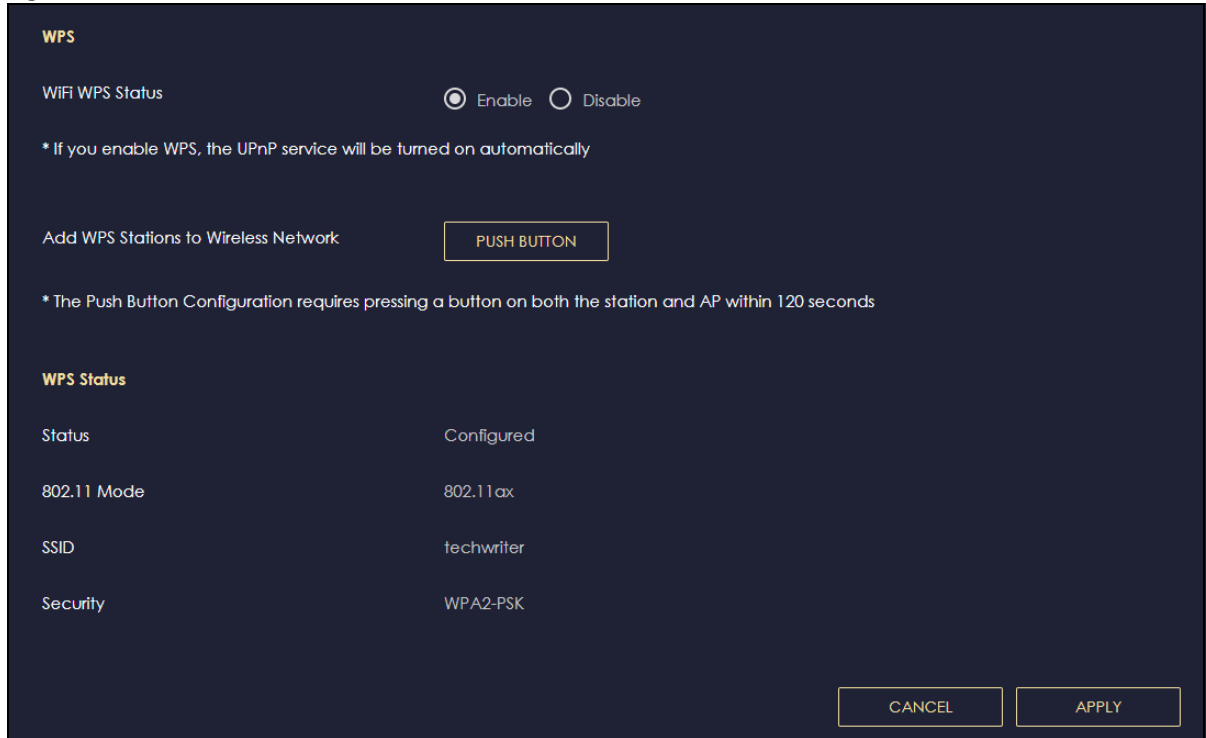
LABEL	DESCRIPTION
Type	This field displays the MAC address of the WiFi station. If you select User-Defined , enter the MAC addresses manually.
MAC Address	Enter a MAC address manually in this field if you select User-Defined in the Type field.
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to exit this screen without saving.

10.5 WPS

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

Note: With WPS, WiFi clients can only connect to the WiFi network using the first SSID on the NBG7815.

Figure 66 Settings > WiFi > WPS



The following table describes the labels in this screen.

Table 39 Settings > WiFi > WPS

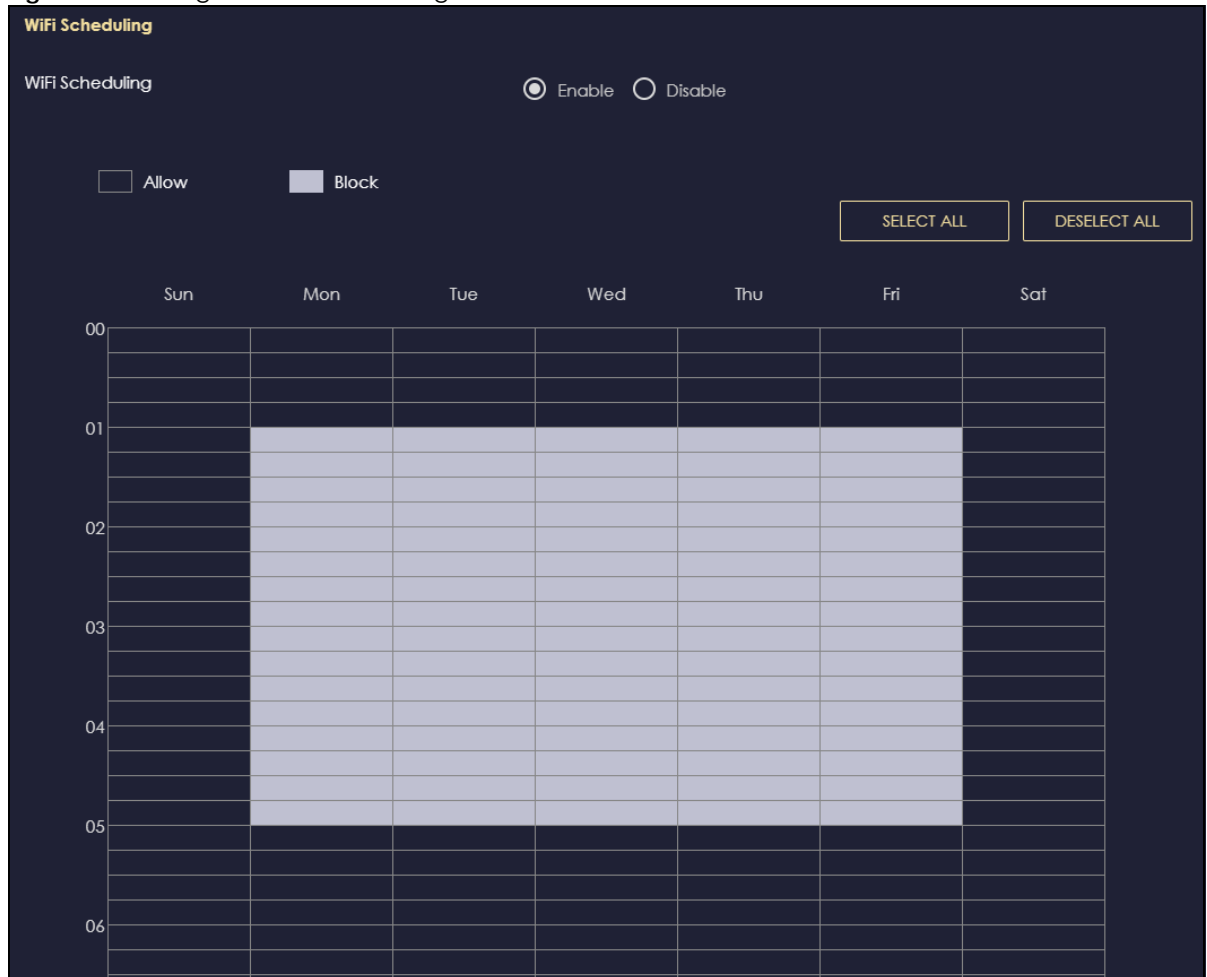
LABEL	DESCRIPTION
WPS	
WiFi WPS Status	Select Enable to turn on the WPS feature. Otherwise, select Disable .
Push Button	Use this button when you use the PBC (Push Button Configuration) method. Click this to start WPS-aware WiFi station scanning and WiFi security information synchronization.
WPS Status	
Status	This displays Configured when a WiFi station has connected to the NBG7815 using WPS and WiFi setup or security settings have been changed from default. The current WiFi setup and security settings also appear in this screen. This displays Unconfigured if WPS is disabled and there are no WiFi setup or security changes on the NBG7815 or if you click Release Configuration to restore WiFi setup and security settings to default.
802.11 Mode	This is the 802.11 mode used. Only compliant WiFi devices can associate with the NBG7815.
SSID	This is the name of the WiFi network (the NBG7815's first SSID) that WPS clients connect to.
Security	This is the type of WiFi security employed by the network.
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to reload the previous configuration for this screen.

10.6 Scheduling

Use this screen to set the times your WiFi is turned on and off. WiFi scheduling is disabled by default. The WiFi 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 on the boxes to select the time period.

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

Figure 67 Settings > WiFi > Scheduling



The following table describes the labels in this screen.

Table 40 Settings > WiFi > Scheduling

LABEL	DESCRIPTION
WiFi Scheduling	Select Enable to activate the WiFi scheduling feature. Select Disable to turn it off. Then select to Allow or Block access to the Internet.
SELECT ALL	Click SELECT ALL or click gray blocks to specify days and times to turn the WiFi 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 WiFi scheduling.

CHAPTER 11

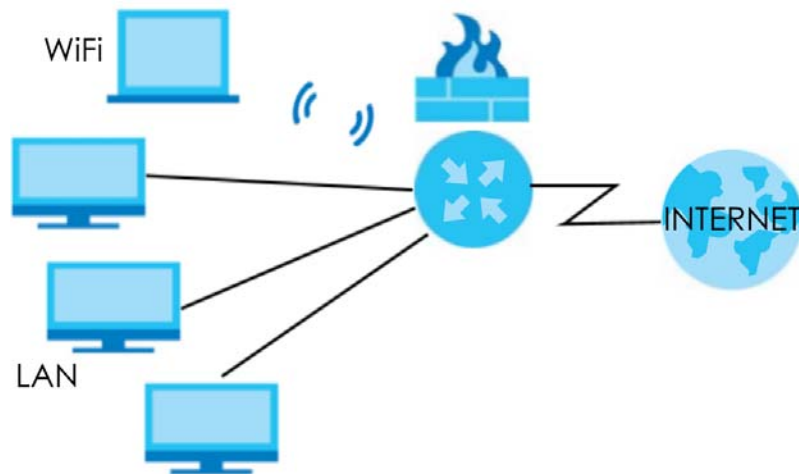
LAN

11.1 LAN (Local Area Network) Overview

This chapter describes how to configure LAN settings.

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

Figure 68 LAN Example



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

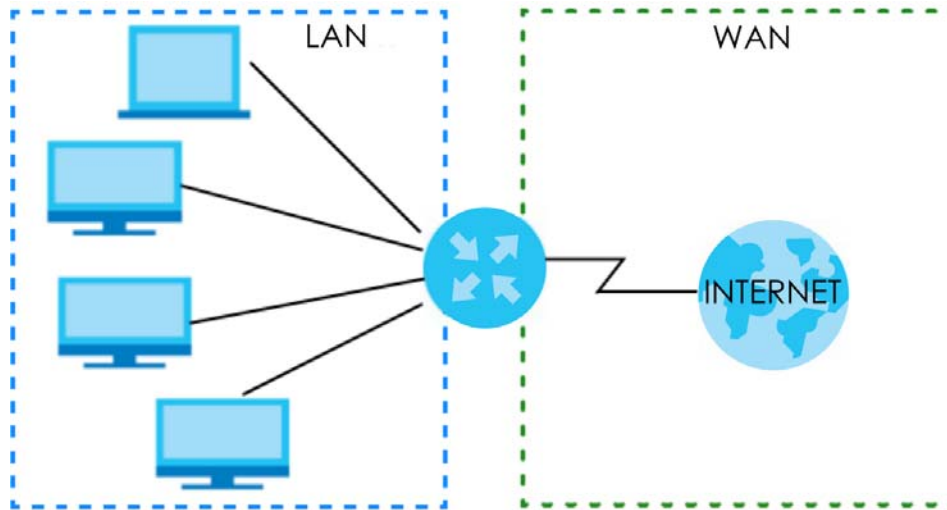
11.2 What You Can Do

- Use the **LAN IP** screen to configure the IPv4 addresses for your NBG7815 on the LAN ([Section 11.4 on page 122](#)).
- Use the **IPv6 LAN** screen to configure the IPv6 address for your NBG7815 on the LAN ([Section 11.5 on page 128](#)).

11.3 What You Need To Know

The actual physical connection determines whether the NBG7815 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 in the following figure.

Figure 69 LAN and WAN IP Addresses



The LAN parameters of the NBG7815 are preset in the factory with the following values:

- IPv4 address of 192.168.123.1 with subnet mask of 255.255.255.0 (24 bits).
- DHCP server enabled with 128 client IPv4 addresses starting from 192.168.123.33.

These parameters should work for the majority of installations.

11.4 LAN IP

Use this screen to change the IPv4 address for your NBG7815 in standard (router) mode. Click **Settings** > **LAN** > **LAN IP** to show the following screen.

Figure 70 Settings > LAN > LAN IP (Standard Mode)

LAN IP Rule

IP Address: 192.168.123.1

IP Subnet Mask: 255.255.255.0

DHCP Server

DHCP Server: Enable Disable

IP Pool Starting Address: 192.168.123. 33

DHCP Pool Size: 200

DNS Server

DNS Servers Assigned by DHCP Server

First DNS Server: LAN IP 192.168.123.1

Second DNS Server: None

Third DNS Server: None

Static DHCP Table (The maximum number of rules is 64.) + Add Rule

No.	Name	MAC Address	IP Address	Actions
1		34:64:A9:27:D6:42	172.21.40.6	
2	TWNBNT02231-02	F0:76:1C:73:D1:CA	192.168.123.143	

CANCEL APPLY



Figure 71 Settings > LAN > LAN IP (Bridge Mode)

The following table describes the labels in this screen.

Table 41 Settings > LAN > LAN IP

LABEL	DESCRIPTION
LAN IP Rule	
IP Address	Enter the IPv4 address of your NBG7815 in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG7815 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 NBG7815.
DHCP Server	
Note: This is not available if you are using bridge mode.	
DHCP Server	Select Enable to activate DHCP for LAN. Select Disable to stop the NBG7815 from 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 NBG7815 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 IPv4 address pool for LAN.
DHCP Pool Size	This field specifies the size, or count of the IPv4 address pool for LAN.
DNS Server	
DNS Servers Assigned by DHCP Server	

Table 41 Settings > LAN > LAN IP (continued)

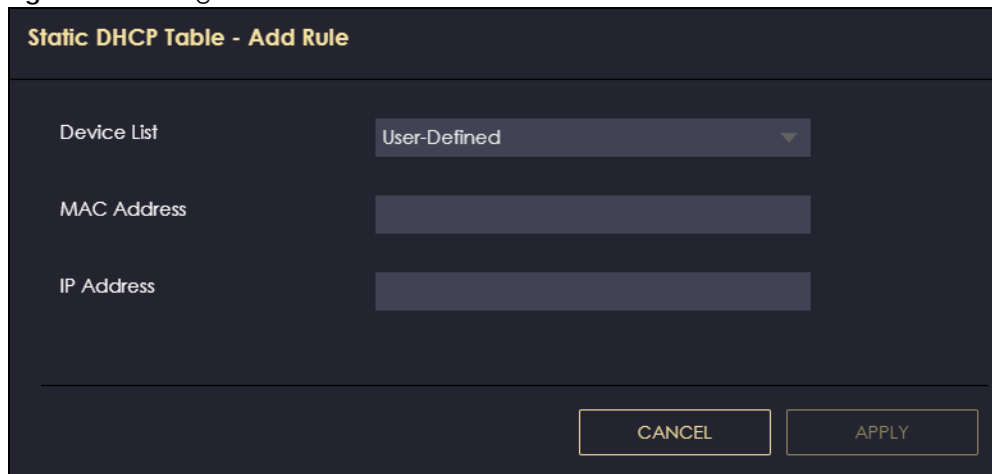
LABEL	DESCRIPTION
First DNS Server	Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the NBG7815's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.
Second DNS Server	
Third DNS Server	
	Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.
	Select LAN IP and the field to the right displays the (read-only) 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	
Note: This is not available if you are using bridge mode.	
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 NBG7815.
CANCEL	Click CANCEL to begin configuring this screen afresh.

11.4.1 Static DHCP Table-Add/Edit Rule

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.

Note: This is not available if you are using bridge mode.

Figure 72 Settings > LAN > LAN IP > Add Rule



Static DHCP Table - Add Rule

Device List: User-Defined

MAC Address: [Empty field]

IP Address: [Empty field]

CANCEL APPLY

Figure 73 Settings > LAN > LAN IP > Edit

The following table describes the labels in these screens.

Table 42 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 NBG7815 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 addresses 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 addresses manually.
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to exit this screen without saving.

11.4.2 Configure LAN Screen in Bridge Mode

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

Click **Settings > LAN > LAN IP** to show the following screen.

Note: If you change the IP address of the NBG7815 in the screen below, you will need to log into the NBG7815 again using the new IP address.

Figure 74 Settings > LAN > LAN IP

The table below describes the labels in the screen.

Table 43 Settings > LAN > LAN IP

LABEL	DESCRIPTION
IP Address setting	
Obtain an IP Address Automatically (DHCP)	<p>When you enable this, the NBG7815 gets its IPv4 address from the network's DHCP server (for example, your ISP). Users connected to the NBG7815 can now access the network (for example, the Internet if the IP address is given by the ISP).</p> <p>The Web Configurator may no longer be accessible unless you know the IP address assigned by the DHCP server to the NBG7815. You need to reset the NBG7815 to be able to access the Web Configurator again (see Section 13.6 on page 144 for details on how to reset the NBG7815).</p> <p>Also when you select this, you cannot enter an IP address for your NBG7815 in the field below.</p>
Static IP Address	Click this if you want to specify the IPv4 address of your NBG7815. Or if your ISP or network administrator gave you a static IP address to access the network or the Internet.
IP Address	Enter the IPv4 address in dotted decimal notation. The default setting is 192.168.123.2. 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 NBG7815 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 NBG7815.
Gateway	Enter a gateway IPv4 address (if your ISP or network administrator gave you one) in this field.
DNS Server	

Table 43 Settings > LAN > LAN IP (continued)

LABEL	DESCRIPTION
First DNS Server	Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the NBG7815's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.
Second DNS Server	
Third DNS Server	
	Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined , but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply . If you set a second choice to User-Defined , and enter the same IP address, the second User-Defined changes to None after you click Apply .
	Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
APPLY	Click APPLY to save your changes to the NBG7815.
CANCEL	Click CANCEL to reload the previous configuration for this screen.

11.5 IPv6 LAN

Use this screen to configure the IPv6 address for your NBG7815 on the LAN. Click **Settings > LAN > IPv6 LAN** to show the following screen.

Note: This is not available if you are using bridge mode.

Figure 75 Settings > LAN > IPv6 LAN

The following table describes the labels in this screen.

Table 44 Settings > LAN > IPv6 LAN

LABEL	DESCRIPTION
LAN IPv6 Address Assignment	
Enable DHCPv6-PD	Select this option to use DHCPv6 prefix delegation. The NBG7815 will obtain an IPv6 prefix from the ISP or a connected uplink router for the LAN.
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 IPv6 addresses that this address object represents.
IPv6 Address range (End)	Enter the end of the range of IPv6 address that this address object represents.
IPv6 Lifetime	Enter the IPv6 lifetime in the LAN.

Table 44 Settings > LAN > IPv6 LAN (continued)

LABEL	DESCRIPTION
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 NBG7815 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 NBG7815 interfaces in the LAN.	
ULA	
Select this option to identify a unique local address of the NBG7815 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 NBG7815.
CANCEL	Click CANCEL to begin configuring this screen afresh.

CHAPTER 12

Security

12.1 Security Overview

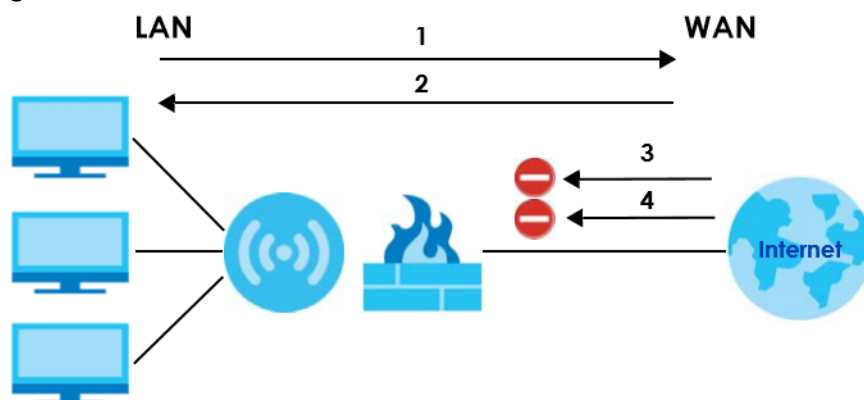
Use these screens to enable and configure the firewall that protects your NBG7815 and your LAN from unwanted or malicious traffic.

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 76 Default Firewall Action



Note: Features in this chapter are not available if you are using bridge mode.

12.1.1 What You Can Do

- Use the **IPv4 Firewall** screen to enable or disable the NBG7815's IPv4 firewall ([Section 12.2 on page 132](#)).
- Use the **IPv6 Firewall** screen to enable or disable the NBG7815's IPv6 firewall ([Section 12.3 on page 135](#)).

12.1.2 What You Need To Know

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

About the NBG7815 Firewall

The NBG7815'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 NBG7815's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG7815 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 NBG7815 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 NBG7815 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 email, 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 through 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 Do not enable any local service (such as NTP) that you do not 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.

12.2 IPv4 Firewall

Use this screen to enable or disable the NBG7815's IPv4 firewall. Click **Settings > Firewall > IPv4 Firewall** to show the following screen.



Figure 77 Settings > Firewall > IPv4 Firewall

The following table describes the labels in this screen.

Table 45 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 NBG7815 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 NBG7815 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.
Dest IP Address	This is the IP address of the computer to which traffic for the application or service is entering.

Table 45 Settings > Firewall > IPv4 Firewall (continued)

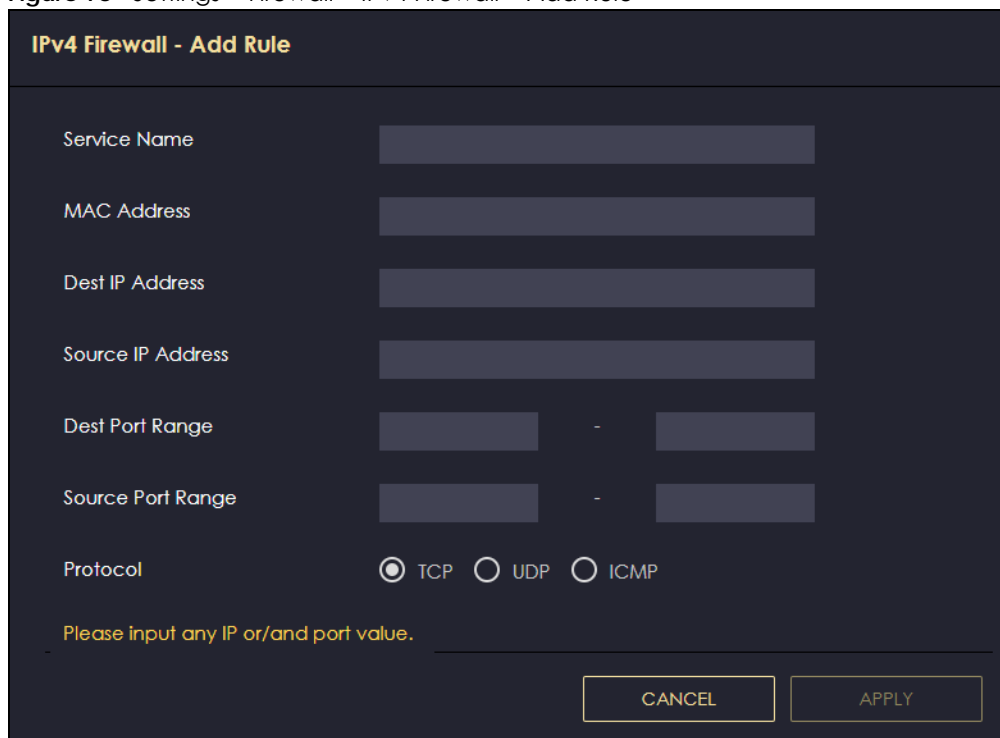
LABEL	DESCRIPTION
Source IP Address	This is the IP address of the computer from which traffic for the application or service is initialized.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 25 defines SMTP traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 25 defines SMTP 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.

12.2.1 IPv4 Firewall – Add Rule

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

Note: For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website.

Figure 78 Settings > Firewall > IPv4 Firewall > Add Rule



IPv4 Firewall - Add Rule

Service Name

MAC Address

Dest IP Address

Source IP Address

Dest Port Range -

Source Port Range -

Protocol TCP UDP ICMP

Please input any IP or/and port value.

CANCEL **APPLY**

The following table describes the labels in this screen.

Table 46 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 NBG7815 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 NBG7815 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 25 defines SMTP traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 25 defines SMTP 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 exit this screen without saving.

12.3 IPv6 Firewall

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 79 Settings > Firewall > IPv6 Firewall

Configuration

Simple Security Enable Disable

Rule Status Enable Disable



Actions Drop Accept

Firewall Rule (The maximum number of rules is 64.) + Add Rule

No.	Service Name	MAC Address	Dest IP Address	Source IP Address	Dest Port Range	Source Port Range	Protocol	Actions

The following table describes the labels in this screen.

Table 47 Settings > Firewall > IPv6 Firewall

LABEL	DESCRIPTION
Configuration	
Simple Security	Select Enable to enabled simple security on your NBG7815.
Rule Status	Select Enable to enabled rule status on your NBG7815.
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 25 defines SMTP traffic.
Source Port Range	This is the port number/range of the source that defines the traffic type, for example TCP port 25 defines SMTP 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.

12.3.1 IPv6 Firewall – Add Rule

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

Figure 80 Settings > Firewall > IPv6 Firewall > Add Rule

IPv6 Firewall - Add Rule

Service Name

MAC Address

Dest IP Address

Source IP Address

Dest Port Range -

Source Port Range -

Protocol TCP UDP ICMPv6

Please input any IP or/and port value.

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 NBG7815 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 NBG7815 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 25 defines SMTP traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 25 defines SMTP 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 exit this screen without saving.

CHAPTER 13

System

13.1 System Overview

This chapter provides information on checking the NBG7815's status and logs, configuring basic and remote management settings, using maintenance and firmware upgrade tools, and changing the operating mode.

13.2 What You Can Do

- Use the **Status** screen to view the basic information of the NBG7815 ([Section 13.3 on page 138](#)).
- Use the **General Setting** screen to change password or to set the timeout period of the management session ([Section 13.4 on page 141](#)).
- Use the **Remote Access** screen to configure the interface/s from which the NBG7815 can be managed remotely and specify a secure client that can manage the NBG7815 ([Section 13.5 on page 143](#)).
- Use the **Maintenance** screen to upload firmware, reboot the NBG7815 without turning the power off or reset the NBG7815 to factory defaults ([Section 13.6 on page 144](#)).
- Use the **Operating Mode** screen select whether you want the NBG7815 to act as a router or a bridge ([Section 13.7 on page 145](#)).
- Use the **Logs** screen to see the system logs recorded by the NBG7815 ([Section 13.8 on page 146](#)).

13.3 Status

Use this screen to view some basic information of your NBG7815. Click **Settings > System > Status** to show the following screen.

Figure 81 Settings > System > Status (Standard Mode)



The screenshot displays the system status page for the NBG7815 router. It is organized into three main sections: System, WAN Information, and LAN Information. Each section lists various parameters and their current values.

System	
Model Name	NBG7815
Firmware Version	V1.00(ABSK.2)B1
System Operation Mode	Standard Mode
Enable IPv4 Firewall	Enable
Enable IPv6 Simple Security	Enable
System Uptime	0 Days 0 Hours 24 Minutes 45 Seconds

WAN Information	
MAC Address	BC:CF:4F:B7:53:61
IP Address	
IP Subnet Mask	
Gateway	
IPv6 Address	

LAN Information	
MAC Address	BC:CF:4F:B7:53:60
IP Address	10.0.0.1
IP Subnet Mask	255.255.255.0
DHCP Server	Enable
IPv6 Address	

Figure 82 Settings > System > Status (Bridge Mode)

System	
Model Name	NBG7815
Firmware Version	V1.00(ABSK.2)B1
System Operation Mode	Bridge Mode
Enable IPv4 Firewall	Enable
Enable IPv6 Simple Security	Enable
System Uptime	0 Days 0 Hours 19 Minutes 20 Seconds
LAN Information	
MAC Address	BC:CF:4F:B7:53:60
IP Address	192.168.1.34
IP Subnet Mask	255.255.255.0
DHCP Server	Enable
IPv6 Address	

The following table describes the labels in this screen.

Table 49 Settings > System > Status

LABEL	DESCRIPTION
System	
Model Name	This is the model name of your NBG7815.
Firmware Version	This is the firmware version.
System Operation Mode	This is the device mode in which the NBG7815 is currently running. See Section 13.7 on page 145 for more information.
Enable IPv4 Firewall	This shows if the IPv4 firewall is enabled on the NBG7815.
Enable IPv6 Simple Security	This shows if the IPv6 firewall is enabled on the NBG7815.
System Uptime	This is the total time the NBG7815 has been on.
WAN Information	
Note: : This is not available if you are using bridge mode.	
MAC Address	This shows the WAN Ethernet adapter MAC address of your NBG7815.
IP Address	This shows the NBG7815's WAN IP address.
IP Subnet Mask	This shows the NBG7815's WAN subnet mask.
Gateway	This shows the WAN port's gateway IP address.
IPv6 Address	This shows the current IPv6 address of the NBG7815.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC address of your NBG7815.
IP Address	This shows the NBG7815's LAN IP address.
IP Subnet Mask	This shows the NBG7815's LAN subnet mask.

Table 49 Settings > System > Status (continued)

LABEL	DESCRIPTION
DHCP Server	This shows whether the NBG7815 acts as a DHCP Server and provides LAN IP addresses to its clients or not.
IPv6 Address	This shows the current LAN IPv6 address of the NBG7815.

13.4 General Setting

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

Figure 83 Settings > System > General Setting (Standard Mode)

System Settings

System Name: NBG7815

Domain Name:

Admin Inactivity Timer: 9999

Select Language: Auto

Admin Password

Current Password:

New Password:

Confirm New Password:

CANCEL APPLY

Figure 84 Settings > System > General Setting (Bridge Mode)

The following table describes the labels in this screen.

Table 50 Settings > System > General Setting

LABEL	DESCRIPTION
System Settings	
System Name	System Name is a unique name to identify the NBG7815 in an Ethernet network.
Domain Name (This is not available if you are using bridge mode)	Enter the domain name you want to give to the NBG7815.
Admin Inactivity Timer	Enter 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 NBG7815.
Admin Password	
Current Password	Enter the default password or the existing password you use to access the system in this field.
New Password	Enter your new system password (up to 30 characters). Note that as you enter a password, the screen displays a dot for each character you enter.
Confirm New Password	Enter the new password again in this field.
APPLY	Click APPLY to save your changes back to the NBG7815.
CANCEL	Click CANCEL to discard all changes.

13.5 Remote Access

Use this screen to change your NBG7815's remote management settings. You can use HTTPS or Wake on LAN to access and manage the NBG7815.

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 (such as 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 client to use this feature. It may be on a label on the device.

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

Figure 85 Settings > System > Remote Access (Standard Mode)

The following table describes the labels in this screen.

Table 51 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 interfaces through which a computer may access the NBG7815 using this service.

Table 51 Settings > System > Remote Access (continued)

LABEL	DESCRIPTION
Wake on LAN	
Wake on LAN Status	Select Enable to have the NBG7815 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	Enter 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.
Start	Click this to have the NBG7815 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 NBG7815.
CANCEL	Click CANCEL to begin configuring this screen afresh.

13.6 Maintenance Setup

Use this screen to upgrade firmware, restart or reset your NBG7815.

Online Firmware

Find firmware at www.zyxel.com in a file that uses the version number and project code with a "*.bin" extension, for example, "V1.00(ABCS.0)C0.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to 2 minutes. After a successful upload, the system will reboot.

System Restart

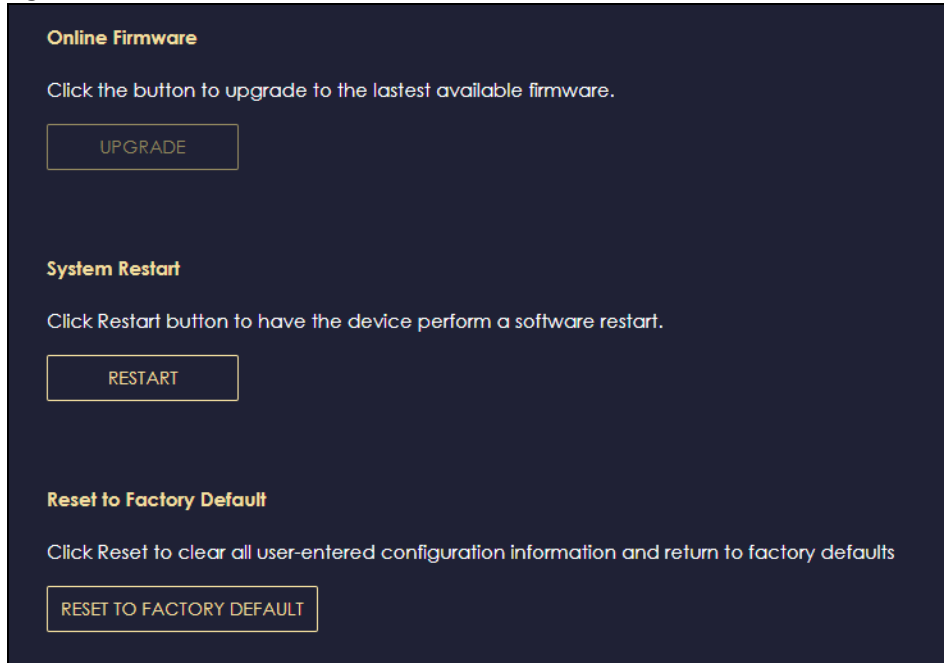
System restart allows you to reboot the NBG7815 without turning the power off.

Reset to Factory Default

Click the **RESET TO FACTORY DEFAULT** button in this section to clear all user-entered configuration information and returns the NBG7815 to its factory defaults.

You can also press the **Reset** button on the rear panel to reset the factory defaults of your NBG7815.

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

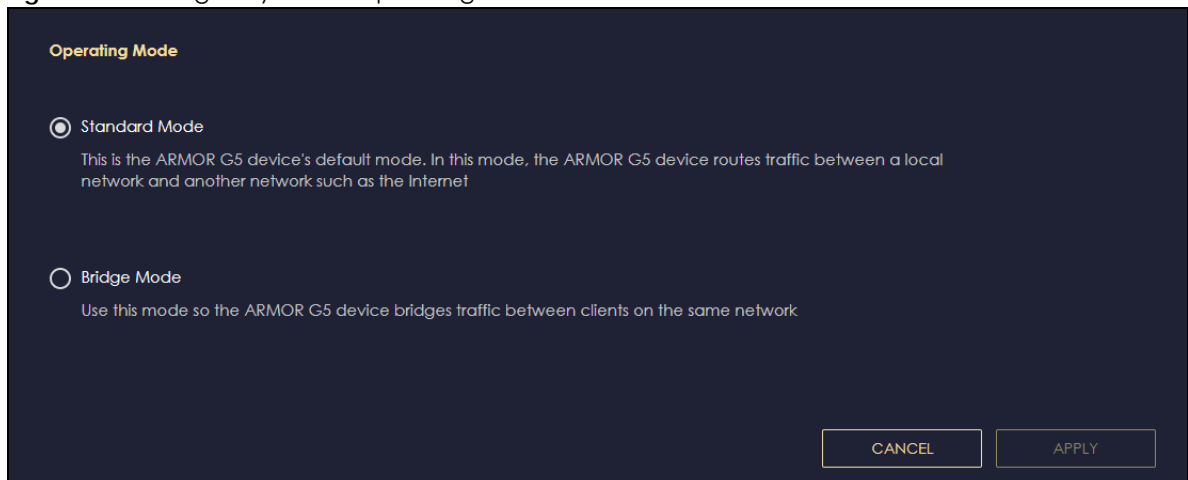
Figure 86 Settings > System > Maintenance

13.7 Operating Mode

Use this screen to select how you want to use your NBG7815.

The **Operating Mode** function lets you configure your NBG7815 as a router or bridge. You can choose between **Standard Mode**, and **Bridge Mode** depending on your network topology and the features you require from your NBG7815.

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

Figure 87 Settings > System > Operating Mode

The following table describes the labels in this screen.

Table 52 Settings > System > Operation Mode

LABEL	DESCRIPTION
Standard Mode	Select Standard 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.
Bridge Mode	Select Bridge Mode if your device bridges traffic between clients on the same network. <ul style="list-style-type: none"> In Bridge Mode, all Ethernet ports have the same IP address. All ports on the rear panel of the device are LAN ports, including the port labeled WAN. There is no WAN port. The DHCP server on your device is disabled. Router functions (such as NAT, bandwidth management, remote management, firewall and so on) are not available when the NBG7815 is in Bridge Mode. The IP address of the device on the local network is set to 192.168.123.2.
APPLY	Click APPLY to save your settings.
CANCEL	Click CANCEL to return your settings to the default (Standard).

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

13.8 Logs

Use this screen to see the logged messages for the NBG7815.

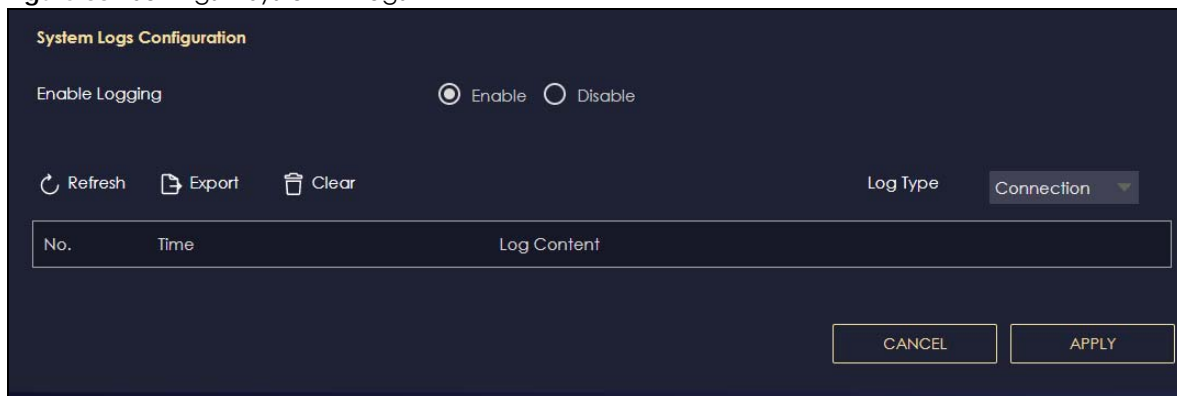
You can configure which logs to display in the Log screen.

The newest log replaces the oldest log after it fills. Select what logs you want to see from the **Log Type** drop-down list box. The log choices depend on your other settings in the **System** screens. Click **Refresh** to renew the log screen. Click **Export** to save the current list of logs to your computer. Click **Clear** to delete all the logs.

Click **APPLY** to save your settings. Click **CANCEL** to discard all changes.

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

Figure 88 Settings > System > Logs



PART III

Troubleshooting and Appendices

CHAPTER 14

Troubleshooting

14.1 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](#)
- [NBG7815 Access and Login](#)
- [Internet Access](#)
- [Resetting the NBG7815 to Its Factory Defaults](#)
- [WiFi Connections](#)
- [OpenVPN Problems](#)
- [USB File Sharing Problems](#)

14.2 Power, Hardware Connections, and LEDs

[The NBG7815 does not turn on. None of the LEDs turn on.](#)

- Make sure you are using the power adapter or cord included with the NBG7815.
- Make sure the power adapter or cord is connected to the NBG7815 and plugged in to an appropriate power source. Make sure the power source is turned on.
- Disconnect and re-connect the power adapter or cord to the NBG7815.
- If the problem continues, contact the vendor.

[One of the LEDs does not behave as expected.](#)

- Make sure you understand the normal behavior of the LED.
- Check the hardware connections. See the Quick Start Guide.
- Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- Disconnect and re-connect the power adapter to the NBG7815.
- If the problem continues, contact the vendor.

14.3 NBG7815 Access and Login

I do not know the IP address of my NBG7815.

- The default IP address of the NBG7815 in **Standard Mode** is **192.168.123.1**. If the NBG7815 obtains a WAN IP address in the same subnet as the LAN IP address 192.168.123.1, the default LAN IP address will be changed to 10.0.0.1 automatically. See [Auto-IP Change on page 17](#) for more information. The default IP address of the NBG7815 in **Bridge Mode** is **192.168.123.2**.
- If you changed the IP address and have forgotten it, you might get the IP address of the NBG7815 in **Standard 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 NBG7815 (it depends on the network), so enter this IP address in your Internet browser.
- If your NBG7815 in **Bridge 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.
- Reset your NBG7815 to change all settings back to their default. This means your current settings are lost. See [Section 14.5 on page 152](#) in the **Troubleshooting** for information on resetting your NBG7815.

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

- Make sure you are using the correct IP address.
- The default IP address of the NBG7815 in **Standard Mode** is **192.168.123.1**. If the NBG7815 obtains a WAN IP address in the same subnet as the LAN IP address 192.168.123.1, the default LAN IP address will be changed to 10.0.0.1 automatically. See [Auto-IP Change on page 17](#) for more information. The default IP address of the NBG7815 in **Bridge Mode** is **192.168.123.2**.
- If you changed the IP address ([Section 11.4 on page 122](#)), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I do not know the IP address of my NBG7815](#).
- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See [Appendix B on page 161](#) for more information.
- Make sure your computer is in the same subnet as the NBG7815. (If you know that there are routers between your computer and the NBG7815, skip this step.)
- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See [Section 11.4 on page 122](#).
- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG7815. See [Section 11.4 on page 122](#).
- Reset the device to its factory defaults, and try to access the NBG7815 with the default IP address. See [Section on page 19](#).
- If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the NBG7815 using another service, such as Telnet. If you can access the NBG7815, check the remote management settings and firewall rules to find out why the NBG7815 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 NBG7815.

- This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.
- Disconnect and re-connect the power adapter or cord to the NBG7815.
- If this does not work, you have to reset the device to its factory defaults. See [Section 14.5 on page 152](#).

14.4 Internet Access

I cannot access the Internet.

- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- Go to **Expert > Maintenance > Operation Mode**. Check your System Operation Mode setting.
If the NBG7815 is in **Standard Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access. Your computer and the NBG7815 should be in the same subnet.
If the NBG7815 is in **Bridge Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access and your computer is set to obtain a dynamic IP address.
- If the NBG7815 is in **Standard 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.
- If you are trying to access the Internet wirelessly, make sure the WiFi settings in the WiFi client are the same as the settings in the AP.
- Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NBG7815), but my Internet connection is not available anymore.

- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- Reboot the NBG7815.

- If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

- There might be a lot of traffic on the network. Look at the LEDs. If the NBG7815 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- Check the signal strength. If the signal strength is low, try moving the NBG7815 closer to the AP if possible, and look around to see if there are any devices that might be interfering with the WiFi network (for example, microwaves, other WiFi networks, and so on).
- Reboot the NBG7815.
- If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

14.5 Resetting the NBG7815 to Its Factory Defaults

If you reset the NBG7815, you lose all of the changes you have made. The NBG7815 reloads its default settings (for example, default Standard (Router) operation mode and login IP address of 192.168.123.1, WiFi SSID and password). 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 NBG7815:

- Make sure the power LED is on.
- Press the **Reset** button for 1 to 4 seconds to restart/reboot the NBG7815.
- Press the **Reset** button for longer than 8 seconds to set the NBG7815 back to its factory-default configurations.

If the NBG7815 restarts automatically, wait for the NBG7815 to finish restarting, and log in to the Web Configurator.

If the NBG7815 does not restart automatically, disconnect and reconnect the NBG7815's power. Then, follow the directions above again.

14.6 WiFi Connections

I cannot access the NBG7815 or ping any computer from the WLAN.

- Make sure the WiFi is enabled on the NBG7815.
- Make sure the WiFi adapter on your computer is working properly.

- Make sure the WiFi adapter installed on your computer is IEEE 802.11 compatible and supports the same WiFi standard as the NBG7815.
- Make sure your computer (with a WiFi adapter installed) is within the transmission range of the NBG7815.
- Check that both the NBG7815 and the WiFi adapter on your computer are using the same WiFi and WiFi security settings.
- Make sure traffic between WiFi and the LAN is not blocked by the firewall on the NBG7815.
- Make sure you allow the NBG7815 to be remotely accessed through the WLAN interface. Check your remote management settings.

I cannot access the Web Configurator after I switched to Bridge Mode.

- When you change from **Standard Mode** to **Bridge Mode**, your computer must have an IP address in the range between "192.168.123.3" and "192.168.123.254".

The WiFi connection is slow or intermittent.

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 WiFi devices.

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

- Move your WiFi device closer to the NBG7815 if the signal strength is low.
- Reduce WiFi interference that may be caused by other WiFi networks or surrounding wireless electronics such as cordless phones.
- Place the NBG7815 where there are minimum obstacles (such as walls and ceilings) between the NBG7815 and the WiFi client. Avoid placing the NBG7815 inside any type of box that might block WiFi signals.
- Reduce the number of WiFi clients connecting to the same NBG7815 simultaneously, or add additional NBG7815s if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the WiFi 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 NBG7815 is placed on a table or floor, point the antennas upwards. If the NBG7815 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 WiFi clients.

14.7 OpenVPN Problems

Client devices cannot connect to the NBG7815 server.

- Make sure the NBG7815 is in standard (router) mode.
- Make sure DDNS is enabled in the **Settings > Internet > Dynamic DNS** screen.
- Make sure the OpenVPN Server account is enabled in the **OpenVPN Server > OpenVPN Server** screen.
- Make sure **Advertise DNS to Clients** is enabled in **OpenVPN Server > OpenVPN Server** screen.
- Make sure the VPN client is using a reliable Internet connection.
- Make sure the VPN client is using the correct protocol (TCP/UDP) to connect to the OpenVPN Server.
- Make sure the client connecting to the OpenVPN Server account is using the same port number (default server port number is 1194) to access the server account.
- Make sure the "key" the VPN clients use to access the OpenVPN Server account is correct. If not, export the new .ovpn configuration file and send it to all OpenVPN clients so that they can use the new key.
- Temporarily disable any Internet security and antivirus software installed on the client device. Some Internet security and antivirus products are known to cause interference with VPN connections and should be disabled. Re-enable Internet security and antivirus software after the client device connects to the NBG7815 server.

The NBG7815 client cannot connect to an OpenVPN server.

- Do NOT activate OpenVPN Server and OpenVPN Client at the same time on the NBG7815.
- Try to ping the OpenVPN server.
- Make sure connection to an OpenVPN Server account is enabled in the **OpenVPN Server > OpenVPN Client** screen.
- Make sure the interface through which the NBG7815 connects to an OpenVPN Server account is allowed in the **OpenVPN Server > OpenVPN Client** screen's **Enable VPN on** field.
- Make sure you enter the correct user name and password to connect to the OpenVPN Server account.

14.8 USB File Sharing Problems

I cannot access or see a USB device that is connected to the NBG7815.

- Disconnect the problematic USB device, then reconnect it to the NBG7815.
- Ensure that the USB device has power.
- Check your cable connections.

- Restart the NBG7815 by disconnecting the power and then reconnecting it.
- 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 NBG7815 and try to connect to it again with your computer.
- If the problem persists, contact your vendor.

What kind of USB devices do the NBG7815 support?

- 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 NBG7815.
- The NBG7815 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.

For Zyxel Communication offices, see <https://service-provider.zyxel.com/global/en/contact-us> for the latest information.

For Zyxel Network offices, see <https://www.zyxel.com/index.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
- <https://www.zyxel.com>

Asia

China

- Zyxel Communications (Shanghai) Corp.
- Zyxel Communications (Beijing) Corp.
- Zyxel Communications (Tianjin) Corp.
- <https://www.zyxel.com/cn/zh/>

India

- Zyxel Technology India Pvt Ltd.
- <https://www.zyxel.com/in/en/>

Kazakhstan

- Zyxel Kazakhstan
- <https://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
- <https://www.zyxel.com/tw/zh/>

Thailand

- Zyxel Thailand Co., Ltd.
- <https://www.zyxel.com/th/th/>

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- <https://www.zyxel.com/vn/vi>

Europe

Belarus

- Zyxel BY
- <https://www.zyxel.by>

Bulgaria

- Zyxel България
- <https://www.zyxel.com/bg/bg/>

Czech Republic

- Zyxel Communications Czech s.r.o
- <https://www.zyxel.com/cz/cs/>

Denmark

- Zyxel Communications A/S
- <https://www.zyxel.com/dk/da/>

Finland

- Zyxel Communications
- <https://www.zyxel.com/fi/fi/>

France

- Zyxel France
- <https://www.zyxel.fr>

Germany

- Zyxel Deutschland GmbH
- <https://www.zyxel.com/de/de/>

Hungary

- Zyxel Hungary & SEE
- <https://www.zyxel.com/hu/hu/>

Italy

- Zyxel Communications Italy
- <https://www.zyxel.com/it/it/>

Netherlands

- Zyxel Benelux
- <https://www.zyxel.com/nl/nl/>

Norway

- Zyxel Communications
- <https://www.zyxel.com/no/no/>

Poland

- Zyxel Communications Poland
- <https://www.zyxel.com/pl/pl/>

Romania

- Zyxel Romania

- <https://www.zyxel.com/ro/ro>

Russia

- Zyxel Russia
- <https://www.zyxel.com/ru/ru/>

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- <https://www.zyxel.com/sk/sk/>

Spain

- Zyxel Communications ES Ltd.
- <https://www.zyxel.com/es/es/>

Sweden

- Zyxel Communications
- <https://www.zyxel.com/se/sv/>

Switzerland

- Studerus AG
- <https://www.zyxel.ch/de>
- <https://www.zyxel.ch/fr>

Turkey

- Zyxel Turkey A.S.
- <https://www.zyxel.com/tr/tr/>

UK

- Zyxel Communications UK Ltd.
- <https://www.zyxel.com/uk/en/>

Ukraine

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

South America

Argentina

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

Brazil

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

Colombia

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

Ecuador

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

South America

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

Middle East

Israel

- Zyxel Communications Corporation
- <http://il.zyxel.com/>

North America

USA

- Zyxel Communications, Inc. – North America Headquarters
- <https://www.zyxel.com/us/en/>

APPENDIX B

Setting Up Your Computer's IP Address

Note: The NBG7815 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.

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.

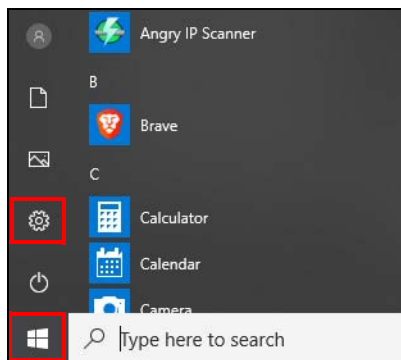
In this appendix, you can set up an IP address for:

- [Windows 10](#) on [page 161](#)
- [macOS: Big Sur 11](#) on [page 165](#)
- [Linux: Ubuntu 20 \(GNOME\)](#) on [page 168](#)
- [Linux: openSUSE 10.3 \(KDE\)](#) on [page 172](#)

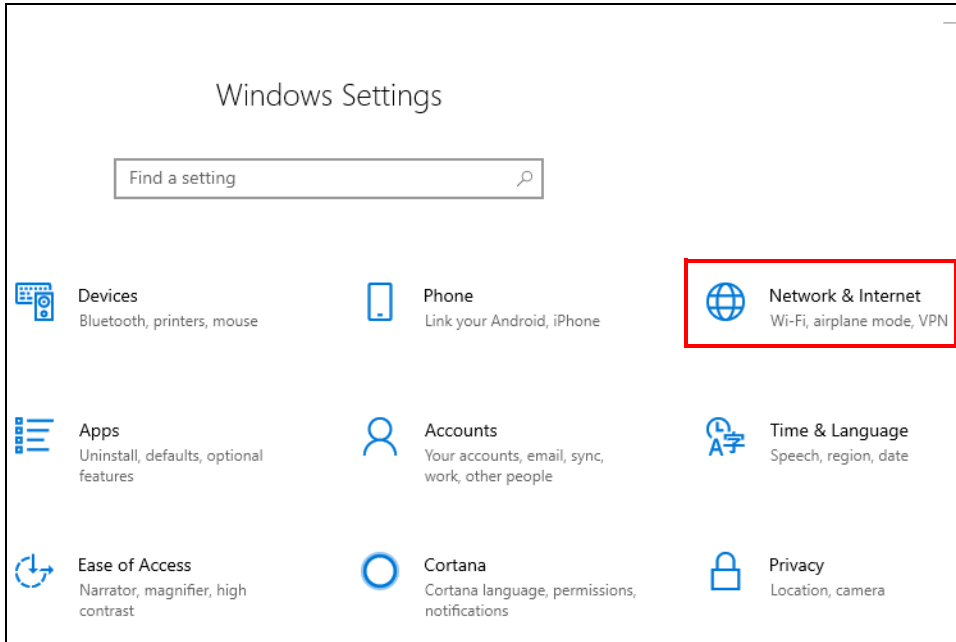
Windows 10

This section shows the screens from Windows 10 Professional.

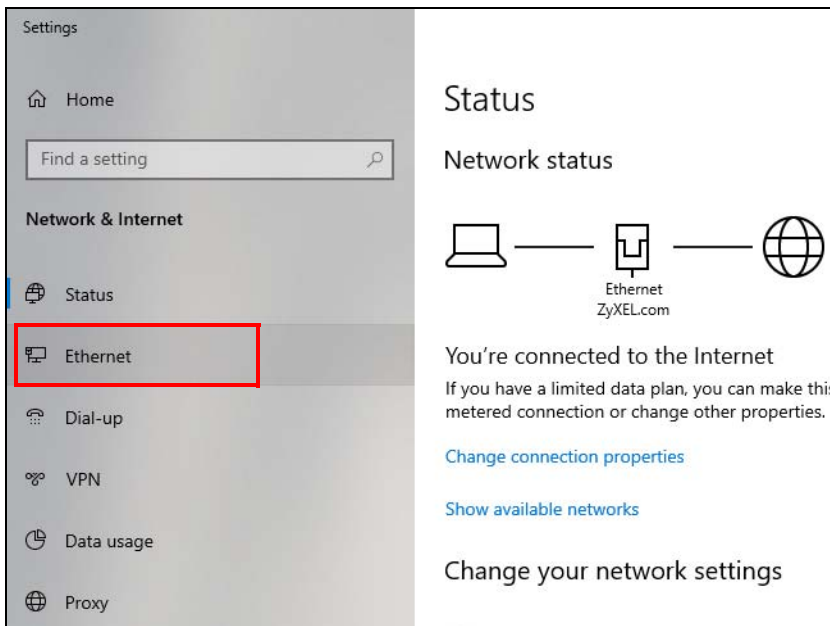
- 1 Click **Start**  > **Settings** .



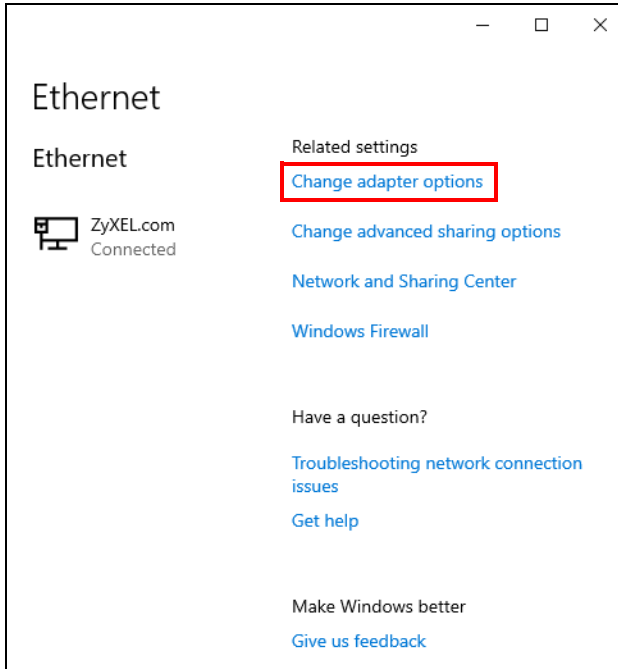
- 2 In the **Windows Settings** panel, click **Network & Internet**.



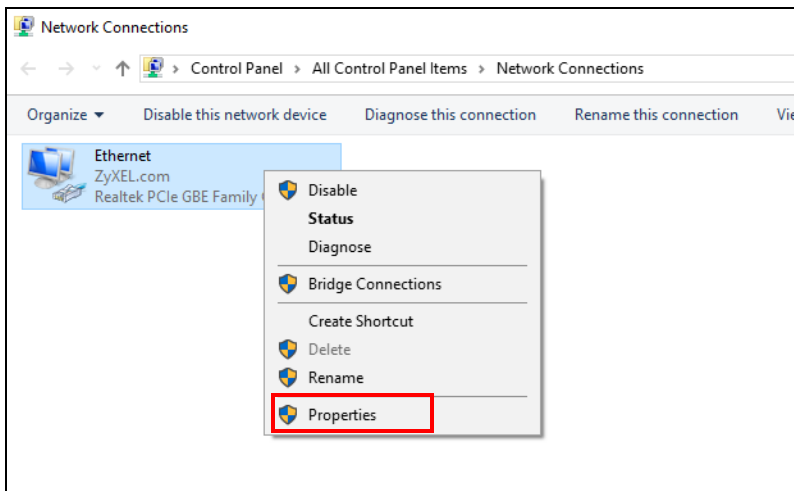
- 3 In the **Network & Internet** panel, click **Ethernet**.



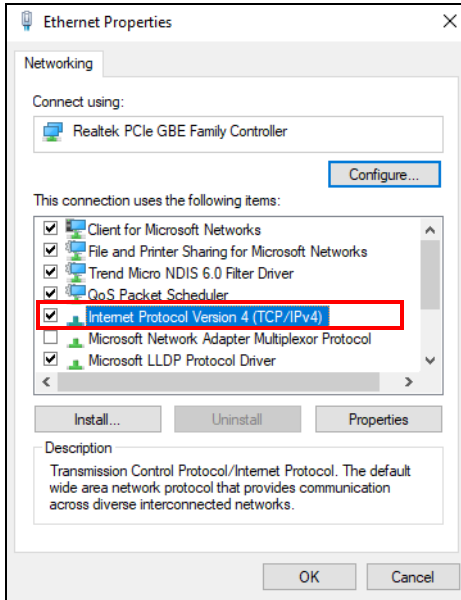
- 4 Click **Change adapter options**. The **Network Connections** panel opens.



- 5 Right-click the Ethernet network you are connected to, then select **Properties**.

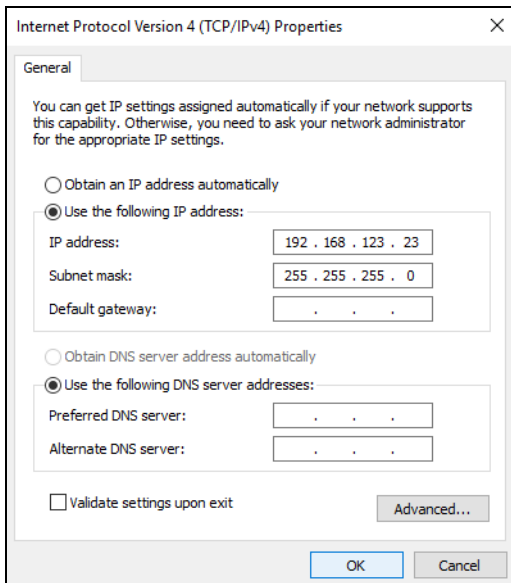


- 6 Double-click **Internet Protocol Version 4 (TCP/IPv4)**.



- 7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens. Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

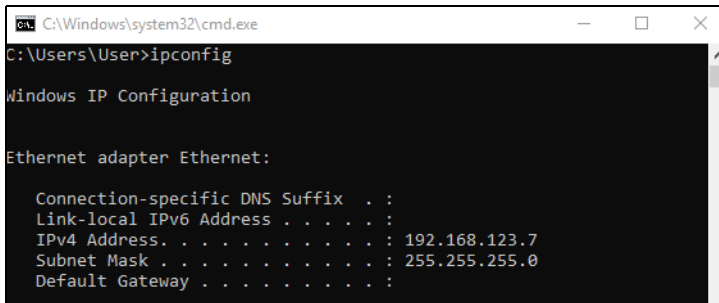
Alternatively, select **Use the following IP address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate 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 Version 4 (TCP/IPv4) Properties** window.
- 9 Click **OK** to close the **Ethernet Properties** window.

Verify the Settings

- 1 Use [Win] + [R] to open the **Run** window.
- 2 Enter "cmd" and click **OK** or press [ENTER] to open the **Command Prompt** window.
- 3 In the **Command Prompt** window, enter "ipconfig" and then press [ENTER].
- 4 The IP settings are displayed as follows.



```
C:\Windows\system32\cmd.exe
C:\Users\User>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . :
    IPv4 Address. . . . . : 192.168.123.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

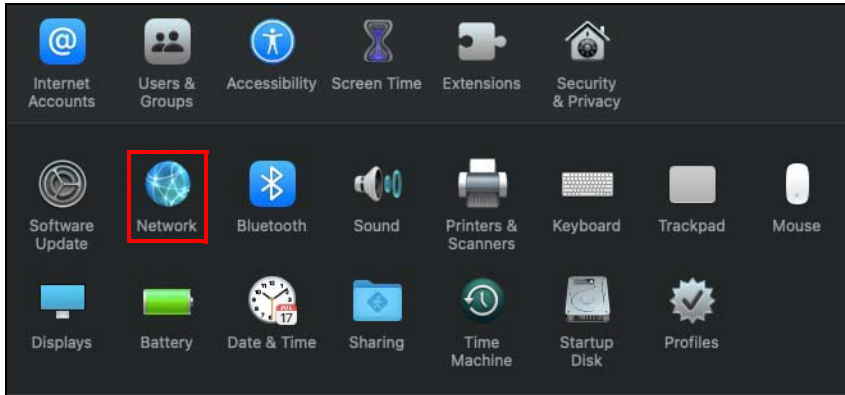
macOS: Big Sur 11

The screens in this section are from macOS Big Sur (v11).

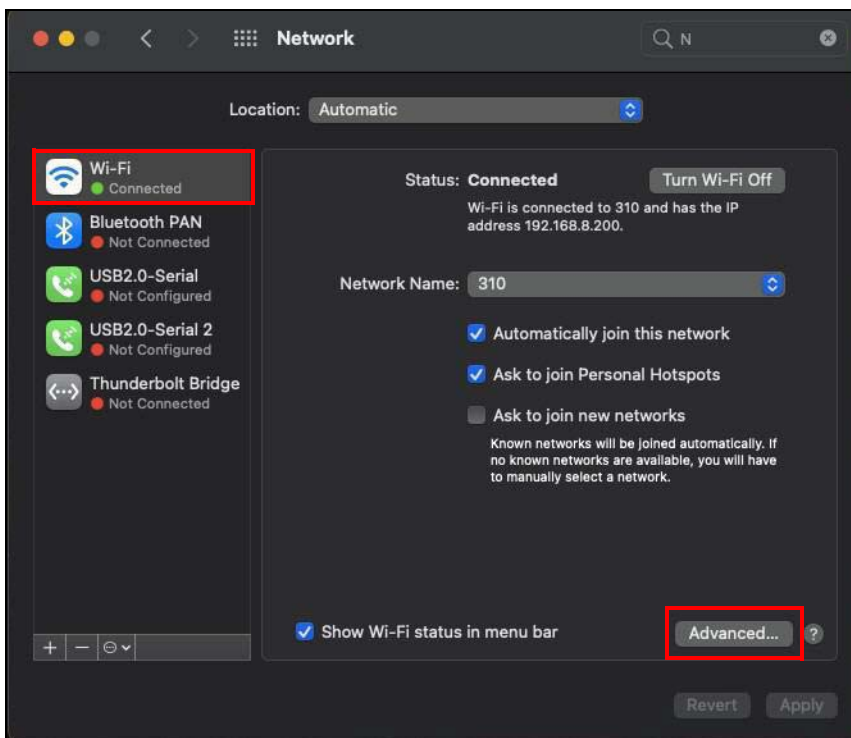
- 1 Click **Apple > System Preferences**.



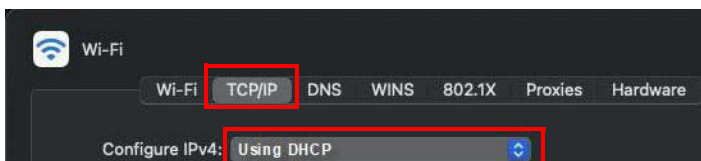
- 2 In the **System Preferences** window, click the **Network** icon.



- 3 The **Network** preferences pane opens. Select the connection type you want to configure from the network connection type list, and then click **Advanced**. Here, we use **Wi-Fi** connection as an example.

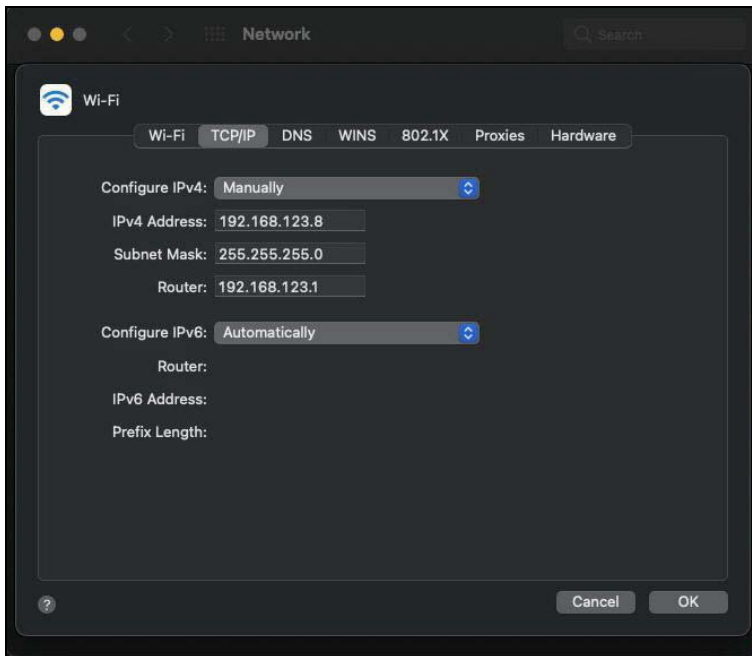


- 4 Select the **TCP/IP** tab to configure IP settings. For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list.



- 5 For statically assigned settings, do the following:
 - From the **Configure IPv4** list, select **Manually**.
 - In the **IP Address** field, enter your IP address.

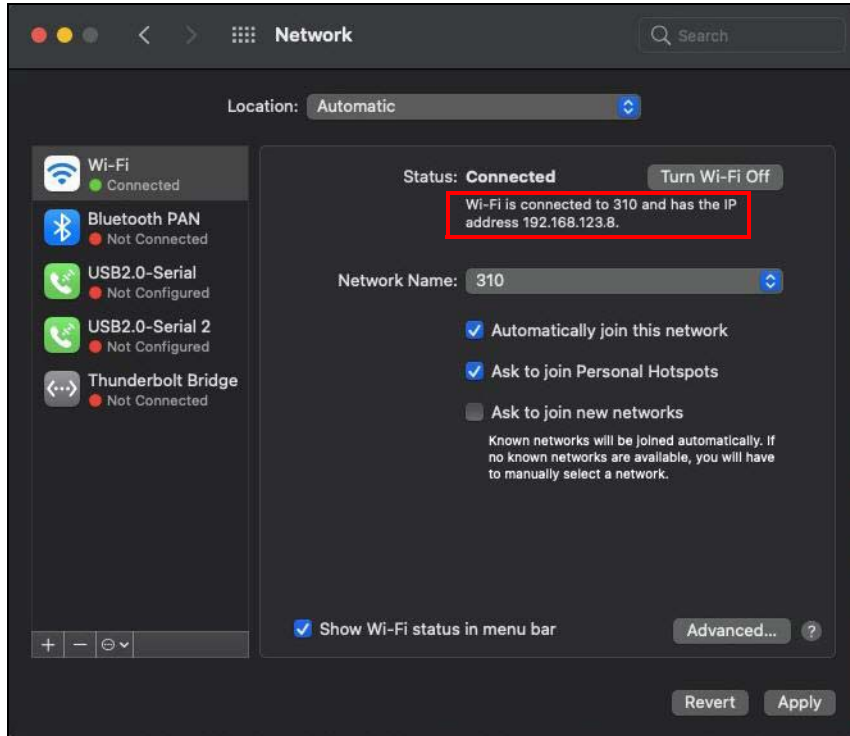
- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your NBG7815.



- 6 Click **OK**.
- 7 Click **Apply** on the **Network** panel to apply the settings.

Verify the Settings

Check your TCP/IP properties by clicking **Apple > System Preferences > Network**, and then selecting the appropriate connection type from the Internet connection list.



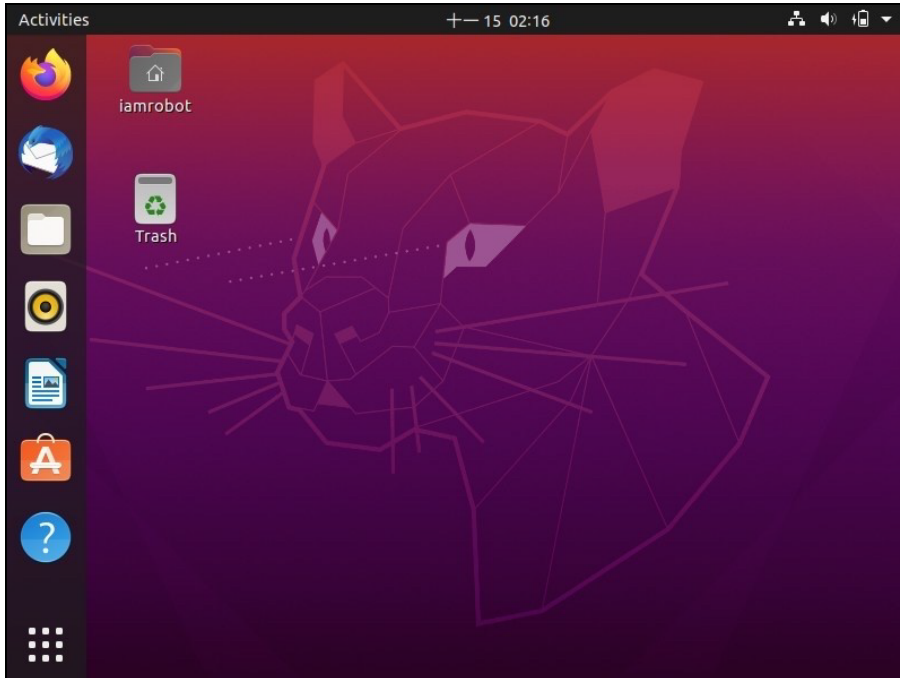
Linux: Ubuntu 20 (GNOME)

This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 20 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.

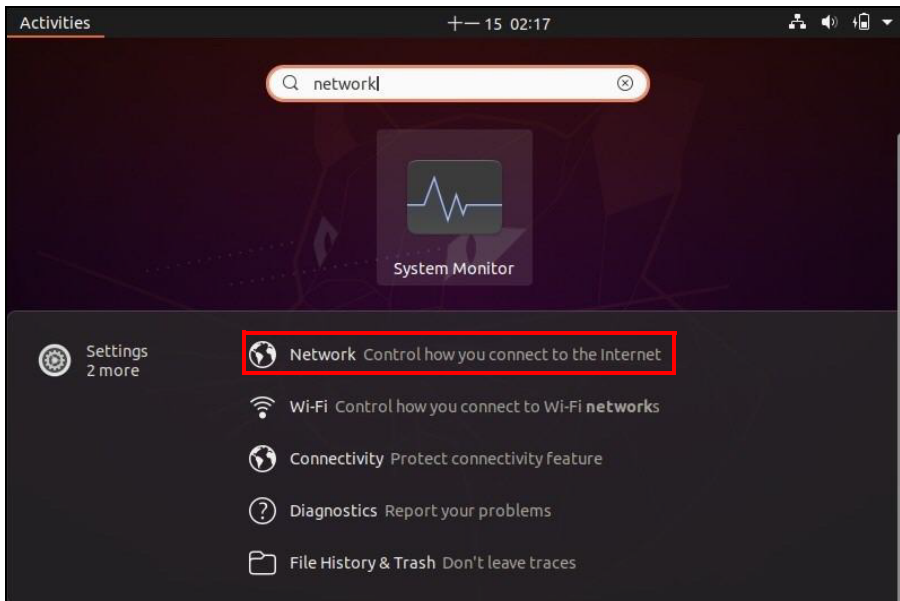
Note: Make sure you are logged in as the root administrator.


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

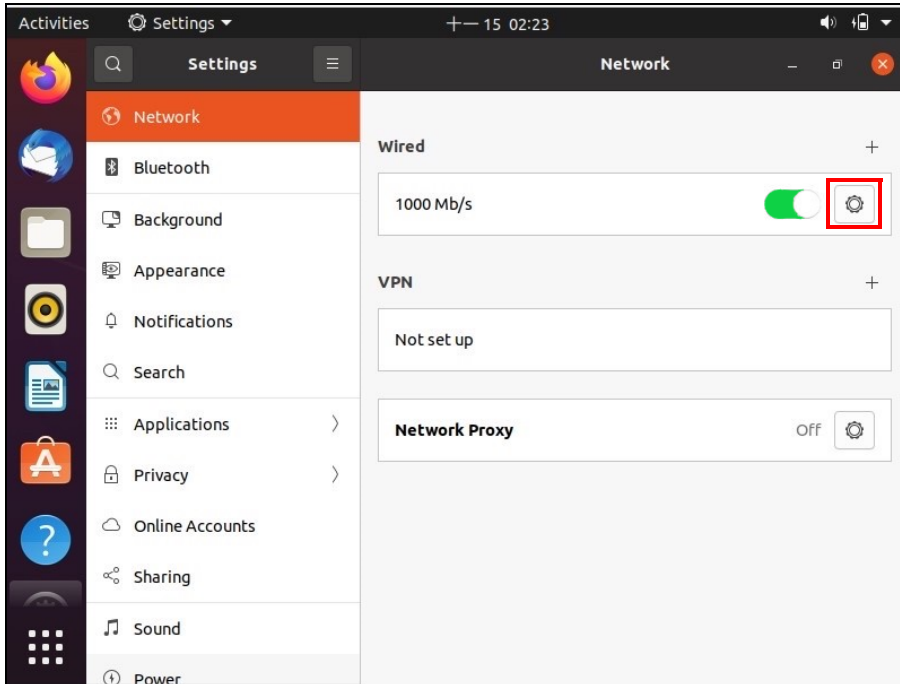
- 1 Click **Activities** (upper left) to open the search panel.



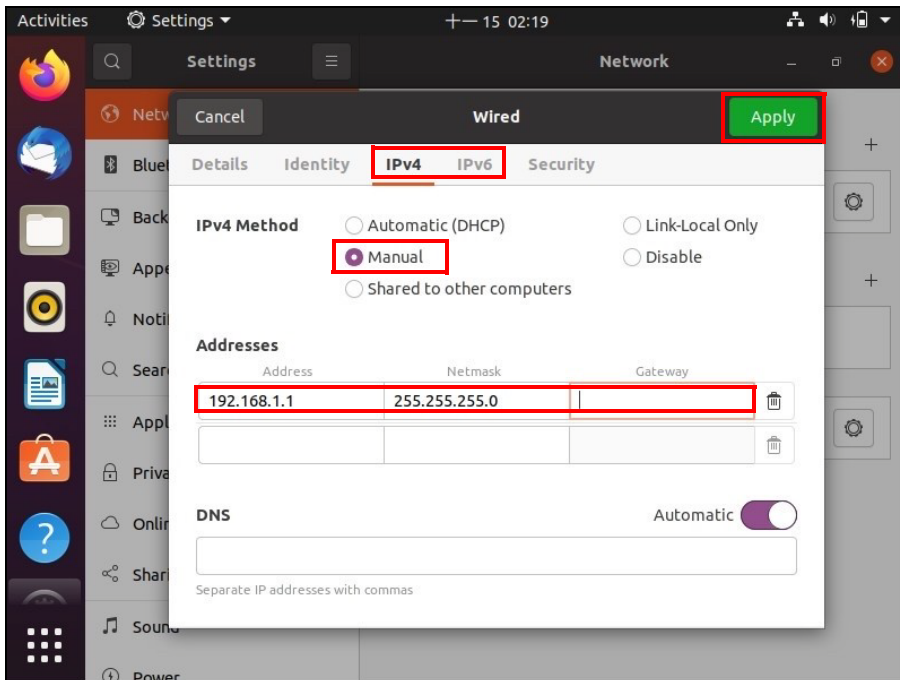
- 2 Enter "network" and the system will display the search results related to "network". Click **Network** to open the **Network** panel.



- 3 Click the settings icon  of the connection you want to configure.



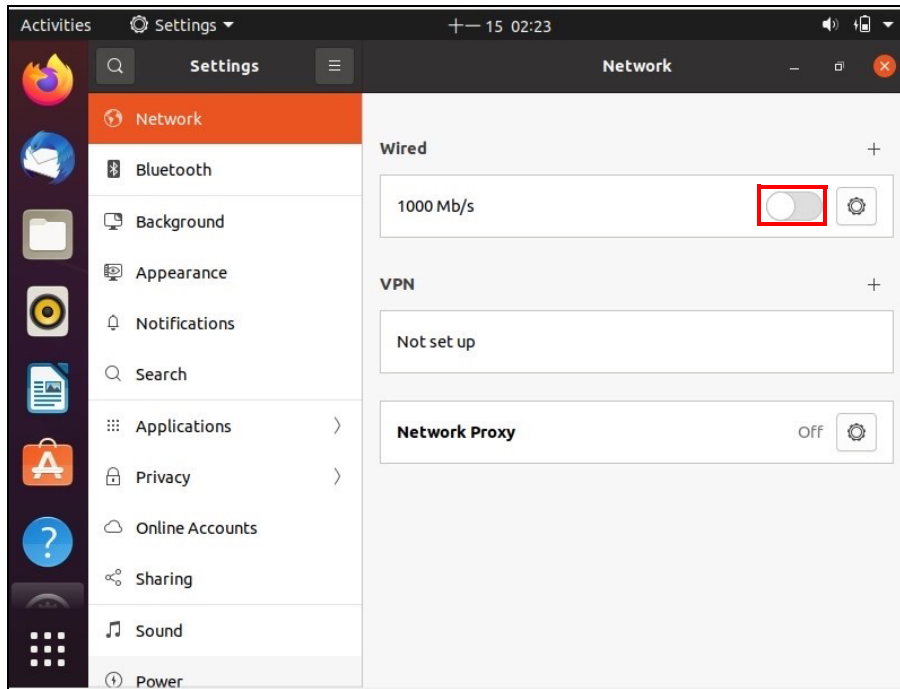
- 4 Click the **IPv4** or **IPv6** tab to configure their settings. In this example, we select **IPv4**.
 - Under **IPv4 Method**, select **Manual** if you have a static IP address. Fill in the **IP Address**, **Netmask**, and **Gateway** address fields. Enter the DNS settings if you know your DNS server IP addresses.
 - Alternatively, select **Automatic (DHCP)** if you are assigned a dynamic IP address.



- 5 Click **Apply** to save the configuration.

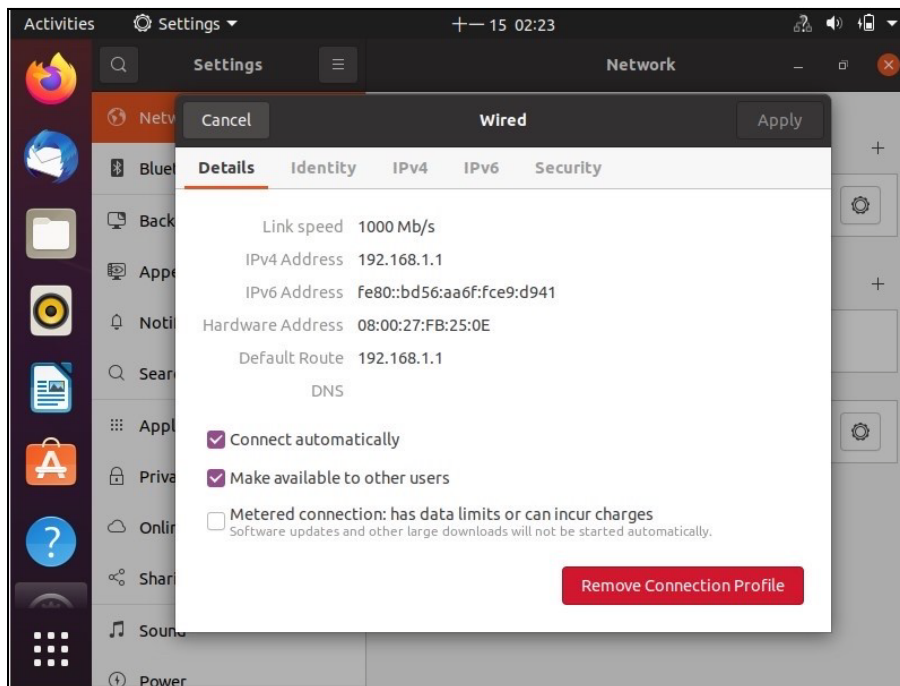
Note: The configuration will be applied after rebooting or connection interface restart.

- 6 To apply the configuration, click the switch to turn off and on to restart the connection interface.



Verify the Settings

Check your TCP/IP properties by opening the connection settings panel and selecting the **Details** tab.



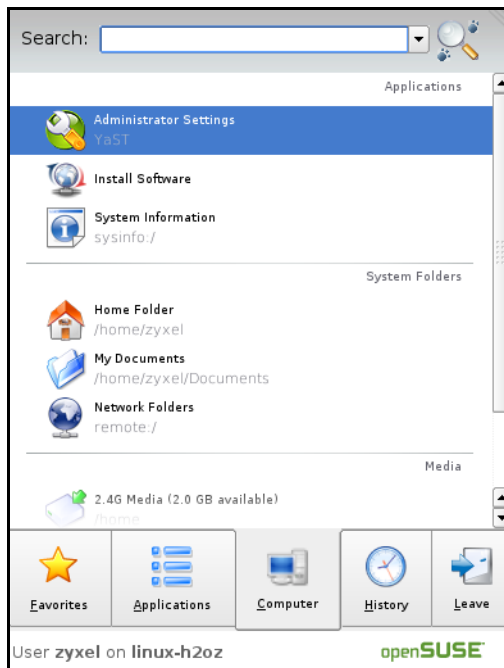
Linux: openSUSE 10.3 (KDE)

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's IP address in KDE:

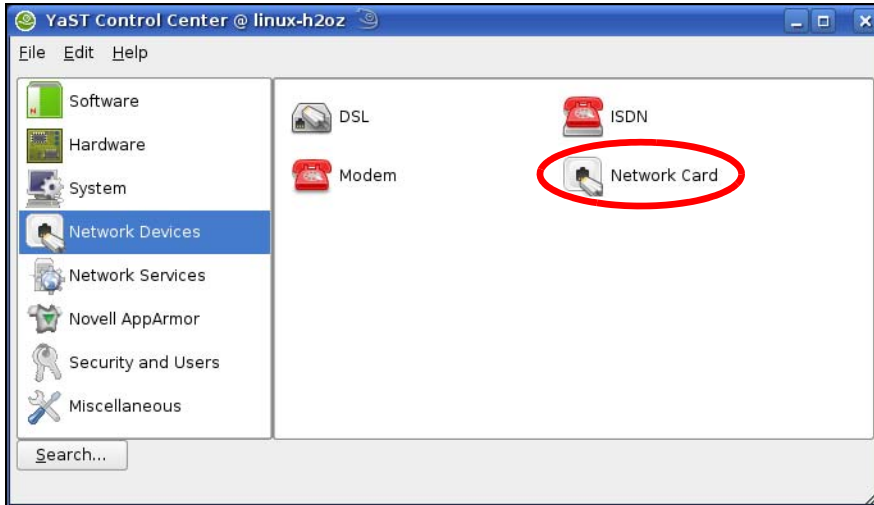
- 1 Click **K Menu > Computer > Administrator Settings (YaST)**.



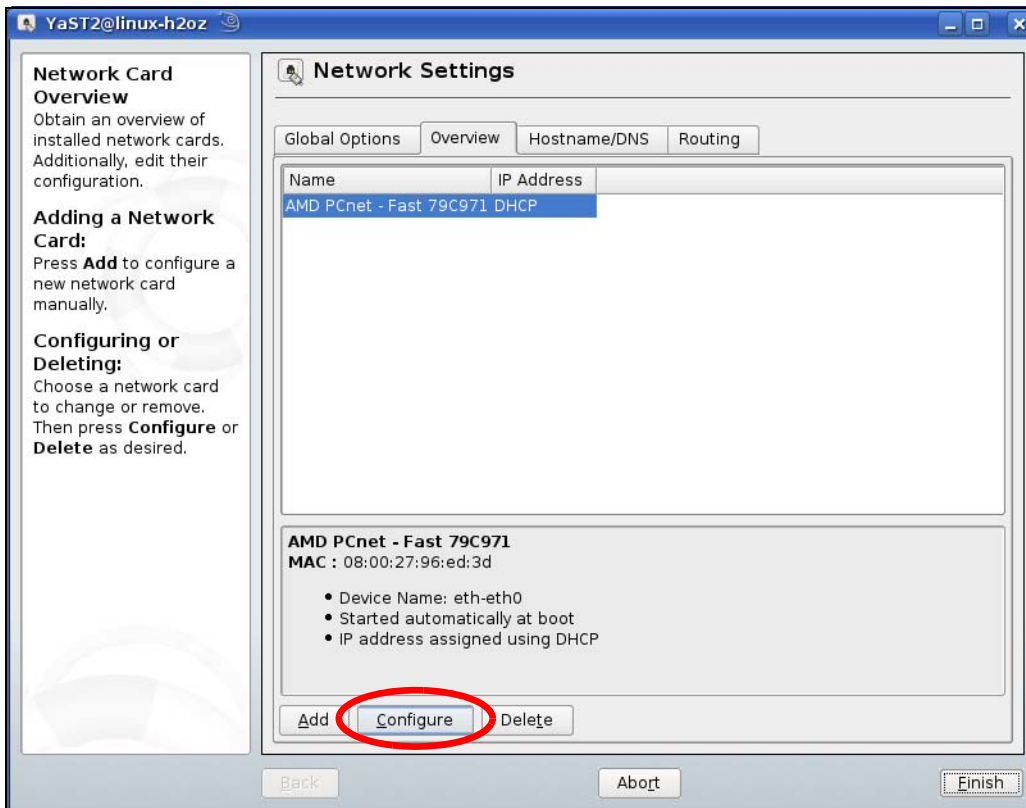
- 2 When the **Run as Root – KDE su** dialog opens, enter the **Administrator Password** and click **OK**.



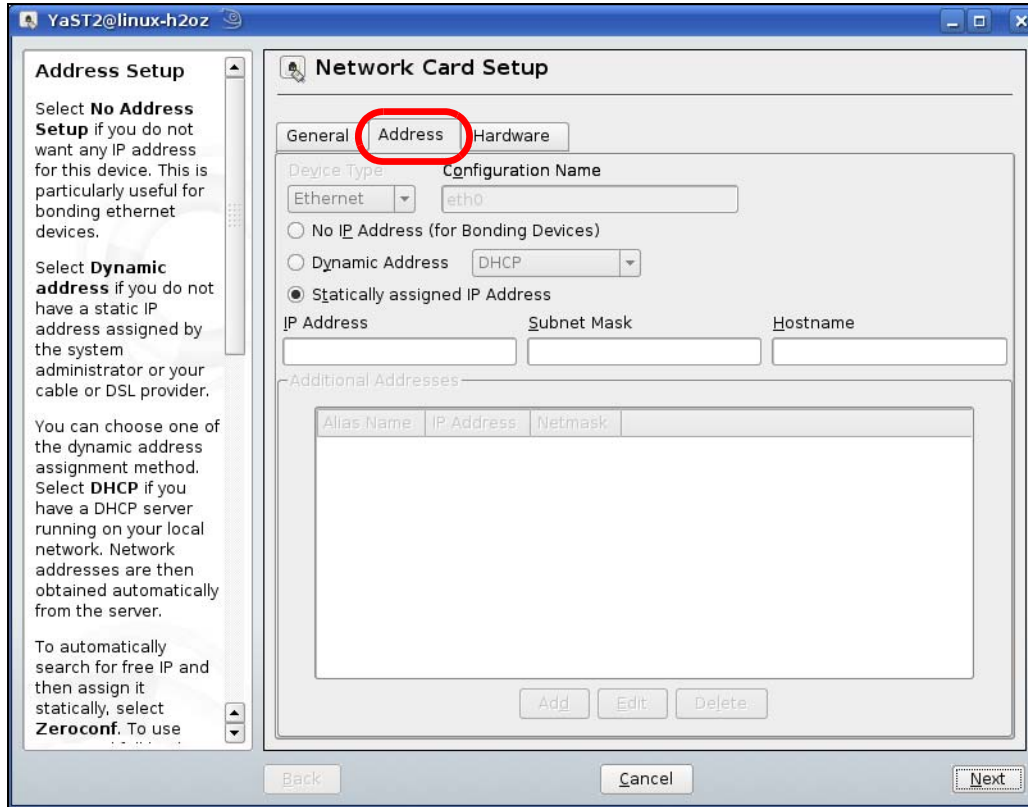
- 3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.



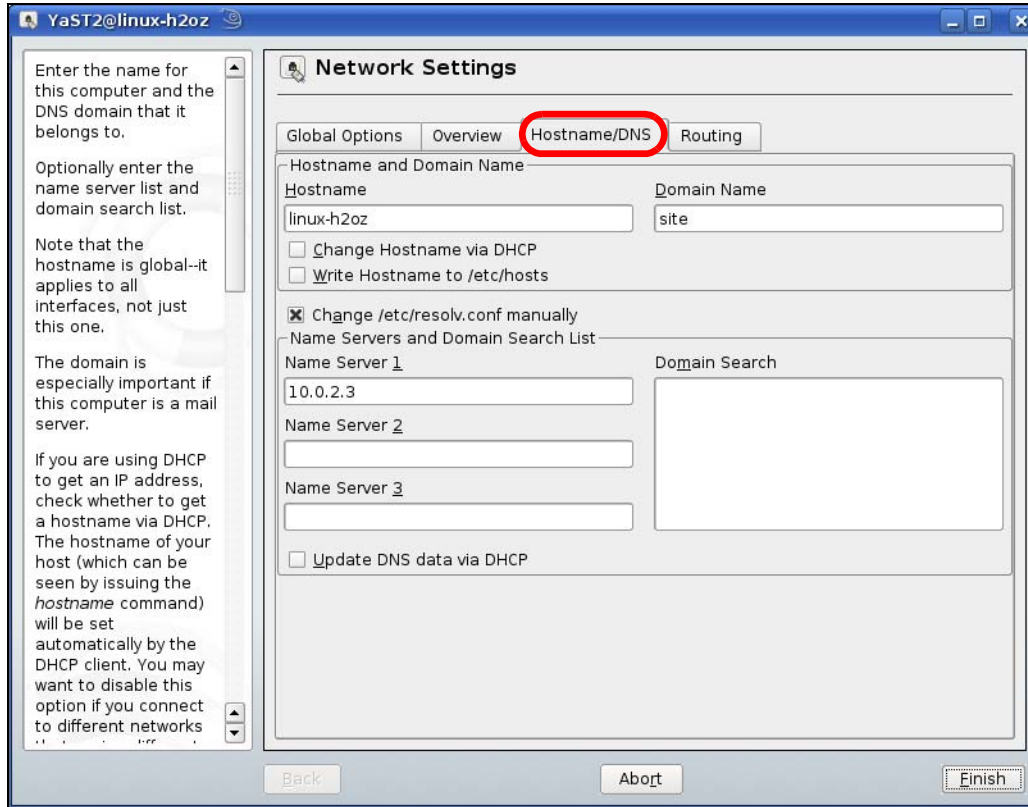
- 4 When the **Network Settings** window opens, click the **Overview** tab. Select the appropriate connection **Name** from the list, and then click the **Configure** button.



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



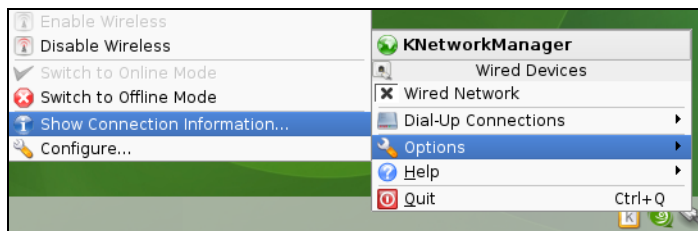
- 6 Select **Dynamic Address (DHCP)** if you are using a dynamic IP address. Alternatively, select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP Address**, **Subnet Mask**, and **Hostname** fields.
- 7 Click **Next** to save the changes and close the **Network Card Setup** window.
- 8 If you know your DNS server IP addresses, click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.



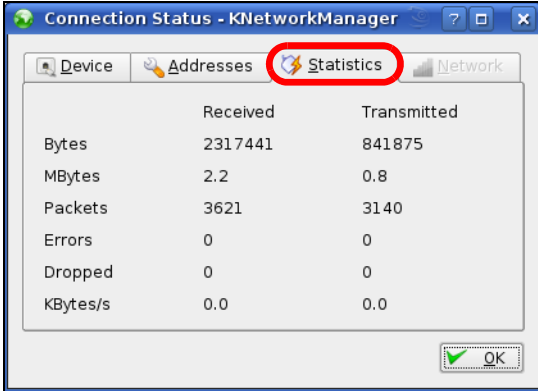
- 9 Click **Finish** to save your settings and close the window.

Verify the 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**.



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



APPENDIX C

Legal Information

Copyright

Copyright © 2022 by Zyxel and/or its affiliates.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel and/or its affiliates.

Published by Zyxel and/or its affiliates. All rights reserved.

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

UNITED STATES of AMERICA



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

US Importer: Zyxel Communications, Inc, 1130 North Miller Street Anaheim, CA92806-2001, <https://www.zyxel.com/us/en/>

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.

EUROPEAN UNION and UNITED KINGDOM



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

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

- Compliance information for wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED) and UK regulation. And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) and United Kingdom without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5 GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5 GHz 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 20 cm 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 99.54 mW,
 - the bands 5,150 MHz to 5,350 MHz is 180.3 mW,
 - the 5,470 MHz to 5,725 MHz is 907.82 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 <ul style="list-style-type: none"> 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 overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. National Restrictions <ul style="list-style-type: none"> 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 seadme vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ ΕΞΟΤΙΣΜΟΣ 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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details. 2.4 GHz frekvenču joslas izmantošanai ārpus telpām nepieciešama atļauja no Elektronisko sakaru direkcijas. Vairāk informācijas: http://www.esd.lv.
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 alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ftiġġiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 2014/53/EU.
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/EU.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/EU.
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, 110 V AC in North America or 230 V 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.
- 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.

Environment Statement

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

- 取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材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。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材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。
- 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。
- 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 is 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 at www.zyxel.com to receive email notices of firmware upgrades and related information.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses.

To request the source code covered under these licenses, please go to: https://www.zyxel.com/form/gpl_oss_software_notice.shtml

Numbers

- 10 Gbps [12](#)
- 10 Gigabit port [12](#)
- 192.168.123.1
 - standard (router) mode IP [62](#)
- 192.168.123.2
 - bridge mode IP [62](#)
- 2.4G network [11](#), [14](#)
- 5G network [11](#), [14](#)
- 6rd
 - IPv6 [87](#)
- 802.11 mode [119](#)

A

- access point (AP) [109](#)
- access schedule
 - parental control [68](#)
- Add FTP Account screen [82](#)
- address assignment [86](#)
- air circulation
 - NBG7815 [23](#)
- ALG [100](#)
 - and NAT [100](#)
 - and security policy [100](#)
- AP [11](#)
- AP Mode
 - menu [63](#)
- AP+Bridge [11](#)
- Application Layer Gateway, see ALG
- applications
 - NBG7815 [12](#)
- ARMOR mobile app [19](#)
- Auto-IP Change [17](#)
 - conditions [18](#)

B

- bandwidth
 - WiFi [37](#)
- bandwidth capacity
 - cable type [12](#)
- Bluetooth
 - LED behavior [21](#)
- bridge mode [18](#), [44](#)
 - default IP address [150](#)
 - select [146](#)
 - set to [61](#)
 - Status screen [62](#)
- bridge mode example [18](#)
- Bridge/Repeater [11](#)
- button
 - reset [20](#)

C

- cable type
 - Ethernet [12](#)
- Cat cable [12](#)
- certifications [179](#)
 - viewing [181](#)
- channel [110](#)
 - WiFi [37](#)
- CIFS [66](#)
- client
 - add to a profile [40](#)
- Common Internet File System, see CIFS
- connection speed
 - check [35](#)
- contact information [156](#)
- cooling the NBG7815
 - desk-mount [23](#)
- copyright [177](#)
- customer support [156](#)

D

- DDNS
 - service providers [135, 137](#)
- DDNS account
 - register at [104](#)
- DDNS settings [104](#)
- desk mounting
 - NBG7815 [19, 21, 23](#)
- DHCP (Dynamic Host Configuration Protocol) [124](#)
- DHCP client [150](#)
- DHCP server [122, 124](#)
- DHCP table [125](#)
- Digital Living Network Alliance [65](#)
- Digital Living Network Alliance (DLNA) [16](#)
- disclaimer [177](#)
- distance maximum
 - cable type [12](#)
- DLNA [65](#)
 - indexing [81](#)
 - overview [16](#)
 - rescan [81](#)
- DLNA-compliant client [65](#)
- DLNA-compliant media server [16, 81](#)
- DNS server [86, 124](#)
- domain name
 - setup [142](#)
- Domain Name System. See DNS
- downstream data rate
 - show [52](#)
- downstream traffic
 - data rate show [36](#)
- dual-band application [14](#)
- dual-band gateway [14](#)
- dual-band WiFi [13](#)
- Dynamic DNS
 - enable first [71](#)
- Dynamic DNS screen [104](#)
- DynDNS [135, 137](#)
- DynDNS see also DDNS [135, 137](#)

E

- encapsulation method [86](#)
- encryption [111](#)
- ESSID [152](#)
- Ethernet port [20](#)
- Ethernet WAN port [20](#)

F

- Facebook icon [31](#)
- FAT32 file system [65](#)
- features
 - supported list [11](#)
- File Allocation Table (FAT) [65](#)
- File Explorer
 - USB application [75](#)
 - use [81](#)
- file server feature [16](#)
- file sharing
 - access right [78, 80](#)
 - bandwidth [80](#)
 - File Explorer [55, 57, 76](#)
 - FTP server [78](#)
 - Samba [55, 57, 76](#)
 - USB [16](#)
 - user account [76, 78](#)
 - work group [55, 57](#)
 - workgroup [76](#)
- file system [65](#)
- File Transfer Protocol (FTP) [66](#)
- files shared
 - access from a computer [81](#)
- FileZilla [82](#)
- filter action [117](#)
- firewall [132](#)
 - guidelines [132](#)
 - ICMP packet [135](#)
 - stateful inspection [131](#)
 - turn off [27](#)
- firewall action
 - default [131](#)
- firewall rule
 - activate [133](#)
- firmware

find online [144](#)
wizard check [30](#)

firmware upgrade
LED [21](#)

FTP [66](#)
ALG [100](#)
USB application [75](#)

FTP (file transfer protocol)
file sharing [16](#)

FTP account
add rule [79](#)

FTP program
use [82](#)

FTP setup [83](#)

G

General Setting screen [141](#)

Google icon [31](#)

guest WiFi [14](#), [111](#)
enable [116](#)

guest WiFi bandwidth [112](#)

Guest WiFi screen [116](#)

H

H.323
ALG [100](#)

HTML5 supported browser [51](#)

http
//(DHCP-assigned IP) [62](#)

HTTP (Hypertext Transfer Protocol) [144](#)

I

IANA (Internet Assigned Number Authority) [134](#)

IEEE 802.11a/b/g/n/ac/ax compliant [13](#)

IEEE 802.3bz [12](#)

Internet access
pause/resume on profile [42](#)
problem [151](#)

Internet access application [13](#)

Internet connection
configure [86](#)
slow or intermittent [152](#)

Internet Connection screen [88](#)

Internet Control Message Protocol (ICMP) [133](#)

Internet Protocol version 6 [15](#)

IP address [124](#)

IP settings
configure on computer [161](#)

ipconfig [150](#)

IPoE encapsulation [88](#)

IPSec connection [102](#)

IPv4 firewall
add rule [134](#)
enable [140](#)

IPv4 Firewall screen [132](#)

IPv4/IPv6 dual stack [15](#)

IPv6 [15](#)
addressing [87](#)
prefix and length [87](#)
subnet mask [87](#)

IPv6 address
abbreviation [87](#)

IPv6 address range [129](#)

IPv6 firewall
add rule [136](#)
enable [140](#)

IPv6 Firewall screen [135](#)

IPv6 LAN screen [128](#)

IPv6 rapid deployment [87](#)

IPv6 rapid deployment (6RD) [15](#)

IPv6 stateless auto-configuration
enable [129](#)

IRC
ALG [100](#)

ISP (Internet Service Provider) [86](#)

J

Java enabled [150](#)

Java permission [51](#)

JavaScript [51](#), [150](#)

L

LAN **121**
 LAN example **121**
 LAN IP screen **122, 126**
 LAN overview **121**
 LAN setup **121**
 language
 select **142**
 LED
 Bluetooth pairing **21**
 description **21**
 firmware upgrade **21**
 reset the NBG7815 **21**
 turn on/off **43**
 WPS in process **21**
 local (user) database **111**
 Local Area Network **121**
 local password
 create **34**
 log message
 view **146**
 Logs screen **146**

M

MAC **117**
 MAC address **86, 110**
 add **118**
 cloning **86**
 MAC address filter **110**
 MAC address filtering **117**
 enable **117**
 MAC address list
 maximum **117**
 MAC filter **117**
 Magic Packet method **143**
 Main WiFi screen **113**
 Maintenance screen **144**
 manage
 NBG7815 **18**
 managing NBG7815
 good habits **19**
 managing the device

 using the Web Configurator. See Web Configurator
 Maximum Transmission Unit (MTU) **93**
 MBSSID **11**
 Media Access Control **117**
 media client **16**
 media file **16, 81**
 play **16**
 type **81**
 media server
 overview **16**
 media server feature **16**
 media sharing
 USB **80**
 Microsoft Point-to-Point Encryption (MPPE) **96**
 mode **11**
 MTU (Maximum Transmission Unit) **90, 96**
 Multi-Gigabit (IEEE 802.3bz) **12**
 multiple servers behind NAT
 example **97**
 Multi-User Multiple-Input, Multiple-Output (MU-MIMO) **115**
 MU-MIMO **115**
 myZyxeCloud account
 create **30**
 myZyxeCloud login **51**

N

NAT
 and ALG **100**
 enable **98**
 navigation panel
 bridge mode **56**
 standard mode **54**
 Web Configurator **53**
 Network Address Translation (NAT) **98**
 New Technology File System (NTFS) **65**

O

OFDMA-enabled WiFi client **115**
 open port **102**
 maximum **102**

OpenSSL encryption library [14](#)

OpenVPN

- configure as client [49](#)
- configure as server [47](#)

OpenVPN account list

- add rule [73](#)

OpenVPN Account List screen [72](#)

OpenVPN Account Status screen [72](#)

OpenVPN application [15](#)

OpenVPN client [73](#)

OpenVPN clients

- maximum connection [72](#)

OpenVPN server [70](#)

OpenVPN server list

- add rule [50, 75](#)

OpenVPN Server/Client [14](#)

operating mode [11](#)

- change [44, 61](#)
- NBG7815 [17](#)

Operating Mode screen [145](#)

operating system

- supported [161](#)

Orthogonal Frequency-Division Multiple Access (OFDMA) [115](#)

P

parental control [66](#)

Passthrough screen [100](#)

password

- change [19](#)
- guest WiFi [116](#)
- main WiFi [115](#)
- myZyxeCloud [51](#)
- set [142](#)

password authentication [83](#)

PBC (Push Button Configuration) method [119](#)

PIN

- WPS [24](#)

PIN (Personal Identification Number) [112](#)

ping [152](#)

Point-to-Point Protocol over Ethernet [91](#)

pop-up window

- web browser [51](#)

port

- Ethernet WAN [20](#)
- LAN [20](#)
- USB [20](#)

port forwarding [97](#)

port forwarding rule [98](#)

- add [99](#)
- configure [45](#)

port trigger [102](#)

- add rule [103](#)
- maximum [102](#)

port trigger process

- example [102](#)

port trigger rule

- maximum [103](#)

power jack [20](#)

PPPoE [91](#)

- dial-up connection

PPPoE encapsulation [91](#)

PPTP encapsulation [94](#)

privilege

- WiFi/wired LAN access [36](#)

profile

- parental control add [68](#)

Profile screen [69](#)

profiling client [40](#)

R

RADIUS server [111](#)

rear panel

- ports [20](#)

Remote Access screen [143](#)

reset

- LED behavior [21](#)
- NBG7815 [23, 152](#)

RESET button [20](#)

reset button [152](#)

Reset hole [23](#)

RESET TO FACTORY DEFAULT button [144](#)

resource unit (RU) [115](#)

restart

- system [144](#)

router mode

status screen [58](#)
RTSP
 ALG [100](#)
rubber feet
 remove for wall-mount [22](#)

S

SAE (Simultaneous Authentication of Equals handshake) [111](#)
Samba [66](#)
SAMBA account
 add rule [77](#)
SAMBA setup [76](#)
schedule
 set for client device [40](#)
scheduling [120](#)
Scheduling screen [120](#)
screen resolution
 minimum recommended [51](#)
screw anchor
 wall mounting [21](#)
screw specifications
 wall mounting [19, 22](#)
security mode
 guest WiFi [39](#)
 select [115, 116](#)
 WiFi [37](#)
security policy
 and ALG [100](#)
security setting
 WiFi network [36](#)
Server Message Block, see SMB
server port number [143](#)
service provider
 Dynamic DNS [105](#)
Service Set [115](#)
Service Set IDentification [115](#)
Service Set IDentity. See SSID.
Session Initiation Protocol (SIP) [100](#)
SIP
 ALG [100](#)
SMB [66](#)
SMB server

 free [66](#)
SNMP
 ALG [100](#)
speed test
 run [35](#)
SSID [110, 115](#)
SSID (Service Set IDentifier) [116](#)
SSLv3/TLSv1 protocol [14](#)
standard (router) mode [17](#)
standard mode [44](#)
 default IP address [150](#)
 select [146](#)
standard mode example [17](#)
stateful inspection firewall [131](#)
Static DHCP table
 add/edit rule [125](#)
status
 bridge mode [140](#)
 standard mode [139](#)
Status screen [58, 62, 138](#)
stream file [16](#)
subnet mask [124](#)
supported features [11](#)
system
 general setup [141](#)
system restart [144](#)

T

TCP port 7547 [102](#)
Telnet
 access the NBG7815 [151](#)
transmission range
 WiFi [153](#)
transmission speed
 cable type [12](#)
transport layer protocol
 select [100](#)
trigger port [102](#)

U

unique local address (ULA) [130](#)

- Universal Plug and Play (UPnP) [105](#)
 - UPnP
 - activate in Windows 10 example [106](#)
 - UPnP setup [106](#)
 - upstream data rate
 - show [52](#)
 - upstream traffic
 - data rate show [36](#)
 - USB file sharing [16](#)
 - USB hard drive [16](#)
 - USB media sharing [16](#)
 - USB Media Sharing screen [80](#)
 - USB memory stick [16](#)
 - USB port [20](#)
 - USB storage device
 - supported [155](#)
 - user authentication [111](#)
 - local (user) database [111](#)
 - RADIUS server [111](#)
 - user name
 - myZyxeCloud [51](#)
- ## V
- virtual private network (VPN) [66](#)
 - VoIP pass through
 - see also ALG
 - VPN [66](#)
 - VPN client
 - example [74](#)
 - VPN passthrough [101](#)
 - VPN protocol
 - OpenVPN [14](#)
 - VPN server
 - example [70](#)
 - maximum connection [74](#)
- ## W
- Wake On LAN (WoL) [143](#)
 - wall mounting
 - information [21](#)
 - NBG7815 [21](#)
 - WAN (Wide Area Network) [85](#)
 - WAN information [140](#)
 - WAN IP address [86](#)
 - WAN MAC address [86](#)
 - warranty
 - note [182](#)
 - Web Configurator [18](#)
 - access in bridge mode [62](#)
 - how to access [51](#)
 - overview [51](#)
 - WiFi
 - dual-band [13](#)
 - WiFi adapter [153](#)
 - WiFi channel [152](#)
 - WiFi connection
 - optimize speed and quality [153](#)
 - slow or intermittent [153](#)
 - WiFi interference
 - factors [153](#)
 - WiFi name
 - configure [37](#)
 - setup [28](#)
 - WiFi network
 - basic guidelines [110](#)
 - channel [110](#)
 - configure [36](#)
 - encryption [111](#)
 - example [109](#)
 - MAC address filter [110](#)
 - overview [109](#)
 - security [110](#)
 - SSID [110](#)
 - WiFi password
 - setup [28](#)
 - WiFi Protected Setup (WPS) [24, 112](#)
 - WiFi schedule
 - configure for profile [40](#)
 - WiFi scheduling [120](#)
 - WiFi security [110, 119, 152](#)
 - overview [110](#)
 - type [110](#)
 - WiFi security setting [153](#)
 - WiFi tutorial [35](#)
 - WiFi5 (802.11ac) [115](#)
 - WiFi6 (802.11ax) [115](#)
 - Windows Media Player [16](#)

- wireless LAN [152](#)
- wizard
 - accessing [25](#)
 - overview [25](#)
- workgroup [65](#)
 - name [65](#)
 - Windows [65](#)
- WPA-PSK (WiFi Protected Access-Pre-Shared Key) [111](#)
- WPS
 - activate [24](#)
- WPS (WiFi Protected Setup) [14](#)
- WPS button
 - in Web Configurator [24](#)
- WPS in process
 - LED [21](#)
- WPS screen [118](#)
- WPS-aware WiFi station [119](#)