



ARMOR Z2

AC2600 MU-MIMO Wireless Gigabit Router

Model: NBG6817

Version 1.00
Edition 1, 06/2016

User's Guide

Default Login Details

LAN IP Address	http://192.168.1.1 (Router Mode) http://192.168.1.2 (Access Point Mode)
Password	1234

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

Related Documentation

- Quick Start Guide

The Quick Start Guide shows how to connect the NBG6817 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 NBG6817.



Contents Overview

User's Guide	9
Introduction	10
Introducing the Web Configurator	15
eaZy 123 Wizard	18
NBG6817 Modes	27
Easy Mode	28
Router Mode	36
Access Point Mode	42
Tutorials	49
Technical Reference	59
Status	60
WAN	73
Wireless LAN	94
LAN	114
Applications	119
Security	143
Maintenance	149
Troubleshooting	163

Table of Contents

Contents Overview	3
Table of Contents	4
Part I: User's Guide	9
Chapter 1	
Introduction.....	10
1.1 Overview	10
1.2 Applications	10
1.3 Ways to Manage the NBG6817	10
1.4 Good Habits for Managing the NBG6817	11
1.5 Resetting the NBG6817	11
1.5.1 How to Use the RESET Button	11
1.6 The WPS Button	11
1.7 LEDs	12
Chapter 2	
Introducing the Web Configurator	15
2.1 Overview	15
2.2 Accessing the Web Configurator	15
2.2.1 Login Screen	16
2.2.2 Change Default Password Screen	16
Chapter 3	
eaZy 123 Wizard.....	18
3.1 Overview	18
3.2 Accessing the eaZy 123 Wizard	18
3.3 Internet Type	20
3.3.1 WAN Selection Type: Automatic - DHCP	21
3.3.2 WAN Selection Type: PPPoE	21
3.3.3 WAN Selection Type: Static	22
3.4 Wireless Network	23
Chapter 4	
NBG6817 Modes	27
4.1 Overview	27
4.1.1 Web Configurator Modes	27

4.1.2 Device Modes	27
Chapter 5	
Easy Mode	28
5.1 Overview	28
5.2 What You Can Do	28
5.3 What You Need to Know	29
5.4 Navigation Panel	29
5.5 Network Map	30
5.6 Control Panel	31
5.6.1 Wi-Fi	32
5.6.2 Guest Wi-Fi	33
5.6.3 Parental Control	34
5.6.4 Notification	35
5.6.5 LED	35
Chapter 6	
Router Mode	36
6.1 Overview	36
6.2 Router Mode Status Screen	36
6.2.1 Navigation Panel	39
Chapter 7	
Access Point Mode	42
7.1 Overview	42
7.2 What You Can Do	42
7.3 What You Need to Know	42
7.3.1 Setting your NBG6817 to AP Mode	43
7.3.2 Accessing the Web Configurator in Access Point Mode	43
7.3.3 Configuring your WLAN and Maintenance Settings	44
7.4 AP Mode Status Screen	44
7.4.1 Navigation Panel	46
7.5 LAN Screen	46
Chapter 8	
Tutorials	49
8.1 Overview	49
8.2 Set Up a Wireless Network Using WPS	49
8.2.1 Push Button Configuration (PBC)	49
8.2.2 PIN Configuration	50
8.3 Connect to NBG6817 Wireless Network without WPS	51
8.3.1 Configure Your Notebook	53
8.4 Using Guest SSIDs on the NBG6817	55

8.4.1 Configuring Security Settings of Guest SSIDs56

Part II: Technical Reference..... 59

**Chapter 9
Status 60**

9.1 Overview 60
 9.1.1 What You Can Do 60
 9.2 Live Network Monitor Screen 60
 9.3 Usage Monitor Screens 63
 9.3.1 Internet Data Usage Monitor 63
 9.3.2 Bandwidth History 64
 9.3.3 Time Tracker 66
 9.3.4 Data Usage Alert 66
 9.4 Common Usage Screen 69
 9.5 Download Traffic Statistics Screen 70
 9.6 Client Tables Screen 71

**Chapter 10
WAN 73**

10.1 Overview 73
 10.2 What You Can Do 73
 10.3 What You Need To Know 73
 10.3.1 Configuring Your Internet Connection 74
 10.4 Internet Connection Screen 76
 10.4.1 IPoE Encapsulation 76
 10.4.2 PPPoE Encapsulation 81
 10.4.3 PPTP Encapsulation 85
 10.5 NAT 88
 10.5.1 General Screen 88
 10.5.2 Port Trigger Screen 90
 10.5.3 Passthrough Screen 90
 10.6 Dynamic DNS Screen 92

**Chapter 11
Wireless LAN..... 94**

11.1 Overview 94
 11.1.1 What You Can Do 95
 11.1.2 What You Should Know 95
 11.2 Wireless Screen 99
 11.3 Wireless Security 101

11.3.1 No Security	101
11.3.2 WPA-PSK/WPA2-PSK	102
11.3.3 WPA/WPA2	103
11.4 Guest Wireless Screen	105
11.4.1 Guest Wireless Edit	106
11.5 MAC Filter Screen	108
11.6 Advanced Screen	109
11.7 WPS Screen	110
11.8 Scheduling Screen	112
Chapter 12	
LAN	114
12.1 Overview	114
12.2 What You Can Do	114
12.3 What You Need To Know	114
12.4 LAN IP Screen	115
12.5 Static DHCP Screen	116
12.6 IPv6 LAN Screen	117
Chapter 13	
Applications	119
13.1 Overview	119
13.1.1 What You Can Do	119
13.1.2 What You Need To Know	119
13.1.3 Before You Begin	121
13.2 Parental Control	121
13.2.1 General Screen	121
13.2.2 Notification Screen	125
13.3 Bandwidth Management	127
13.3.1 Bandwidth Screen	128
13.3.2 Priorities Screen	129
13.4 USB Media Sharing Screen	130
13.5 UPnP Screen	132
13.6 File Sharing	133
13.6.1 SAMBA Server Screen	133
13.6.2 FTP Server Screen	135
13.6.3 Example of Accessing Your Shared Files From a Computer	136
13.7 ONE Connect Screen	140
13.8 Technical Reference	141
Chapter 14	
Security.....	143
14.1 Overview	143

14.1.1 What You Can Do	143
14.1.2 What You Need To Know	143
14.2 IPv4 Firewall Screen	144
14.3 IPv6 Firewall Screen	146
Chapter 15	
Maintenance	149
15.1 Overview	149
15.2 What You Can Do	149
15.3 General Screen	149
15.4 Password Screen	150
15.5 Time Screen	151
15.6 Firmware Upgrade Screen	153
15.7 Backup/Restore Screen	154
15.8 Restart Screen	155
15.9 Language Screen	155
15.10 Remote Management Screen	156
15.10.1 Remote Access	156
15.10.2 Wake On LAN	158
15.11 Log Screen	159
15.12 System Operation Mode Overview	160
15.13 Operation Mode Screen	161
Chapter 16	
Troubleshooting.....	163
16.1 Overview	163
16.2 Power, Hardware Connections, and LEDs	163
16.3 NBG6817 Access and Login	164
16.4 Internet Access	165
16.5 Resetting the NBG6817 to Its Factory Defaults	167
16.6 Wireless Connections	167
16.7 USB Device Problems	169
Appendix A Customer Support	170
Appendix B Setting Up Your Computer's IP Address	176
Appendix C Common Services.....	196
Appendix D Legal Information	199
Index	208

PART I

User's Guide

Introduction

1.1 Overview

This chapter introduces the main features and applications of the NBG6817.

The NBG6817 extends the range of your existing wired network without additional wiring, providing easy network access to mobile users. You can set up a wireless network with other IEEE 802.11a/b/g/n/ac compatible devices. The NBG6817 is able to function both 2.4GHz and 5GHz networks at the same time.

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

There are two USB ports on the side panel of your NBG6817. One is USB 2.0, and the other is USB 3.0. You can connect USB memory sticks, USB hard drives, or USB devices for file sharing. The NBG6817 automatically detects the USB devices.

1.2 Applications

You can have the following networks with the NBG6817:

- **Wired.** You can connect network devices via the Ethernet ports of the NBG6817 so that they can communicate with each other and access the Internet.
- **Wireless.** Wireless clients can connect to the NBG6817 to access network resources. You can use WPS (Wi-Fi Protected Setup) to create an instant network connection with another WPS-compatible device.
- **WAN.** Connect to a broadband modem/router for Internet access.

1.3 Ways to Manage the NBG6817

Use any of the following methods to manage the NBG6817.

- **WPS (Wi-Fi Protected Setup).** You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your NBG6817.
- **Web Configurator.** This is recommended for everyday management of the NBG6817 using a (supported) web browser.

1.4 Good Habits for Managing the NBG6817

Do the following things regularly to make the NBG6817 more secure and to manage the NBG6817 more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the NBG6817 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG6817. You could simply restore your last configuration.

1.5 Resetting the NBG6817

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **RESET** button at the back of the NBG6817 to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to "1234" and the IP address will be reset to "192.168.1.1".

1.5.1 How to Use the RESET Button

- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for one to four seconds to restart/reboot the NBG6817.
- 3 Press the **RESET** button for longer than five seconds to set the NBG6817 back to its factory-default configurations.

1.6 The WPS Button

Your NBG6817 supports Wi-Fi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the Wi-Fi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

You can use the WPS button on the rear panel of the NBG6817 to activate WPS in order to quickly set up a wireless network with strong security.

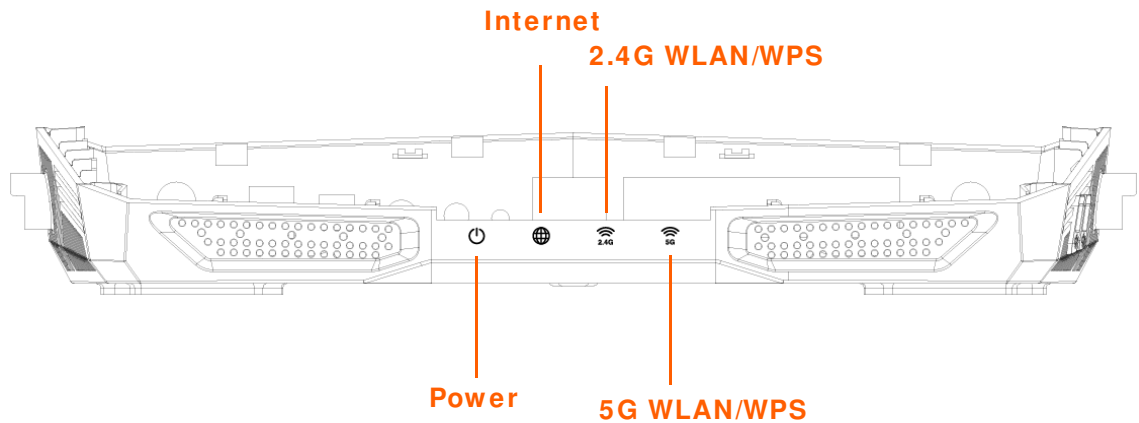
- 1 Make sure the power LED is on (not blinking).
- 2 Press the WPS button for more than three seconds and release it. Press the WPS button on another WPS-enabled device within range of the NBG6817.

Note: You must activate WPS in the NBG6817 and in another wireless device within two minutes of each other.

For more information on using WPS, see [Section 8.2 on page 49](#).

1.7 LEDs

Figure 1 Front Panel



The following table describes the front panel LEDs.

Table 1 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
Power/System	White	On	The NBG6817 is receiving power and functioning properly.
		Blinking	The NBG6817 is in the process of starting up, default restoring, or My ZyXEL Cloud Server online registration pairing.
		Off	The NBG6817 is not receiving power.
Internet	White	On	The NBG6817 has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the connection is up.
		Blinking	The NBG6817 is sending or receiving IP traffic.
		Off	The NBG6817 does not have an IP connection.

Table 1 Front Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
5G WLAN/WPS	White	On	The NBG6817 is ready and the 5GHz wireless LAN is on, but is not sending/receiving data through the wireless LAN.
		Blinking	The NBG6817 is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
	Amber	On	WPS is enabled. The NBG6817 is in the process of firmware upgrading, configuration restoring, or resetting.
		Blinking	The NBG6817 is negotiating a WPS connection with a wireless client.
		Off	WPS is disabled.
2.4G WLAN/WPS	White	On	The NBG6817 is ready and the 2.4GHz wireless LAN is on, but is not sending/receiving data through the wireless LAN.
		Blinking	The NBG6817 is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
	Amber	On	WPS is enabled. The NBG6817 is in the process of firmware upgrading, configuration restoring, or resetting.
		Blinking	The NBG6817 is negotiating a WPS connection with a wireless client.
		Off	WPS is disabled.

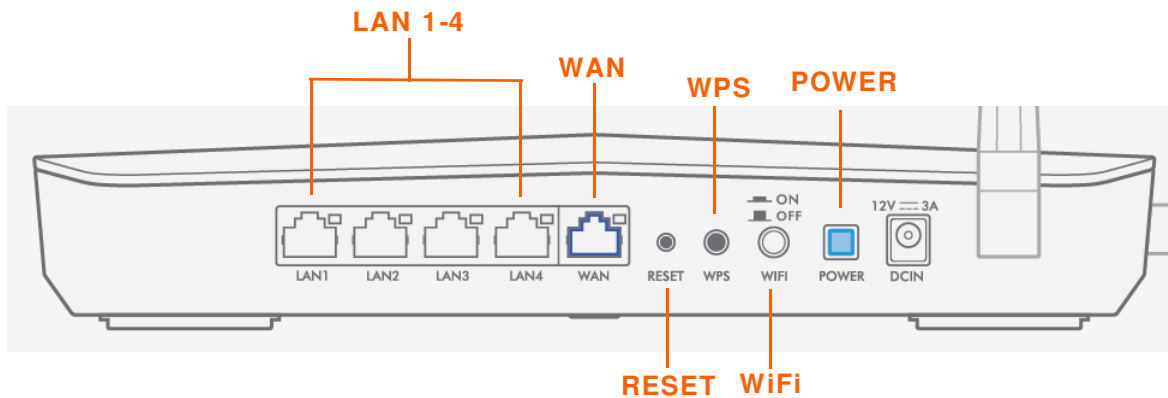
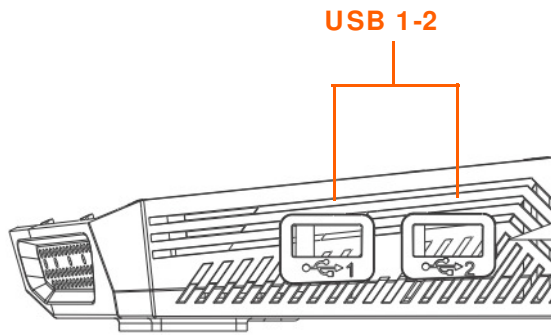
Figure 2 Rear Panel

Figure 3 Side Panel



Introducing the Web Configurator

2.1 Overview

This chapter describes how to access the NBG6817 Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the NBG6817 via Internet browser. Use a browser that supports HTML5, such as Internet Explorer 9.0 and later versions, Mozilla Firefox 21 and later versions, Safari 6.0 and later versions or Google Chrome 26.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows 7.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter ([Chapter 16 on page 163](#)) to see how to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

- 1 Make sure your NBG6817 hardware is properly connected and prepare your computer or computer network to connect to the NBG6817 (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 The NBG6817 is in router mode by default. Type "http://192.168.1.1 or http://myrouter" as the website address. If the NBG6817 obtains a WAN IP address or a DNS server IP address in the same subnet as the LAN IP address 192.168.1.1, the default LAN IP address will be changed to 10.0.0.1 automatically. See [Auto-IP Change on page 75](#) for more information.

If the NBG6817 is in access point, the IP address is 192.168.1.2. See [Chapter 4 on page 27](#) for more information about the modes of the NBG6817.

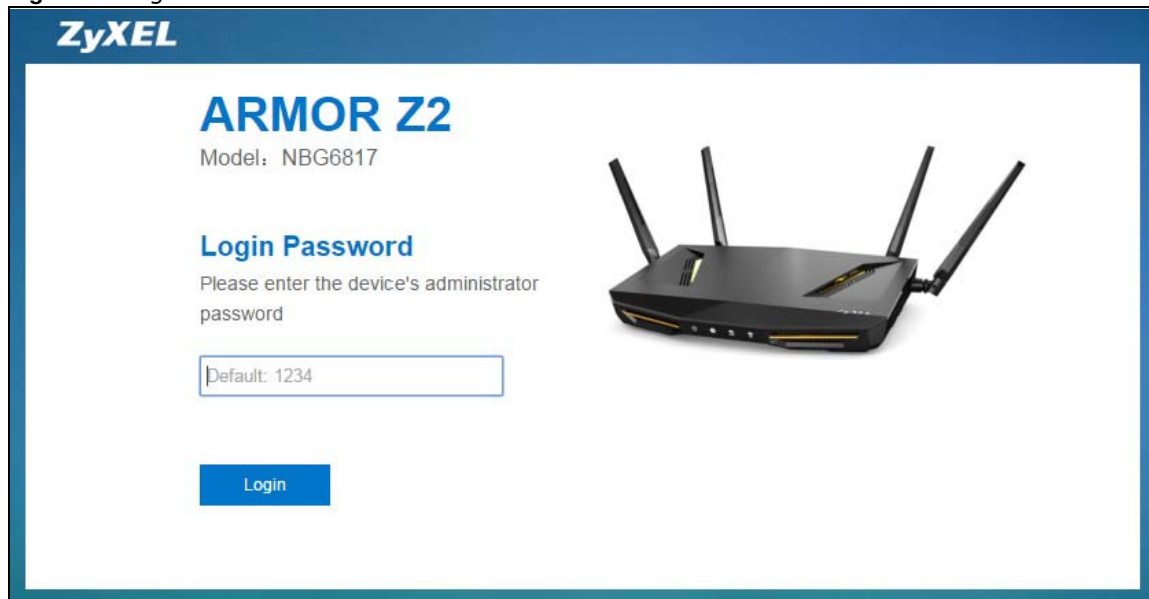
Your computer must be in the same subnet in order to access this website address.

2.2.1 Login Screen

Note: If this is the first time you are accessing the Web Configurator, you may be redirected to the eaZy123 wizard. Refer to [Chapter 3 on page 18](#) for the eaZy123 setup screens.

The Web Configurator initially displays the following login screen.

Figure 4 Login screen



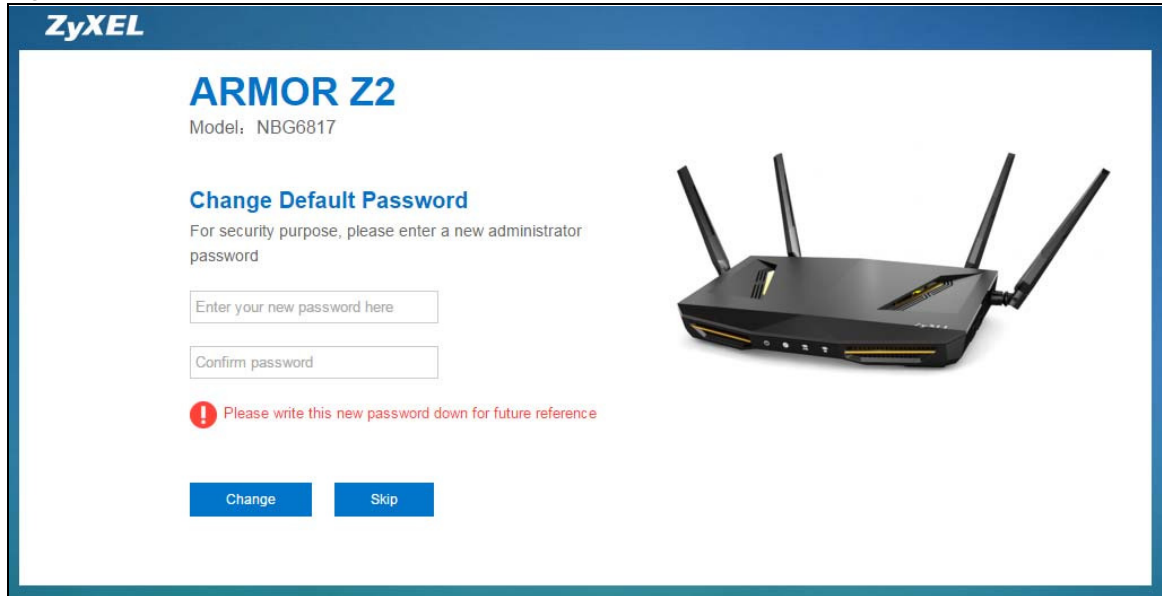
The following table describes the labels in this screen.

Table 2 Login screen

LABEL	DESCRIPTION
Password	Type "1234" (default) as the password. Click Login .

2.2.2 Change Default Password Screen

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

Figure 5 Change Default Password Screen

The following table describes the labels in this screen.

Table 3 Change Default Password Screen

LABEL	DESCRIPTION
Enter your new password here	Type a new password.
Confirm password	Retype the password for confirmation.
Skip	Click Skip if you do not want to change the password this time.
Change	Click Change to save your changes back to the NBG6817.

Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes; go to [Chapter 15 on page 149](#) to change this). Simply log back into the NBG6817 if this happens.

eaZy 123 Wizard

3.1 Overview


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

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

3.2 Accessing the eaZy 123 Wizard

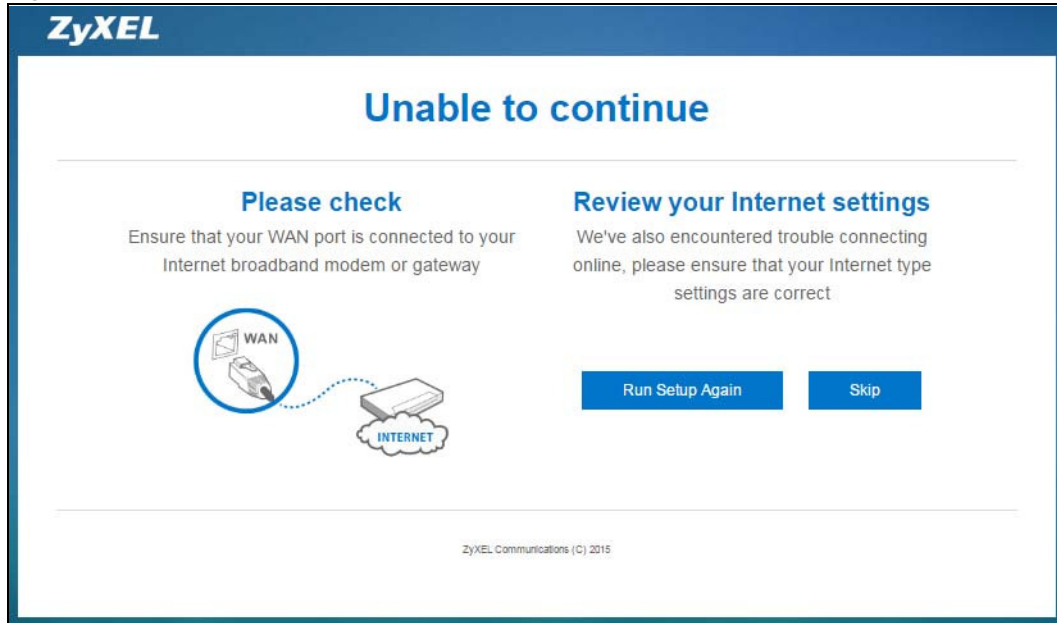
Launch your web browser and type "http://192.168.1.1 or http://myrouter" as the website address. Type "1234" (default) as the password and click **Login**.

Note: The eaZy 123 wizard appears automatically when the NBG6817 is accessed for the first time or when you reset the NBG6817 to its default factory settings. If you didn't configure the wizard screens, you will be redirected to the login page when you connect to the Internet.

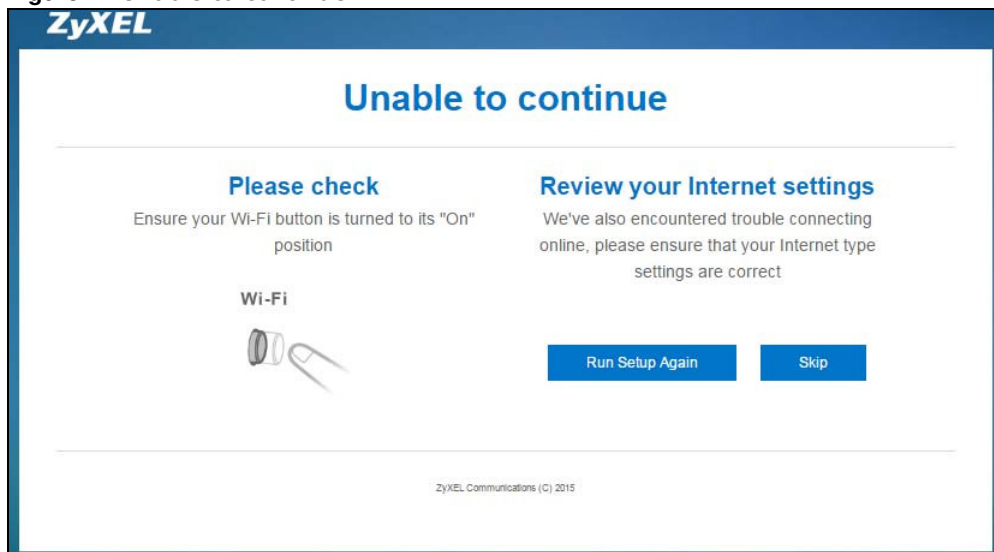
If you have already configured the wizard screens and want to open it again, click  on the upper right corner of any Web Configurator screen. The eaZy 123 wizard attempts to detect which WAN connection type you are using.

If the eaZy 123 wizard does not detect a connection type, you must select one from the drop-down list box. Check with your ISP to make sure you use the correct type.

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

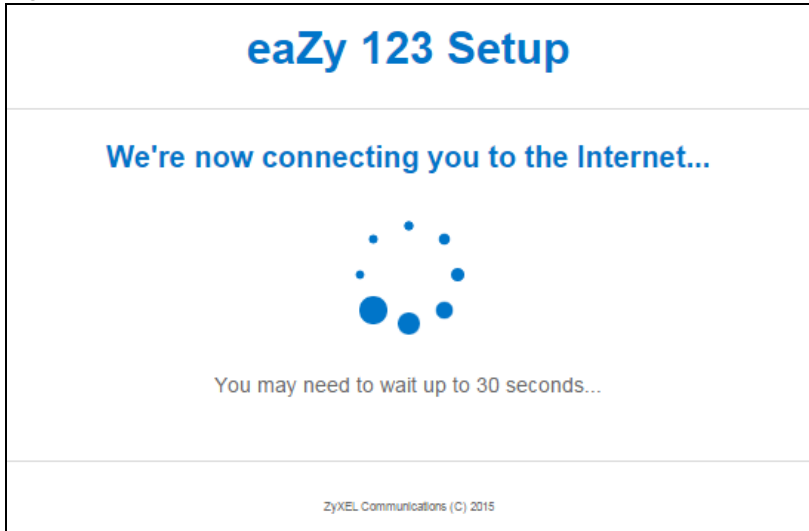
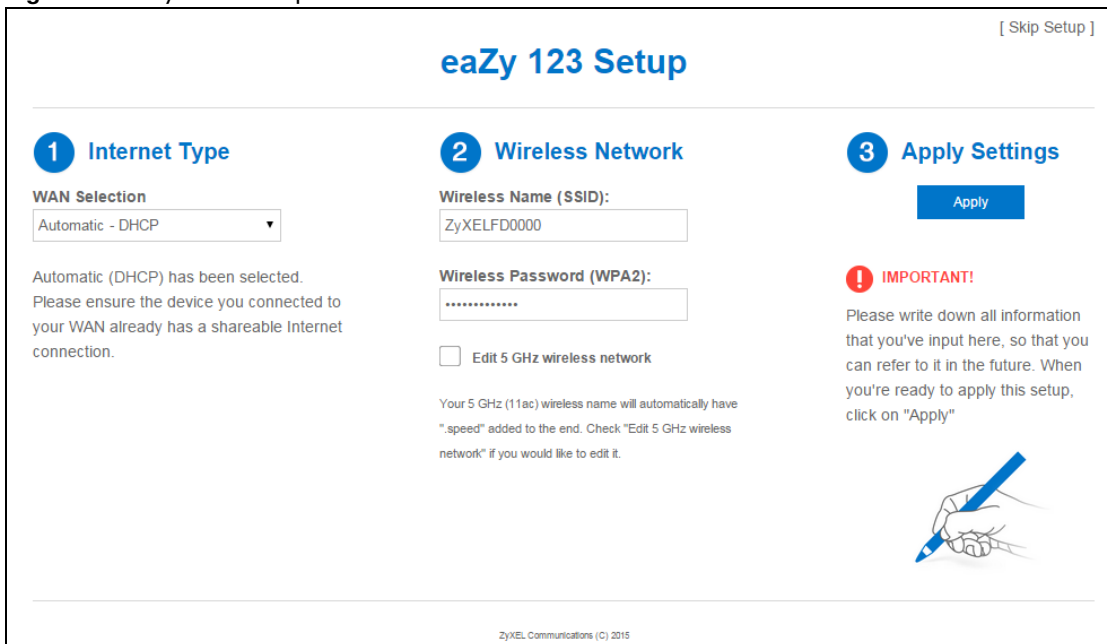
Figure 6 Unable to continue: WAN

If you do not press the Wi-Fi button located on the NBG6817's back panel, the following screen opens.

Figure 7 Unable to continue: Wi-Fi

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

The wizard screen opens.

Figure 8 Detecting your Internet Connection Type**Figure 9** eaZy 123 Setup

3.3 Internet Type

The NBG6817 offers three WAN selection types. They are **Automatic - DHCP**, **PPPoE** or **Static**. Configure the Internet type settings on your NBG6817 in the first part. The following screen depends on your Internet connection type. Enter the details provided by your Internet Service Provider (ISP) in the fields (if any).

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

3.3.1 WAN Selection Type: Automatic - DHCP

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

Figure 10 WAN Selection Type: Automatic - DHCP

The screenshot shows the 'eaZy 123 Setup' wizard with three steps: 1. Internet Type, 2. Wireless Network, and 3. Apply Settings. Step 1 is highlighted with a blue box. In Step 1, the 'WAN Selection' dropdown menu is set to 'Automatic - DHCP'. Below the dropdown, it states: 'Automatic (DHCP) has been selected. Please ensure the device you connected to your WAN already has a shareable Internet connection.' Step 2 shows 'Wireless Name (SSID)' as 'ZyXELFD0000' and 'Wireless Password (WPA2)' as a masked field. Step 3 has an 'Apply' button and an 'IMPORTANT!' warning: 'Please write down all information that you've input here, so that you can refer to it in the future. When you're ready to apply this setup, click on "Apply"'. A hand holding a pen is shown writing on a notepad. The ZyXEL logo and copyright notice are at the bottom.

3.3.2 WAN Selection Type: PPPoE

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

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

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

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

By implementing PPPoE directly on the NBG6817 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG6817 does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Figure 11 WAN Selection Type: PPPoE

[Skip Setup]

eaZy 123 Setup

1 Internet Type

WAN Selection

PPPoE

PPPoE Username:

yourname@isp.com

PPPoE Password:

yourisp-password

Static IP (Optional):

123.123.123.123

Please input your PPPoE username and password. This information is provided by your Internet Service Provider. Usually this Internet type is for DSL users.

2 Wireless Network

Wireless Name (SSID):

ZyXELFD0000

Wireless Password (WPA2):

.....

Edit 5 GHz wireless network

5 GHz Wireless Name (SSID):

ZyXELFD0000.speed

5 GHz Wireless Password (WPA2):

.....

Your 5 GHz (11ac) wireless name will automatically have ".speed" added to the end. Check "Edit 5 GHz wireless network" if you would like to edit it.

3 Apply Settings

Apply

! IMPORTANT!

Please write down all information that you've input here, so that you can refer to it in the future. When you're ready to apply this setup, click on "Apply"

ZyXEL Communications (C) 2015

The following table describes the labels in this screen.

Table 4 WAN Selection Type: PPPoE

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

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

3.3.3 WAN Selection Type: Static

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

Figure 12 WAN Selection Type: Static

[Skip Setup]

eaZy 123 Setup

1 Internet Type

WAN Selection

Static

IP Address:

123.123.123.123

Subnet mask:

255.255.255.0

Gateway IP Address (Optional):

8.8.8.8

DNS Server:

8.8.8.8

Please input your static IP information. This information is provided by your Internet Service Provider.

2 Wireless Network

Wireless Name (SSID):

ZyXELBADB06

Wireless Password (WPA2):

.....

Edit 5 GHz wireless network

5 GHz Wireless Name (SSID):

ZyXELBADB06.speed

5 GHz Wireless Password (WPA2):

.....

Your 5 GHz (11ac) wireless name will automatically have ".speed" added to the end. Check "Edit 5 GHz wireless network" if you would like to edit it.

3 Apply Settings

Apply

IMPORTANT!

Please write down all information that you've input here, so that you can refer to it in the future. When you're ready to apply this setup, click on "Apply"

ZyXEL Communications (C) 2016

The following table describes the labels in this screen.

Table 5 WAN Selection Type: Static

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

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

3.4 Wireless Network

Configure the wireless network settings on your NBG6817 in the second part. The default wireless security setting is WPA2-PSK.

Figure 13 Wireless Network

[Skip Setup]

eaZy 123 Setup

1 Internet Type

WAN Selection
PPPoE

PPPoE Username:
yourname@isp.com

PPPoE Password:
yourisp-password

Static IP (Optional):
123.123.123.123

Please input your PPPoE username and password. This information is provided by your Internet Service Provider. Usually this Internet type is for DSL users.

2 Wireless Network

Wireless Name (SSID):
ZyXELFD0000

Wireless Password (WPA2):
.....

Edit 5 GHz wireless network

5 GHz Wireless Name (SSID):
ZyXELFD0000.speed

5 GHz Wireless Password (WPA2):
.....

Your 5 GHz (11ac) wireless name will automatically have "speed" added to the end. Check "Edit 5 GHz wireless network" if you would like to edit it.

3 Apply Settings

Apply

! IMPORTANT!

Please write down all information that you've input here, so that you can refer to it in the future. When you're ready to apply this setup, click on "Apply"

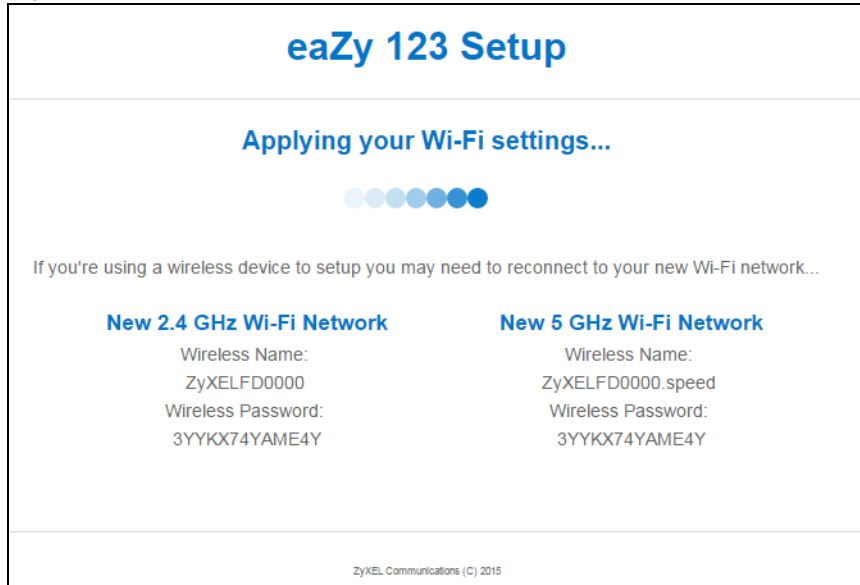
ZyXEL Communications (C) 2015

The following table describes the labels in this screen.

Table 6 Wireless Network

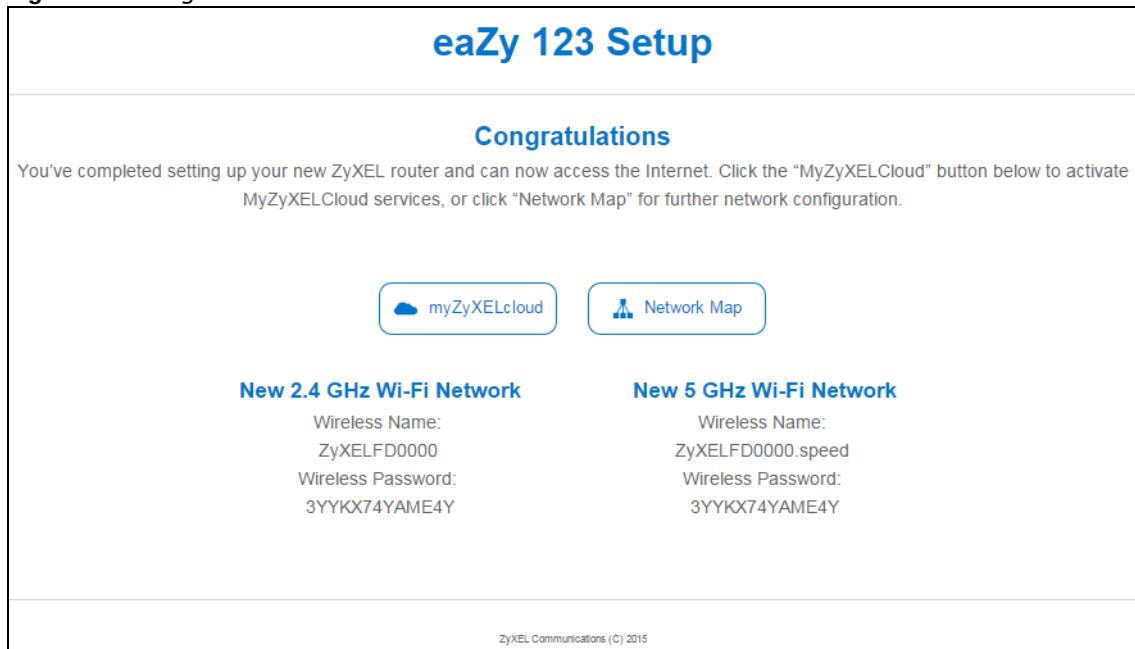
LABEL	DESCRIPTION
Wireless Name (SSID)	Enter a descriptive name for the wireless LAN. Note: The setting here applies to 2.4 GHz wireless radios. If you change this field on the NBG6817, make sure all wireless stations use the same SSID in order to access the network.
Wireless Password (WPA2)	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the wireless LAN screens.
Edit 5 GHz wireless network	Select this check box to configure different SSID and wireless security settings for the NBG6817's 5 GHz wireless network. If you do not select this option, the NBG6817 uses the same SSID and Wi-Fi key (you configured above) for the 5 GHz wireless network.
5GHz Wireless Name (SSID)	Enter a descriptive name for the wireless LAN. If you change this field on the NBG6817, make sure all wireless stations use the same SSID in order to access the network.
5GHz Wireless Password (WPA2)	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the wireless LAN screens.

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

Figure 14 Apply your Wi-Fi settings

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

Note: If you cannot access the Internet when your computer is connected to one of the NBG6817's LAN ports, check your connections. Then turn the NBG6817 off, wait for a few seconds then turn it back on. If that does not work, log in to the web configurator again and check you have typed all information correctly. See the User's Guide for more suggestions.

Figure 15 Congratulations

You can click the **My ZyXEL Cloud Service** button to go to <https://mycloud.zyxel.com>, where you can create an account and register your NBG6817. At the time of writing, you can have free DDNS

service to get a domain name mapped to the NBG6817's dynamic IP address. With DDNS, you can use the domain name to remotely access the NBG6817's Web Configurator through the Internet.

You have successfully set up your NBG6817 to operate on your network and access the Internet.

NBG6817 Modes

4.1 Overview

This chapter introduces the different modes available on your NBG6817. First, the term “mode” refers to two things in this User’s Guide.

- **Web Configurator mode.** This refers to the Web Configurator interface you want to use for editing NBG6817 features.
- **Device mode.** This is the operating mode of your NBG6817, or simply how the NBG6817 is being used in the network.

4.1.1 Web Configurator Modes

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

- **Easy:** The Web Configurator shows this mode by default. Refer to [Chapter 5 on page 28](#) for more information on the screens in this mode. This interface may be sufficient for users who just want to use the device.
- **Expert:** Advanced users can change to this mode to customize all the functions of the NBG6817. Click > **Expert Mode** after logging into the Web Configurator. The User’s Guide [Chapter 9 on page 60](#) through [Chapter 15 on page 161](#) discusses the screens in this mode.

4.1.2 Device Modes

This refers to the operating mode of the NBG6817, which can act as a:

- **Router:** This is the default device mode of the NBG6817. Use this mode to connect the local network to another network, like the Internet. Go to [Section 6.2 on page 36](#) to view the **Status** screen in this mode.
- **Access Point:** Use this mode if you want to extend your network by allowing network devices to connect to the NBG6817 wirelessly. Go to [Section 7.4 on page 44](#) to view the **Status** screen in this mode.

For more information on these modes and to change the mode of your NBG6817, refer to [Chapter 15 on page 161](#).

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

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

When changing to another mode, the IP address of the NBG6817 changes. The running applications and services of the network devices connected to the NBG6817 can be interrupted.

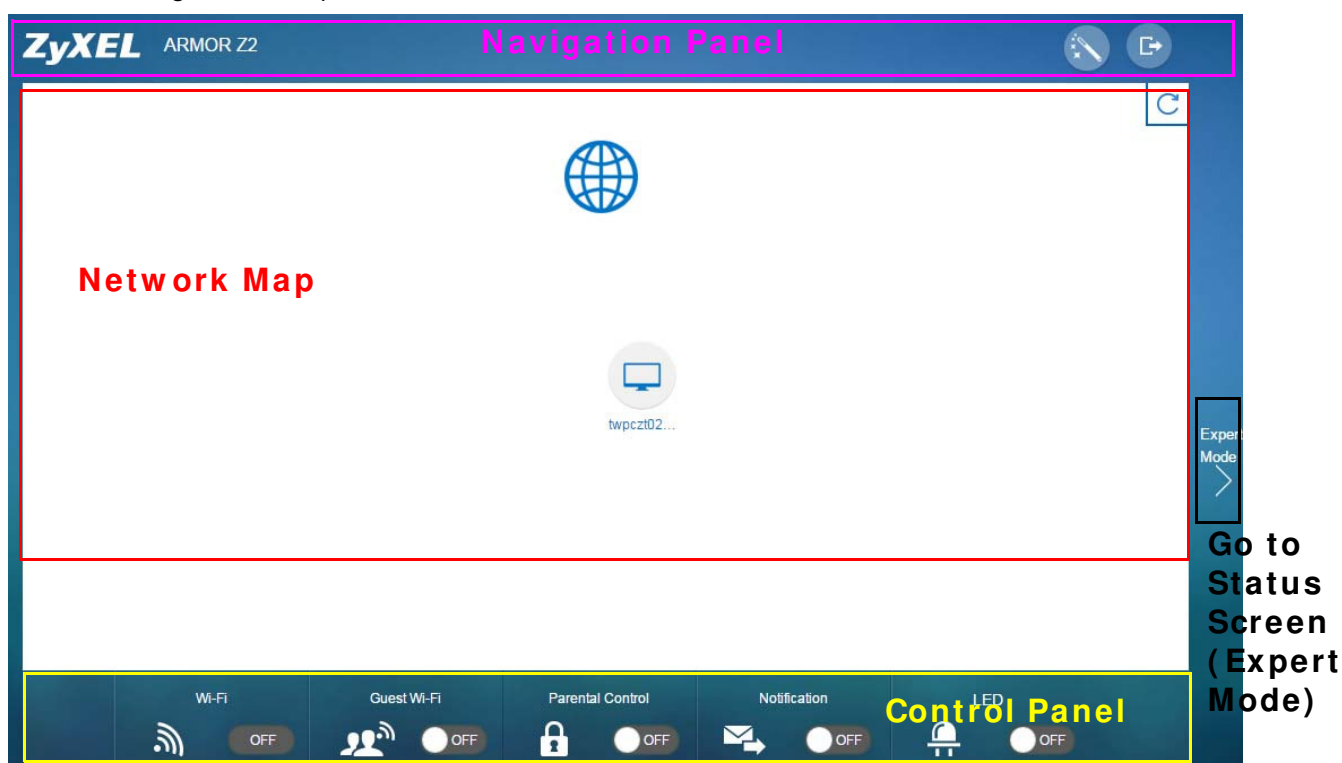
Easy Mode

5.1 Overview

The Web Configurator is set to **Easy Mode** by default. You can configure several key features of the NBG6817 in this mode. This mode is useful for users who are not fully familiar with some features that are usually intended for network administrators.

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

Figure 16 Easy Mode



5.2 What You Can Do

You can do the following in this mode:

- Use this **Navigation Panel** to open the eaZy123 wizard or log out the NBG6817 ([Section 5.4 on page 29](#)).

- Use the **Network Map** screen to check if your NBG6817 is connected to the Internet ([Section 5.5 on page 30](#)).
- Use the **Control Panel** to configure and enable NBG6817 features, including guest Wi-Fi, wireless security, parental control and so on ([Section 5.6 on page 31](#)).

5.3 What You Need to Know

Between the different device modes, the **Control Panel** ([Section 5.6 on page 31](#)) changes depending on which features are applicable to the mode:

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

5.4 Navigation Panel

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

Figure 17 Easy Mode: Navigation Panel



The following table describes the labels in this screen.

Table 7 Easy Mode: Navigation Panel




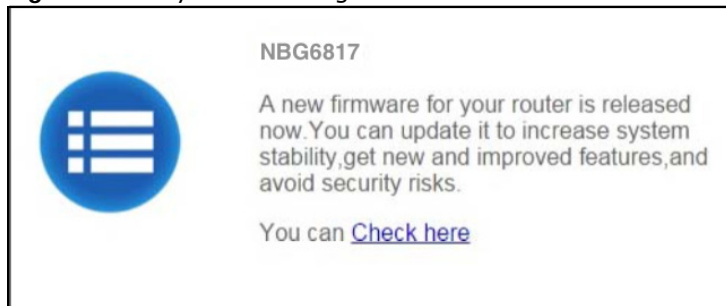
ITEM	DESCRIPTION
 Firmware Notification	Click this icon to open a screen where you can click Check here to redirect your screen to the firmware upgrade page. This icon only displays when new firmware is released.
 Wizard	Click this icon to open the eaZy123 wizard for the NBG6817.
 Logout	Click this to end the Web Configurator session.

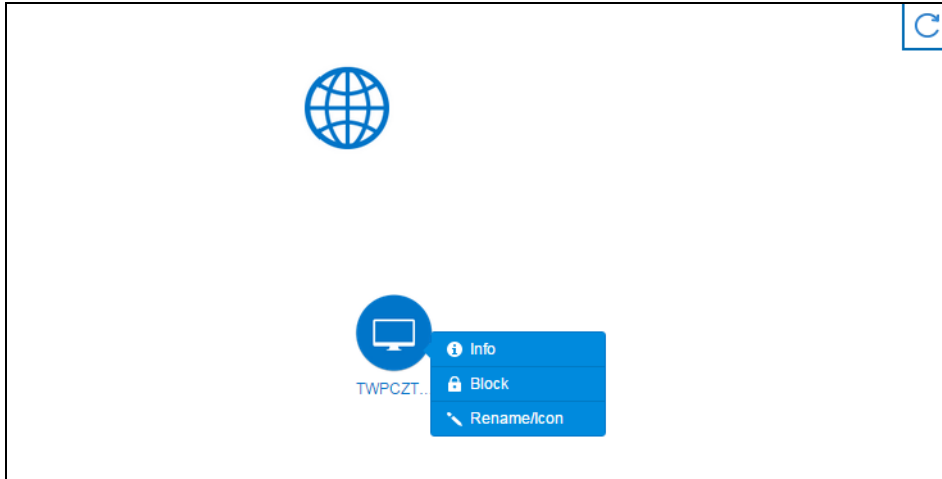
Figure 18 Easy Mode: Navigation Panel: Firmware Notification



5.5 Network Map

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

Figure 19 Easy Mode: Network Map



This screen displays whether the NBG6817 connects to the Internet. It also shows the devices connected to the NBG6817, including those connecting wirelessly. Click the **Refresh** button to refresh the network map.

The following table describes the icons in this screen.

Table 8 Easy Mode: Network Map






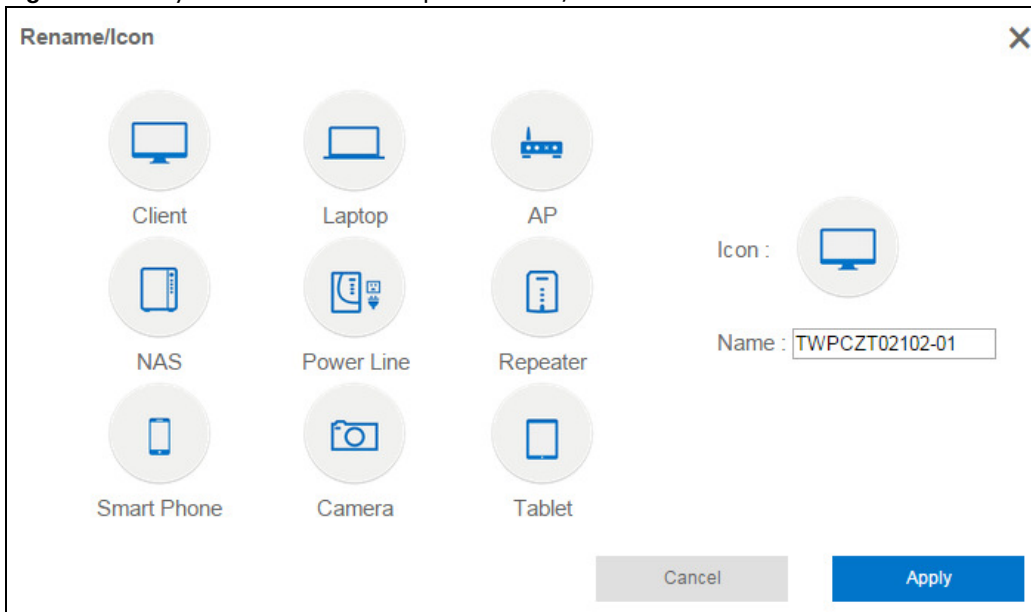
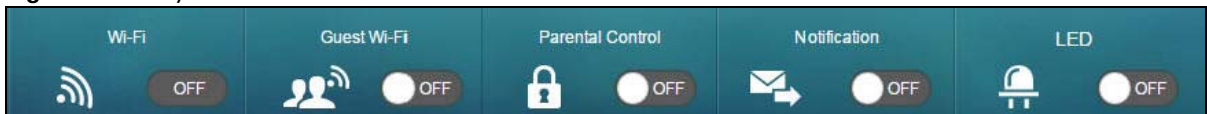
ITEM	DESCRIPTION
	This icon shows the NBG6817's connection status. This icon is grayed out if the user is unable to access the Internet.
	Click this button to refresh the NBG6817's connection status and the network map.
 Info	Click this to view the device's information that is currently connected to the NBG6817.
 Block	Click this to block the device from accessing the Internet through the NBG6817.
 Rename / Icon	Click this to rename the device or change the device's icon.

Figure 20 Easy Mode: Network Map: Info**Figure 21** Easy Mode: Network Map: Rename / Icon

Click **Apply** to save your changes back to the NBG6817. Click **Cancel** to reload the previous configuration for this screen.

5.6 Control Panel

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

Figure 22 Easy Mode: Control Panel

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

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

The following table describes the labels in this screen.

Table 9 Easy Mode: Control Panel

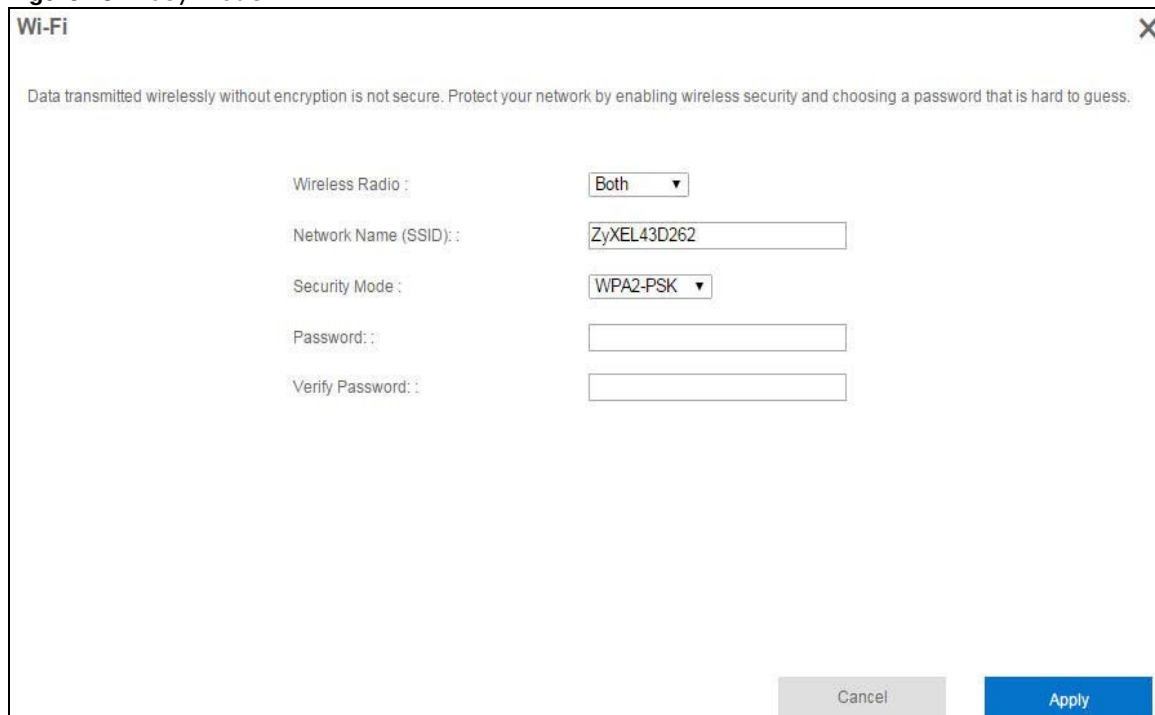
ITEM	DESCRIPTION
Wi-Fi	Click this to configure wireless radio, SSID, security mode and wireless password for the NBG6817's default Wi-Fi network. Refer to Section 5.6.1 on page 32 to see this screen.
Guest Wi-Fi	Click this to configure wireless and wireless security settings for the guest Wi-Fi network.
Parental Control	Switch ON to enable parental control, and click this to view the parental control rules. Otherwise, switch OFF . Refer to Section 5.6.3 on page 34 to see this screen.
Notification	Switch ON to have the NBG6817 send e-mail notifications when the user(s) is connected to the NBG6817 for Internet access during the specified time periods. Otherwise, switch OFF . Refer to Section 5.6.4 on page 35 to see this screen.
LED	Switch ON to have the NBG6817's LEDs (lights) stay lit/blinking. Otherwise, switch OFF .

5.6.1 Wi-Fi

Use this screen to configure security for the NBG6817's default wireless LAN. You can enter the SSID and select the wireless security mode in the following screen. See [Chapter 14 on page 143](#) for how to configure wireless network.

Note: You can enable the wireless function of your NBG6817 by first turning on the **WiFi** switch in the rear panel.

Figure 23 Easy Mode: Wi-Fi



The following table describes the labels in this screen.

Table 10 Easy Mode: Wi-Fi

LABEL	DESCRIPTION
Wireless Radio	Choose whether you want to apply the wireless security to 2.4G Hz , 5G Hz or Both wireless radios.
Network Name (SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 keyboard characters) for the wireless LAN.
Security Mode	Select WPA2-PSK to enable data encryption. Or Select No Security to allow wireless clients to communicate with the access points without any data encryption.
Password	This field appears when you choose wither WPA2-PSK as the security mode. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Verify Password	Type the password again to confirm.
Cancel	Click Cancel to reload the previous configuration for this screen.
Apply	Click Apply to save your changes back to the NBG6817.

5.6.2 Guest Wi-Fi

This screen allows you to configure guest wireless network settings on the NBG6817. Users connected to the guest wireless network can access the Internet via the NBG6817, but not other networks connected to the NBG6817. See [Chapter 11 on page 94](#) for how to enable and set up the guest wireless network.

Figure 24 Easy Mode: Guest Wi-Fi

Guest Wi-Fi X

You can setup a Guest Wi-Fi network to share your Internet access with your guests. Other LAN devices and services in your Host network will not be accessed by the Guest clients under this Guest network.

Wireless Radio :

Network Name (SSID):

Security Mode :

Password :

Verify Password: :

The following table describes the labels in this screen.

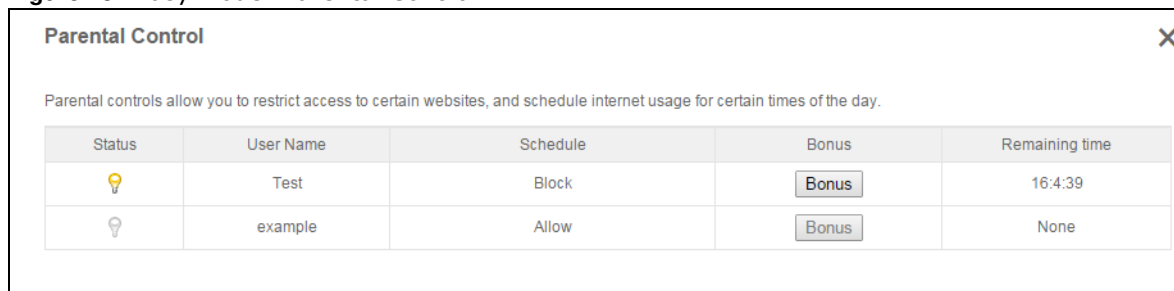
Table 11 Easy Mode: Guest Wi-Fi

LABEL	DESCRIPTION
Wireless Radio	Choose whether you want to apply the wireless settings to the 2.4G Hz or 5G Hz wireless radio.
Network Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the guest wireless network.
Security Mode	Select WPA2-PSK to enable data encryption. Or select No Security to allow wireless clients to communicate with the NBG6817 without any data encryption.
Password	This field appears when you choose WPA2-PSK as the security mode. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Verify Password	Type the password again to confirm.
Cancel	Click Cancel to reload the previous configuration for this screen.
Apply	Click Apply to save your changes back to the NBG6817.

5.6.3 Parental Control

Use this screen to view the parental control rules configured on the NBG6817. See [Section 13.2 on page 121](#) for how to enable and configure parental control rules.

Figure 25 Easy Mode: Parental Control



The screenshot shows a window titled "Parental Control" with a close button (X) in the top right corner. Below the title is a descriptive sentence: "Parental controls allow you to restrict access to certain websites, and schedule internet usage for certain times of the day." Below this is a table with five columns: Status, User Name, Schedule, Bonus, and Remaining time. The table contains two rows of data.

Status	User Name	Schedule	Bonus	Remaining time
	Test	Block	<input type="button" value="Bonus"/>	16:4:39
	example	Allow	<input type="button" value="Bonus"/>	None

The following table describes the labels in this screen.

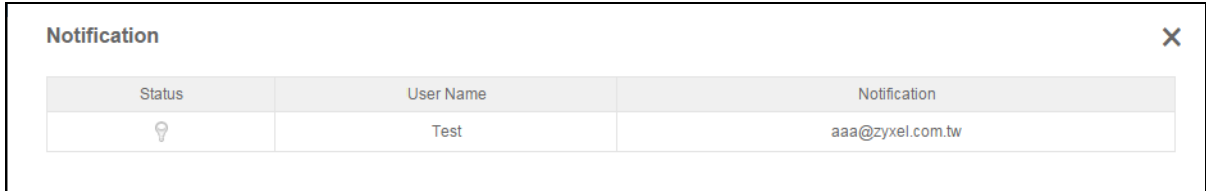
Table 12 Easy Mode: Parental Control

LABEL	DESCRIPTION
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
User Name	This shows the name of the user to which this rule applies.
Schedule	This shows whether the user is allowed to access the Internet (Allow) or not (Block).
Bonus	If the user is currently not permitted to access the Internet, you can click the Bonus to allow access for a specified period of time. A screen then displays allowing you to set how long (in minutes) the user is allowed to access the Internet. This button is grayed out if the user is now able to access the Internet.
Remaining time	This field displays the amount of Internet access time that remains for each user before the NBG6817 blocks the user from accessing the Internet. None means there is no extra Internet access time.

5.6.4 Notification

Use this screen to view the e-mail notification rules configured on the NBG6817. See [Section 13.2.2 on page 125](#) for how to configure e-mail notification rules and e-mail settings.

Figure 26 Easy Mode: Notification



Status	User Name	Notification
⚪	Test	aaa@zyxel.com.tw

The following table describes the labels in this screen.

Table 13 Easy Mode: Notification

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

5.6.5 LED

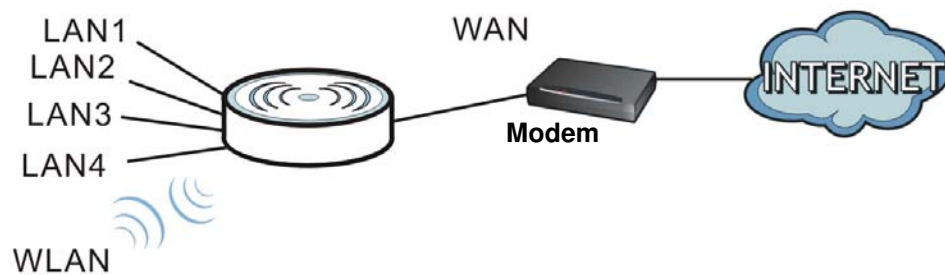
Switch **ON** to turn on the LEDs (lights) on the NBG6817. Otherwise, switch **OFF**.

Router Mode

6.1 Overview

The NBG6817 is set to router mode by default. Routers are used to connect the local network to another network (for example, the Internet). In the figure below, the NBG6817 connects the local network (**LAN1 ~ LAN4**) to the Internet.

Figure 27 NBG6817 Network



Note: After clicking **Login**, the **Easy Mode** appears. Refer to [Chapter 5 on page 28](#) for the **Easy Mode** screens. Change to **Expert Mode** to see the screens described in the sections following this.

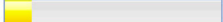
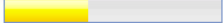
6.2 Router Mode Status Screen

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

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

System Status

Device Information	
Item	Data
Host Name:	NBG6817
Model Number:	NBG6817
Firmware Version:	V1.00(ABCS.0)b5
Sys OP Mode:	Router Mode
WAN Information	
- MAC Address:	EA:5B:64:7F:93:8B
- IP Address:	172.21.56.92
- IP Subnet Mask:	255.255.255.0
- Default Gateway:	172.21.56.254
- IPv6 Address:	
LAN Information:	
- MAC Address:	BE:E5:CC:BE:DF:C7
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
- IPv6 Address:	
WLAN 2.4G Information:	
- WLAN OP Mode:	Access Point Mode
- MAC Address:	11:03:7F:BA:DB:04
- SSID:	ZyXELBADB06
- Channel:	
- Security:	WPA2-PSK
WLAN 5G Information:	
- WLAN OP Mode:	Access Point Mode
- MAC Address:	11:03:7F:BA:DB:05
- SSID:	ZyXELBADB06.speed
- Channel:	
- Security:	WPA2-PSK
Firewall:	Enable

System Status	
Item	Data
System Up Time:	0day 0hr18min 52sec
Current Date/Time:	2016-03-11/07:32:40
System Resource:	
- CPU Usage:	 9%
- Memory Usage:	 38%

Interface Status		
Interface	Status	Rate
WAN	UP	100M
LAN1	Down	
LAN2	Down	
LAN3	UP	1000M
LAN4	Down	
WLAN 2.4G	Down	N/A
WLAN 5G	Down	N/A

Printer Information	
Item	Data
Printer Name:	None

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

Table 14 Expert Mode: Status > System Status: Router Mode

LABEL	DESCRIPTION
Device Information	
Item	This column shows the type of data the NBG6817 is recording.
Data	This column shows the actual data recorded by the NBG6817.
Host Name	This is the System Name you enter in the Maintenance > General screen. It is for identification purposes.
Model Number	This is the model name of your device.
Firmware Version	This is the firmware version.
Sys OP Mode	This is the device mode (Section 4.1.2 on page 27) to which the NBG6817 is set - Router Mode .
WAN Information	
MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
IP Address	This shows the WAN port's IP address.
IP Subnet Mask	This shows the WAN port's subnet mask.
Default Gateway	This shows the WAN port's gateway IP address.
IPv6 Address	This shows the IPv6 address of the NBG6817 on the WAN.
LAN Information	

Table 14 Expert Mode: Status > System Status: Router Mode (continued)

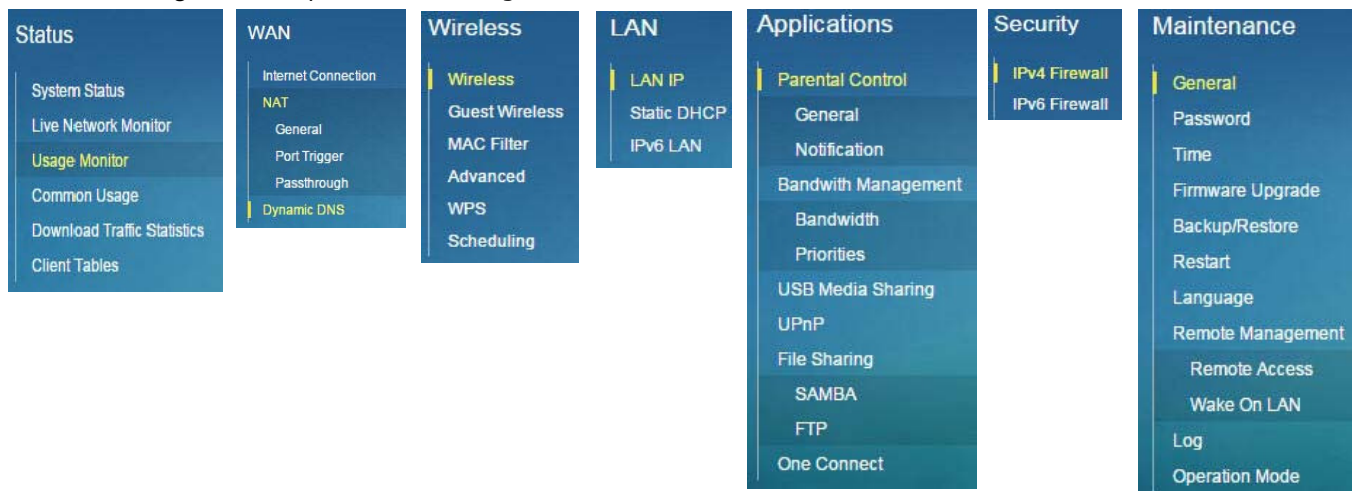
LABEL	DESCRIPTION
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP	This shows the LAN port's DHCP role - Server or Disable .
IPv6 Address	This shows the IPv6 address of the NBG6817 on the LAN.
WLAN 2.4G Information	
WLAN OP Mode	This is the device mode (Section 4.1.2 on page 27) to which the NBG6817's wireless LAN is set - Access Point Mode .
MAC Address	This shows the 2.4GHz wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the NBG6817 in the 2.4GHz wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the NBG6817 is using.
WLAN 5G Information	
WLAN OP Mode	This is the device mode (Section 4.1.2 on page 27) to which the NBG6817's wireless LAN is set - Access Point Mode .
MAC Address	This shows the 5GHz wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the NBG6817 in the 5GHz wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the NBG6817 is using.
Firewall	This shows whether the firewall is enabled or not.
System Status	
System Up Time	This is the total time the NBG6817 has been on.
Current Date/Time	This field displays your NBG6817's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG6817's processing ability is currently used. When this percentage is close to 100%, the NBG6817 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.)
- Memory Usage	This shows what percentage of the heap memory the NBG6817 is using.
Interface Status	
Interface	This displays the NBG6817 port types. The port types are: WAN , LAN and WLAN .
Status	For the LAN and WAN ports, this field displays Down (line is down) or Up (line is up or connected). For the 2.4GHz/5GHz WLAN, it displays Up when the 2.4GHz/5GHz WLAN is enabled or Down when the 2.4G/5G WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or is left blank when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation. This field displays N/ A when the line is disconnected. For the 2.4GHz/5GHz WLAN, it displays the maximum transmission rate when the 2.4GHz/5GHz WLAN is enabled and N/ A when the WLAN is disabled.

Table 14 Expert Mode: Status > System Status: Router Mode (continued)

LABEL	DESCRIPTION
Printer Information	
Printer Name	The NBG6817 can act as a print server and allows you to share a USB printer on your LAN. This displays the name of the printer connected to the NBG6817's USB port. Note: You need to manually install the printer driver in your computer and add the printer to your printer list.

6.2.1 Navigation Panel

Use the sub-menus on the navigation panel to configure NBG6817 features.

Figure 29 Expert Mode: Navigation Panel: Router Mode

The following table describes the sub-menus.

Table 15 Expert Mode: Navigation Panel: Router Mode

LINK	TAB	FUNCTION
Status		
System Status		This screen shows the NBG6817's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Live Network Monitor		This screen shows transmission data rates between the NBG6817 and the Internet or connected devices.
Usage Monitor		This screen shows transmission data and bandwidth usage between the NBG6817 and the Internet or connected devices.
Common Usage		This screen shows the top five traffic flows transmitting from/to the selected LAN device(s).
Download Traffic Statistics		This screen shows the type and percentage of most download traffic.
Client Tables		Use this screen to view online clients information.
WAN		
Internet Connection		This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address.

Table 15 Expert Mode: Navigation Panel: Router Mode (continued)

LINK	TAB	FUNCTION
NAT	General	Use this screen to enable NAT. Use this screen to configure servers behind the NBG6817 and forward incoming service requests to the server(s) on your local network.
	Port Trigger	Use this screen to change your NBG6817's port triggering settings.
	Passthrough	Use this screen to enable ALGs (Application Layer Gateway) and VPN pass-through settings.
Dynamic DNS		Use this screen to set up dynamic DNS.
Wireless		
Wireless		Use this screen to enable the wireless LAN and configure wireless LAN and wireless security settings.
Guest Wireless		Use this screen to configure multiple BSSs on the NBG6817.
MAC Filter		Use the MAC filter screen to configure the NBG6817 to block access to devices or block the devices from accessing the NBG6817.
Advanced		This screen allows you to configure advanced wireless settings.
WPS		Use this screen to configure WPS.
Scheduling		Use this screen to schedule the times the Wireless LAN is enabled.
LAN		
LAN IP		Use this screen to configure LAN IP address and subnet mask. Use this screen to configure the IPv6 address for the NBG6817 on the LAN. Use this screen to enable the NBG6817's DHCP server.
Static DHCP		This screen allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses.
IPv6 LAN		Use this screen to configure the IPv6 address for your NBG6817 on the LAN.
Applications		
Parental Control	General	Use this screen to enable parental control, set parental controls rules/schedules and block web sites containing certain keywords in the URL.
	Notification	Use this screen to send e-mail notifications, configure e-mail notification rules and e-mail settings.
Bandwidth Management	Bandwidth	Use this screen to enable StreamBoost. Use this screen to configure the maximum allowable bandwidth and enable automatic update.
	Priorities	Use this screen to change the priority of the connected devices.
USB Media Sharing		Use this screen to have the NBG6817 function as a DLNA-compliant media server, that lets DLNA-compliant media clients play video, audio, and photo content files stored on the connected USB storage device.
UPnP		Use this screen to enable UPnP on the NBG6817.
File Sharing	SAMBA	Use this screen to enable file sharing through the NBG6817.
	FTP	Use this screen to have the NBG6817 act as a FTP server.
One Connect		Use this screen to enable or disable Wi-Fi auto-configuration.
Security		
IPv4 Firewall		Use this screen to configure IPv4 firewall rules.
IPv6 Firewall		Use this screen to configure IPv6 firewall rules.
Maintenance		

Table 15 Expert Mode: Navigation Panel: Router Mode (continued)

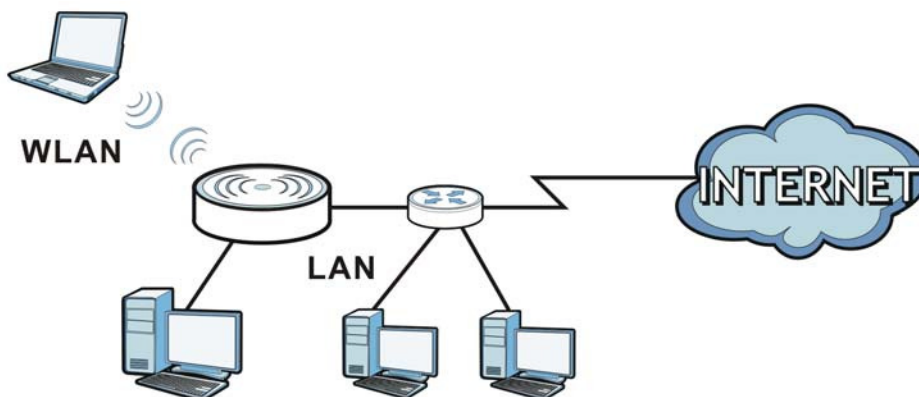
LINK	TAB	FUNCTION
General		Use this screen to view and change administrative settings such as system and domain names.
Password		Use this screen to change the password of your NBG6817.
Time		Use this screen to change your NBG6817's time and date.
Firmware Upgrade		Use this screen to upload firmware to your NBG6817.
Backup/Restore		Use this screen to backup and restore the configuration or reset the factory defaults to your NBG6817.
Restart		This screen allows you to reboot the NBG6817 without turning the power off.
Language		This screen allows you to select the language you prefer.
Remote Management	Remote Access	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet and HTTP/HTTPS to manage the NBG6817.
	Wake On LAN	Use this screen to enable Wake on LAN to remotely turn on a device on the local network.
Log		Use this screen to view the list of activities recorded by your NBG6817.
Operation Mode		This screen allows you to select whether your device acts as a router, or an access point.

Access Point Mode

7.1 Overview

Use your NBG6817 as an access point (AP) if you already have a router or gateway on your network. In this mode your NBG6817 bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

Figure 30 Wireless Internet Access in Access Point Mode



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

7.2 What You Can Do

- Use the **Status** screen to view read-only information about your NBG6817 ([Section 7.4 on page 44](#)).
- Use the **LAN** screen to set the IP address for your NBG6817 acting as an access point ([Section 7.5 on page 46](#)).

7.3 What You Need to Know

See [Chapter 8 on page 49](#) for a tutorial on setting up a network with the NBG6817 as an access point.

7.3.1 Setting your NBG6817 to AP Mode

- 1 Log into the Web Configurator if you haven't already. See the Quick start Guide for instructions on how to do this.
- 2 To use your NBG6817 as an access point, go to **Expert Mode > Maintenance > Operation Mode** and select **Access Point Mode**.

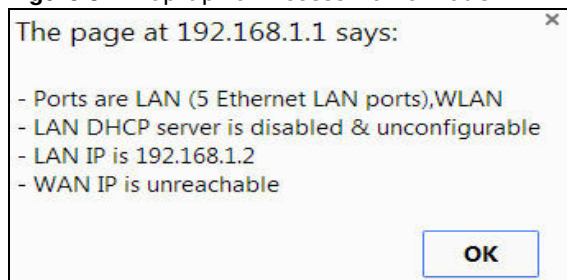
Figure 31 Changing to Access Point mode



Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your NBG6817 is already in Access Point mode.

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

Figure 32 Pop up for Access Point mode



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

7.3.2 Accessing the Web Configurator in Access Point Mode

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

- 1 Connect your computer to the LAN port of the NBG6817.
- 2 The default IP address of the NBG6817 is "192.168.1.2". In this case, your computer must have an IP address in the range between "192.168.1.3" and "192.168.1.254".
- 3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see [Appendix B on page 176](#) for information on changing your computer's IP address.

- After you've set your computer's IP address, open a web browser such as Internet Explorer and type "192.168.1.2" as the web address in your web browser.

Note: After clicking **Login**, the **Easy Mode** appears. Refer to [Section on page 28](#) for the **Easy Mode** screens. Change to **Expert Mode** to see the screens described in the sections following this.

7.3.3 Configuring your WLAN and Maintenance Settings

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

- See [Chapter 11 on page 94](#) for information on the configuring your wireless network.
- See [Chapter 15 on page 149](#) for information on configuring your maintenance settings.

7.4 AP Mode Status Screen

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

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

System Status

Device Information	
Item	Data
Host Name:	NBG6817
Model Number:	NBG6817
Firmware Version:	V1.00(ABCS.0)b5
Sys OP Mode:	Access Point Mode
LAN Information:	
- MAC Address:	66:4C:08:32:05:3D
- IP Address:	192.168.1.2
- IP Subnet Mask:	255.255.255.0
- DHCP:	None
- IPv6 Address:	
WLAN 2.4G Information:	
- WLAN OP Mode:	Access Point Mode
- MAC Address:	11:03:7F:BA:DB:04
- SSID:	ZyXELBADB06
- Channel:	
- Security:	WPA2-PSK
WLAN 5G Information:	
- WLAN OP Mode:	Access Point Mode
- MAC Address:	11:03:7F:BA:DB:05
- SSID:	ZyXELBADB06.speed
- Channel:	
- Security:	WPA2-PSK

System Status	
Item	Data
System Up Time:	0day 0hr3min 49sec
Current Date/Time:	2016-03-11/08:28:29
System Resource:	
- CPU Usage:	<div style="width: 10%; background-color: yellow; border: 1px solid gray;"></div> 10%
- Memory Usage:	<div style="width: 26%; background-color: yellow; border: 1px solid gray;"></div> 26%

Interface Status		
Interface	Status	Rate
LAN1	Down	
LAN2	Down	
LAN3	UP	1000M
LAN4	Down	
LAN5	UP	100M
WLAN 2.4G	Down	N/A
WLAN 5G	Down	N/A

Printer Information	
Item	Data
Printer Name:	None

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

Table 16 Expert Mode: Status > System Status: Access Point Mode

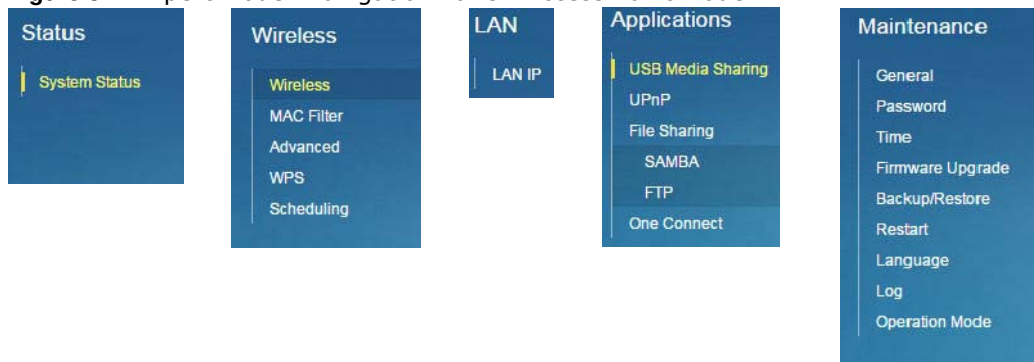
LABEL	DESCRIPTION
Device Information	
Host Name	This is the System Name you enter in the Maintenance > General screen. It is for identification purposes.
Model Number	This is the model name of your device.
Firmware Version	This is the firmware version.
Sys OP Mode	This is the device mode (Section 4.1.2 on page 27) to which the NBG6817 is set - AP Mode .
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP	This shows the LAN port's DHCP role - Client or None .
IPv6 Address	This shows the IPv6 address of the NBG6817 on the LAN.
WLAN 2.4G Information	
WLAN OP Mode	This is the device mode (Section 4.1.2 on page 27) to which the NBG6817's wireless LAN is set - Access Point Mode .
MAC Address	This shows the 2.4GHz wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the NBG6817 in the 2.4GHz wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the NBG6817 is using.
WLAN 5G Information	
WLAN OP Mode	This is the device mode (Section 4.1.2 on page 27) to which the NBG6817's wireless LAN is set - Access Point Mode .
MAC Address	This shows the 5GHz wireless adapter MAC Address of your device.
SSID	This shows a descriptive name used to identify the NBG6817 in the 5GHz wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the NBG6817 is using.
System Status	
Item	This column shows the type of data the NBG6817 is recording.
Data	This column shows the actual data recorded by the NBG6817.
System Up Time	This is the total time the NBG6817 has been on.
Current Date/Time	This field displays your NBG6817's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG6817's processing ability is currently used. When this percentage is close to 100%, the NBG6817 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications.
- Memory Usage	This shows what percentage of the heap memory the NBG6817 is using.
Interface Status	
Interface	This displays the NBG6817 port types. The port types are: LAN and WLAN .
Status	For the LAN ports, this field displays Down (line is down) or Up (line is up or connected). For the 2.4GHz/5GHz WLAN, it displays Up when the 2.4GHz/5GHz WLAN is enabled or Down when the 2.4G/5G WLAN is disabled.

Table 16 Expert Mode: Status > System Status: Access Point Mode (continued)

LABEL	DESCRIPTION
Rate	For the LAN ports, this displays the port speed and duplex setting or is left blank when the line is disconnected. For the 2.4GHz/5GHz WLAN, it displays the maximum transmission rate when the 2.4GHz/5GHz WLAN is enabled and N/ A when the WLAN is disabled.
Printer Information	
Printer Name	The NBG6817 can act as a print server and allows you to share a USB printer on your LAN. This displays the name of the printer connected to the NBG6817's USB port. Note: You need to manually install the printer driver in your computer and add the printer to your printer list.

7.4.1 Navigation Panel

Use the menu in the navigation panel to configure NBG6817 features in **Access Point Mode**.

Figure 34 Expert Mode: Navigation Panel: Access Point Mode

Refer to [Table 15 on page 39](#) for descriptions of the labels shown in the navigation panel.

7.5 LAN Screen

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

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

Note: If you change the IP address of the NBG6817 in the screen below, you will need to log into the NBG6817 again using the new IP address.

Figure 35 LAN > LAN IP

LAN IP		Apply	Cancel
IP Address			
<input type="radio"/> Obtain an IP Address Automatically(DHCP) <input checked="" type="radio"/> Static IP Address			
IP Address :	<input type="text" value="192.168.1.2"/>		
Subnet Mask :	<input type="text" value="255.255.255.0"/>		
Default Gateway :	<input type="text"/>		
DNS Server			
First DNS Server :	<input type="text" value="Obtained From ISP"/>	<input type="text"/>	
Second DNS Server :	<input type="text" value="Obtained From ISP"/>	<input type="text"/>	
Third DNS Server :	<input type="text" value="Obtained From ISP"/>	<input type="text"/>	

The table below describes the labels in the screen.

Table 17 LAN > LAN IP

LABEL	DESCRIPTION
IP Address	
Obtain an IP Address Automatically	<p>When you enable this, the NBG6817 gets its IP address from the network's DHCP server (for example, your ISP). Users connected to the NBG6817 can now access the network (i.e., 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 NBG6817. You need to reset the NBG6817 to be able to access the Web Configurator again (see Section 15.7 on page 154 for details on how to reset the NBG6817).</p> <p>Also when you select this, you cannot enter an IP address for your NBG6817 in the field below.</p>
Static IP Address	Click this if you want to specify the IP address of your NBG6817. Or if your ISP or network administrator gave you a static IP address to access the network or the Internet.
IP Address	Type the IP address in dotted decimal notation. The default setting is 192.168.1.2. If you change the IP address you will have to log in again with the new IP address.
Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG6817 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 NBG6817.
Default Gateway	Enter a gateway IP address (if your ISP or network administrator gave you one) in this field.
DNS Server	
First DNS Server	<p>Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the NBG6817's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
Second DNS Server	
Third DNS Server	

Table 17 LAN > LAN IP (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the NBG6817.
Cancel	Click Cancel to reload the previous configuration for this screen.

8.1 Overview

This chapter provides tutorials for setting up your NBG6817.

- [Set Up a Wireless Network Using WPS](#)
- [Connect to NBG6817 Wireless Network without WPS](#)
- [Using Guest SSIDs on the NBG6817](#)

8.2 Set Up a Wireless Network Using WPS

This section gives you an example of how to set up wireless network using WPS. This example uses the NBG6817 as the AP and NWD210N as the wireless client which connects to a notebook.

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

There are two WPS methods for creating a secure connection via the web configurator or utility. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See [Section 8.2.1 on page 49](#). This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the NBG6817's interface. See [Section 8.2.2 on page 50](#). This is the more secure method, since one device can authenticate the other.

8.2.1 Push Button Configuration (PBC)

- 1 Make sure that your NBG6817 is turned on. Make sure the **WIFI** button (at the back panel of the NBG6817) is pushed in, and that the device is placed within range of your notebook.
- 2 Make sure that you have installed the wireless client (this example uses the NWD210N) driver and utility in your notebook.
- 3 In the wireless client utility, find the WPS settings. Enable WPS and press the WPS button (**Start** or **WPS** button)
- 4 Log into NBG6817's Web Configurator and press the **Push Button** in the **Expert > Wireless > WPS** screen.

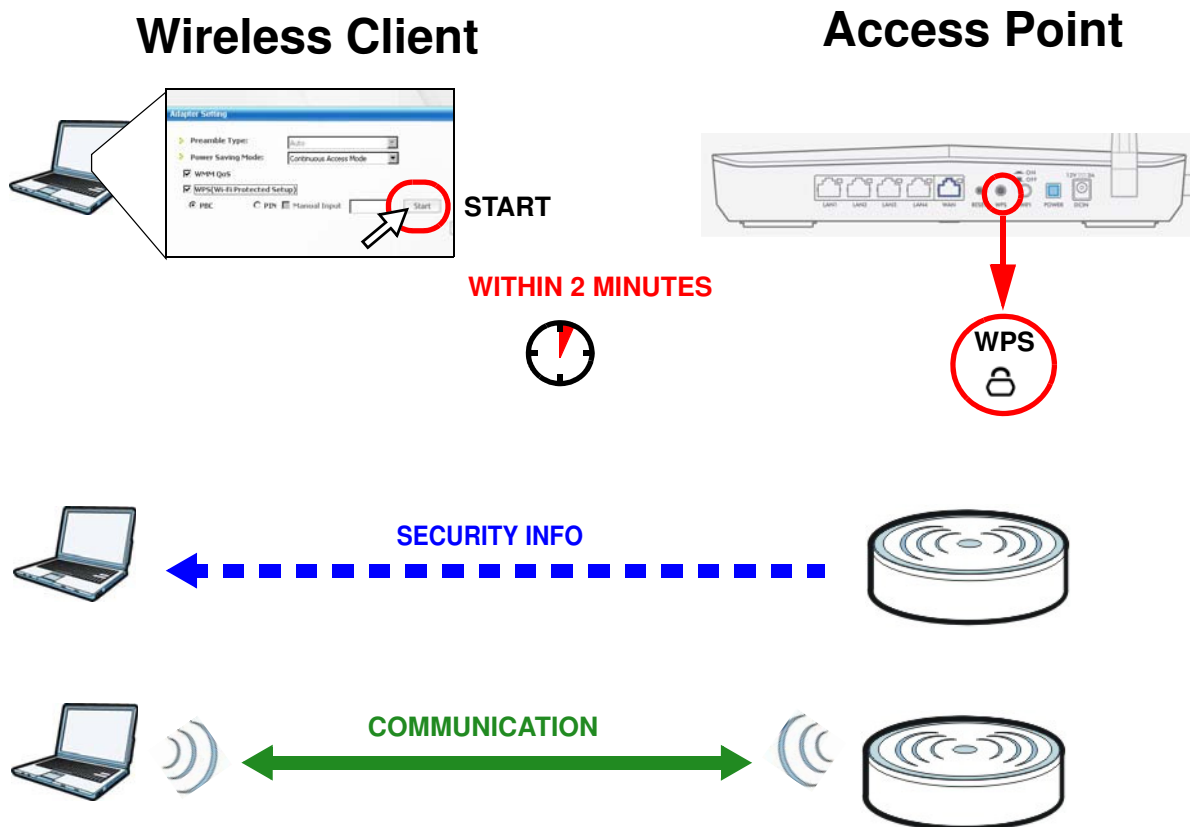
Note: Your NBG6817 has a WPS button located on its rear panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

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

The NBG6817 sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the NBG6817 securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both NBG6817 and wireless client (the NWD210N in this example).

Figure 36 Example WPS Process: PBC Method



8.2.2 PIN Configuration

When you use the PIN configuration method, you need to use both NBG6817's configuration interface and the client's utilities.

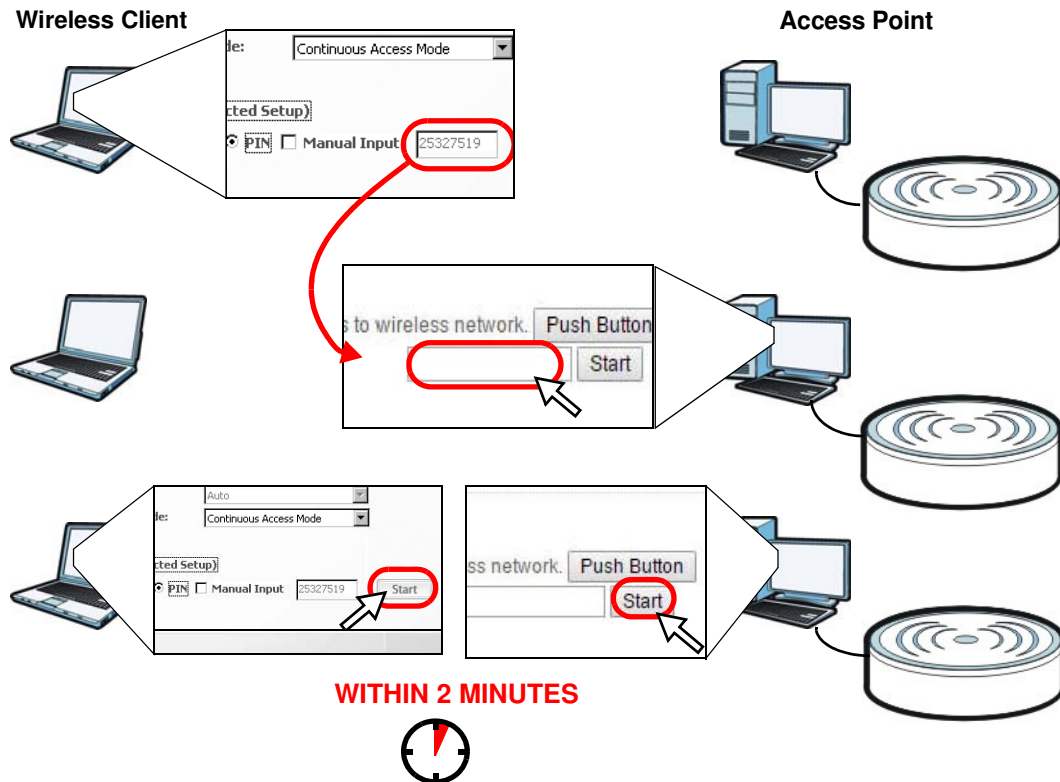
- 1 Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.
- 2 Enter the PIN number to the **PIN** field in the **Expert > Wireless > WPS** screen on the NBG6817.

- Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the NBG6817's **WPS** screen within two minutes.

The NBG6817 authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the NBG6817 securely.

The following figure shows you the example to set up wireless network and security on NBG6817 and wireless client (ex. NWD210N in this example) by using PIN method.

Figure 37 Example WPS Process: PIN Method



8.3 Connect to NBG6817 Wireless Network without WPS

This example shows you how to configure wireless security settings with the following parameters on your NBG6817 and connect your computer to the NBG6817 wireless network.

Band	2.4GHz
SSID	SSID_Example3
Channel	6
Security	WPA2-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your NBG6817.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the Web Configurator through your LAN connection (see [Section 2.2 on page 15](#)).

- 1 Make sure the **WIFI** switch (at the back panel of the NBG6817) is set to **ON**.
- 2 Open the **Expert > Wireless > Wireless** screen in the AP's Web Configurator.
- 3 Confirm that the wireless LAN is enabled on the NBG6817.
- 4 Select to configure the wireless settings for the 2.4GHz wireless radio.
- 5 Enter **SSID_Example3** as the SSID and select **Channel-06** as the channel. Set security mode to **WPA2-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

Wireless 2.4G Apply Cancel

Wireless Setup

Band : 2.4GHz ▾

Wireless LAN : Enable Disable

Name (SSID) : SSID_Example3

Hide SSID

Channel Selection : Channel-6 2437MHz ▾

Operating Channel : Channel-6

Channel Width : Auto 20/40 MHz ▾

802.11 Mode : 802.11bgn ▾

Security

Security Mode : WPA2-PSK ▾

WPA-PSK Compatible

Pre-Shared Key : ThisismyWPA-PSKpre-sharedkey

Group Key Update Timer : 3600 seconds

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

- 6 Click **Expert > Status** to open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

System Status

Device Information	
Item	Data
Host Name:	NBG6817
Model Number:	NBG6817
Firmware Version:	V1.00(ABCS.0)b6_test6
Sys OP Mode:	Router Mode
WAN Information	
- MAC Address:	1A:5A:3D:DB:6A:BF
- IP Address:	172.21.56.71
- IP Subnet Mask:	255.255.255.0
- Default Gateway:	172.21.56.254
- IPv6 Address:	
LAN Information:	
- MAC Address:	0E:E1:28:6C:E7:9E
- IP Address:	192.168.1.1
- IP Subnet Mask:	255.255.255.0
- DHCP:	Server
- IPv6 Address:	
WLAN 2.4G Information:	
- WLAN OP Mode:	Access Point Mode
- MAC Address:	11:03:7F:BA:DB:04
- SSID:	SSID_Example3
- Channel:	6
- Security:	WPA-PSK / WPA2-PSK
WLAN 5G Information:	
- WLAN OP Mode:	Access Point Mode
- MAC Address:	11:03:7F:BA:DB:05
- SSID:	ZyXELBADB06.speed
- Channel:	161
- Security:	WPA-PSK / WPA2-PSK
Firewall:	Enable

System Status	
Item	Data
System Up Time:	0day 3hr 34min 58sec
Current Date/Time:	2016-05-03/14:58:35
System Resource:	
- CPU Usage:	<div style="width: 15%;"></div> 15%
- Memory Usage:	<div style="width: 42%;"></div> 42%

Interface Status		
Interface	Status	Rate
WAN	UP	100M
LAN1	Down	
LAN2	UP	1000M
LAN3	Down	
LAN4	Down	
WLAN 2.4G	UP	800 M
WLAN 5G	UP	1733 M

Printer Information	
Item	Data
Printer Name:	None

8.3.1 Configure Your Notebook

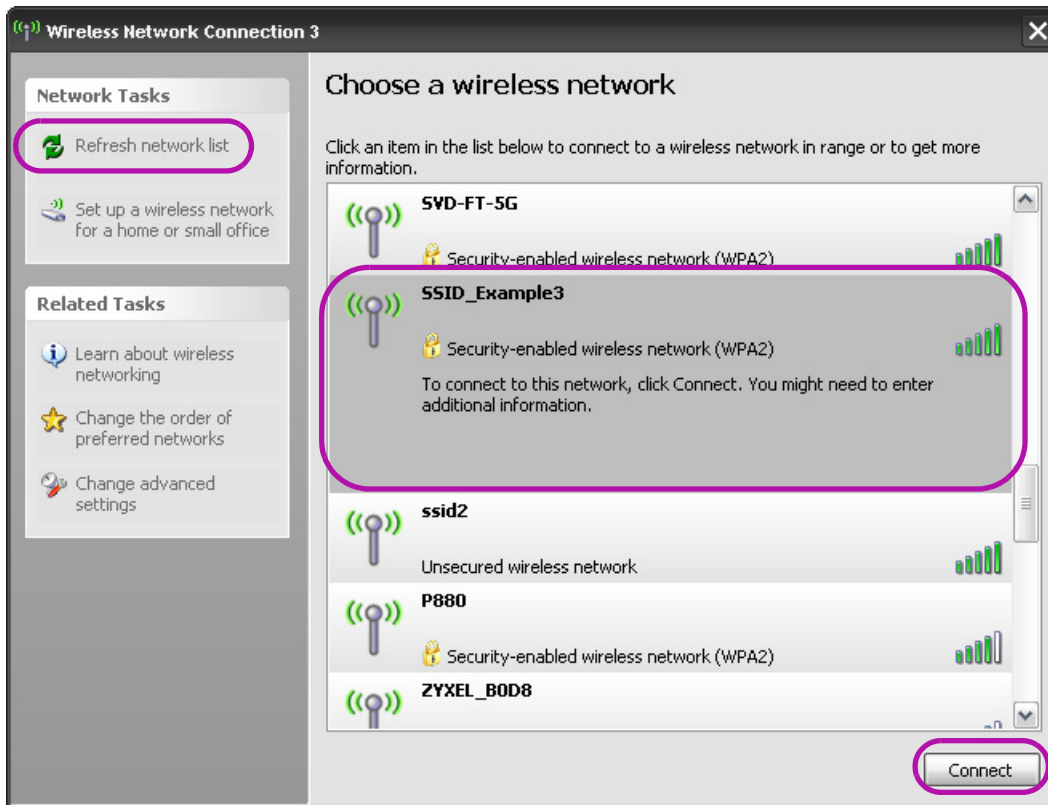
Note: In this example, we use the ZyXEL NWD6505 wireless adapter as the wireless client and use the Windows built-in utility (Windows Zero Configuration (WZC)) to connect to the wireless network.

- 1 The NBG6817 supports IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n and IEEE 802.11ac wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.
- 2 Wireless adapters come with software sometimes called a "utility" that you install on your computer. See your wireless adapter's User's Guide for information on how to do that.
- 3 After you've installed the driver and attached the NWD6505 to your computer's USB port, right-click the **Wireless Network Connection** icon in your computer's system tray, select and click **View Available Wireless Networks**.

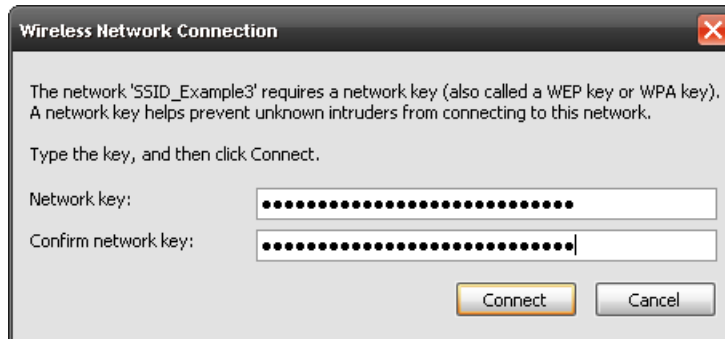


- 4 The **Wireless Network Connection** screen displays. Click **Refresh network list** to view the available wireless APs within range.

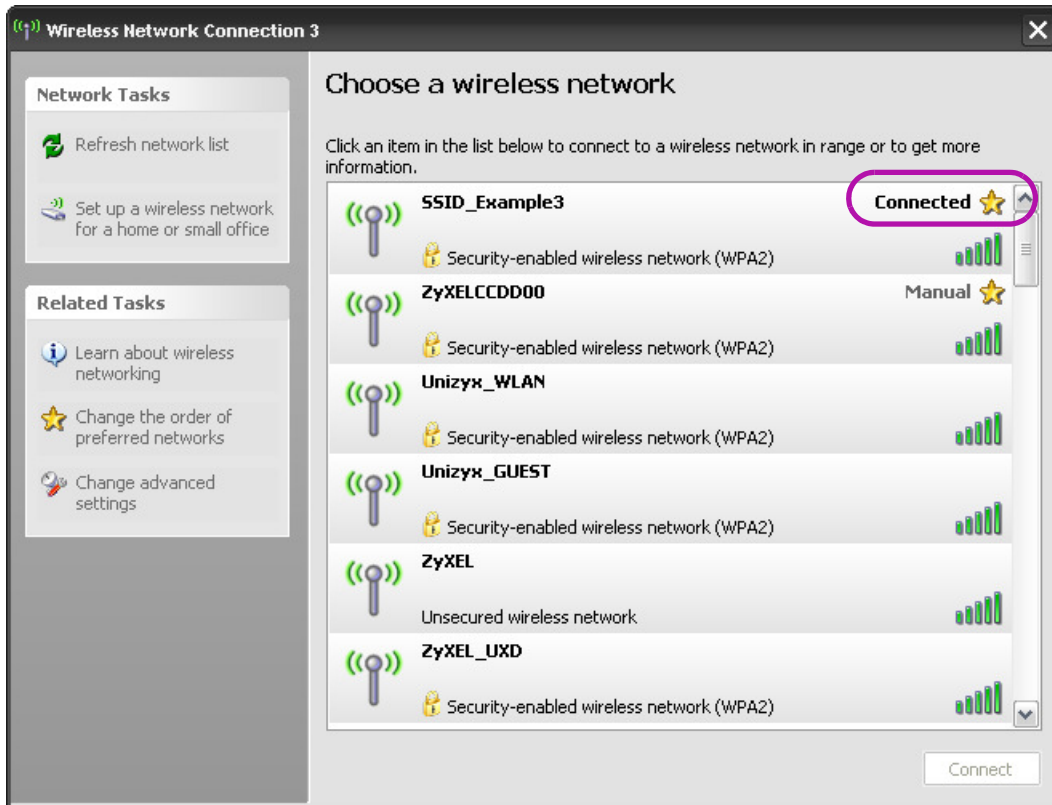
- 5 Select **SSID_Example3** and click **Connect**.



- 6 Type the security key in the following screen. Click **Connect**.



- 7 Check the status of your wireless connection in the screen below.



- 8 If the wireless client keeps trying to connect to or acquiring an IP address from the NBG6817, make sure you entered the correct security key.

If the connection has limited or no connectivity, make sure the DHCP server is enabled on the NBG6817.

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

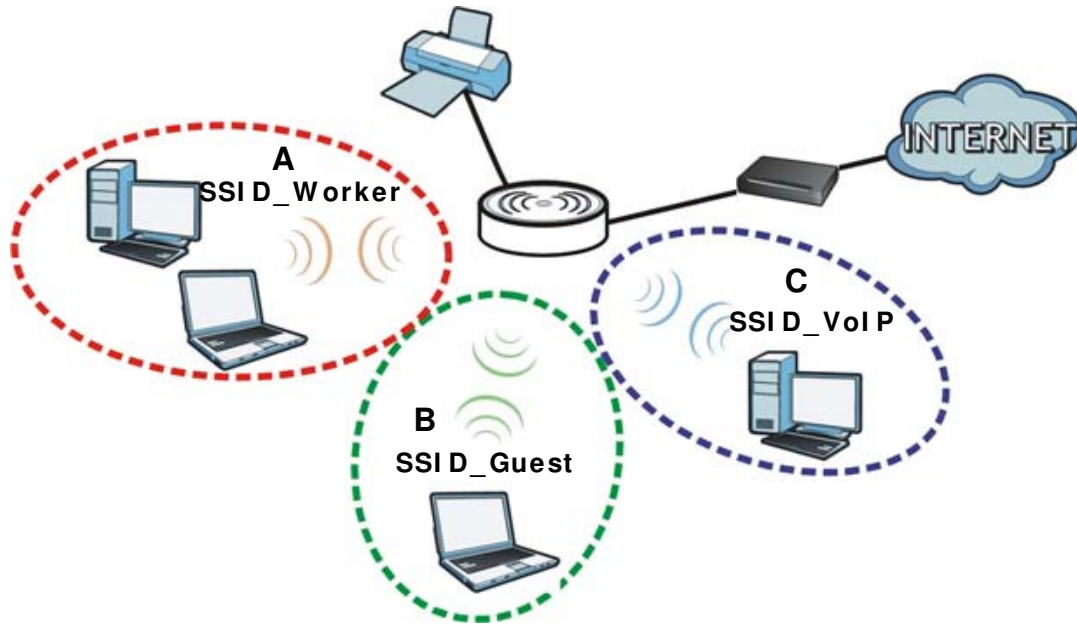
8.4 Using Guest SSIDs on the NBG6817

You can configure more than one guest SSID on a NBG6817. See [Section 11.4 on page 105](#).

This allows you to configure multiple independent wireless networks on the NBG6817 as if there were multiple APs (virtual APs). Each guest SSID has its own wireless security type. That is, each SSID on the NBG6817 represents a different access point/wireless network to wireless clients in the network.

Clients can associate only with the SSIDs for which they have the correct security settings. Clients using different SSIDs can access the Internet and the wired network behind the NBG6817 (such as a printer).

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



8.4.1 Configuring Security Settings of Guest SSIDs

The NBG6817 is in router mode by default.

This example shows you how to configure the SSIDs with the following parameters on your NBG6817 (in router mode).

SSID	SECURITY TYPE	KEY
SSID_Worker	WPA2-PSK WPA Compatible	DoNotStealMyWirelessNetwork
SSID_VoIP	WPA-PSK	VoIPOnly12345678
SSID_Guest	WPA-PSK	keyexample123



- 1 Connect your computer to the LAN port of the NBG6817 using an Ethernet cable.
- 2 The default IP address of the NBG6817 in router mode is "192.168.1.1". In this case, your computer must have an IP address in the range between "192.168.1.2" and "192.168.1.254".
- 3 Click **Start > Run** on your computer in Windows. Type "cmd" in the dialog box. Enter "ipconfig" to show your computer's IP address. If your computer's IP address is not in the correct range then see [Appendix B on page 176](#) for information on changing your computer's IP address.
- 4 After you've set your computer's IP address, open a web browser such as Internet Explorer and type "http://192.168.1.1" as the web address in your web browser.
- 5 Enter "1234" (default) as the password and click **Login**.
- 6 Type a new password and retype it to confirm, then click **Apply**. Otherwise, click **Ignore**.

- 7 The **Easy Mode** appears.
- 8 Go to **Expert > Wireless > Guest Wireless**. Click the **Edit** icon of the first entry to configure wireless and security settings for **SSID_Worker**.

Guest Wireless 2.4G

Band : 2.4GHz ▾

Guest Wireless Setup

#	Status	SSID	Security	Remaining time	Edit
1	💡	ZyXEL_SSID1	No Security	0:0:0 <input type="button" value="Set"/>	
2	💡	ZyXEL_SSID2	No Security	0:0:0 <input type="button" value="Set"/>	
3	💡	ZyXEL_SSID3	No Security	0:0:0 <input type="button" value="Set"/>	

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

Guest Wireless 2.4G Edit

Wireless Setup

Active :

Name (SSID) :

Hide SSID

Intra-BSS Traffic

WMM QoS

Enable Bandwidth Management for (max. bandwidth kbps)

Guest WLAN


Security

Security Mode : ▾

WPA-PSK Compatible

Pre-Shared Key

Group Key Update Timer seconds

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

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

Guest Wireless 2.4G

Band : 2.4GHz ▾

Guest Wireless Setup

#	Status	SSID	Security	Remaining time	Edit
1	💡	SSID_Worker	WPA2-PSK	0:0:0 <input type="button" value="Set"/>	
2	💡	ZyXEL_SSID2	No Security	0:0:0 <input type="button" value="Set"/>	
3	💡	ZyXEL_SSID3	No Security	0:0:0 <input type="button" value="Set"/>	

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

Guest Wireless 2.4G Edit Apply Cancel

Wireless Setup

Active :

Name (SSID) :

Hide SSID

Intra-BSS Traffic

WMM QoS

Enable Bandwidth Management for Guest WLAN (max. bandwidth kbps)

Security

Security Mode :

Pre-Shared Key

Group Key Update Timer seconds

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

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

Guest Wireless 2.4G

Band :

Guest Wireless Setup

#	Status	SSID	Security	Remaining time	Edit
1		SSID_Worker	WPA2-PSK	0:0:0 <input type="button" value="Set"/>	
2		SSID_VoIP	WPA2-PSK	0:0:0 <input type="button" value="Set"/>	
3		ZyXEL_SSID3	No Security	0:0:0 <input type="button" value="Set"/>	

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

Guest Wireless 2.4G Edit Apply Cancel

Wireless Setup

Active :

Name (SSID) :

Hide SSID

Intra-BSS Traffic

WMM QoS

Enable Bandwidth Management for Guest WLAN (max. bandwidth kbps)

Security

Security Mode :

Pre-Shared Key

Group Key Update Timer seconds

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

PART II

Technical Reference

9.1 Overview

This chapter discusses read-only information related to the device state of the NBG6817.

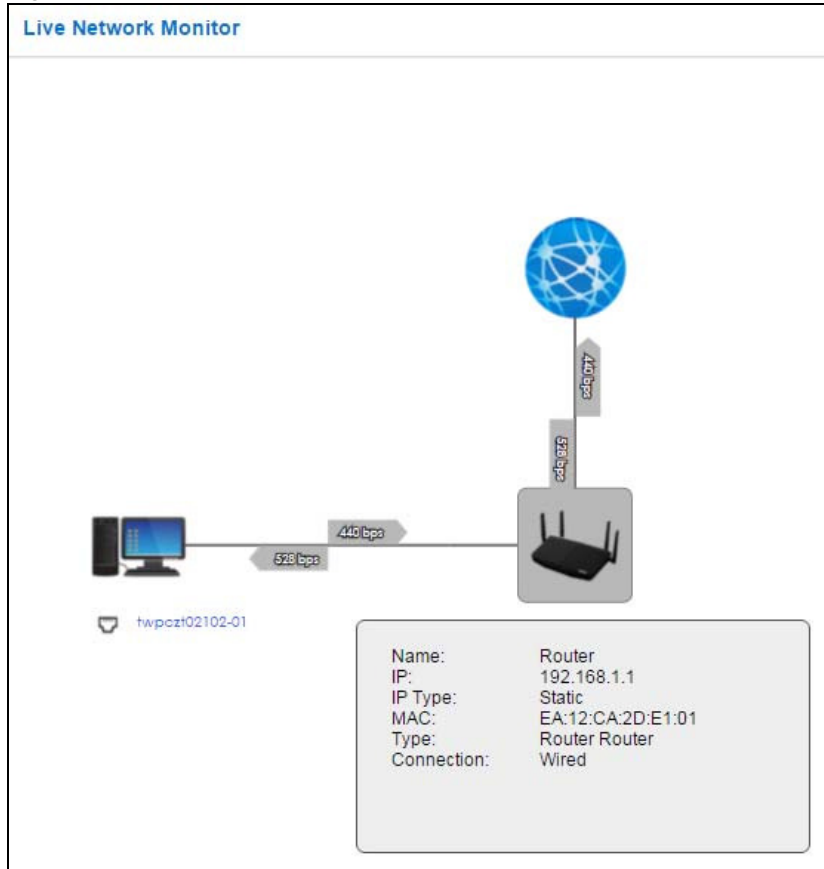
9.1.1 What You Can Do

- Use the **Live Network Monitor** screen to view transmission data rates between the NBG6817 and the Internet or connected devices ([Section 9.2 on page 60](#)).
- Use the **Usage Monitor** screen to view transmission data and bandwidth usage between the NBG6817 and applications or connected devices ([Section 9.3 on page 63](#)).
- Use the **Common Usage** screen to view the top five traffic flows transmitting from/to the selected LAN device(s) ([Section Figure 48 on page 69](#)).
- Use the **Download Traffic Statistics** screen to view the type and percentage of most download traffic ([Section 9.5 on page 70](#)).
- Use the **Client Tables** screen to view the online clients information ([Section 9.6 on page 71](#)).

9.2 Live Network Monitor Screen

Use this screen to view the current upstream and downstream transmission speeds between the NBG6817 and the Internet and/or between the NBG6817 and the connected device(s) (represented by icons indicating the kind of network device), including those connecting wirelessly.

Click **Expert Mode > Status > Live Network Monitor**. The following screen displays. You can move your mouse over a device icon to view information about the device, such as the name, IP address, MAC address, device type and connection type.

Figure 38 Expert Mode > Status > Live Network Monitor

Click a device icon to go to a screen that displays the upstream/downstream bandwidth as a line graph. If you click the NBG6817's icon, it also shows the transmission rate between the NBG6817 and each connected device. If you click a connected device's icon, you can see the current transmission rate for a traffic type. The green ball indicates the traffic flow is given enough bandwidth.

Figure 39 Expert Mode > Status > Live Network Monitor: Traffic Statistics (NBG6817)

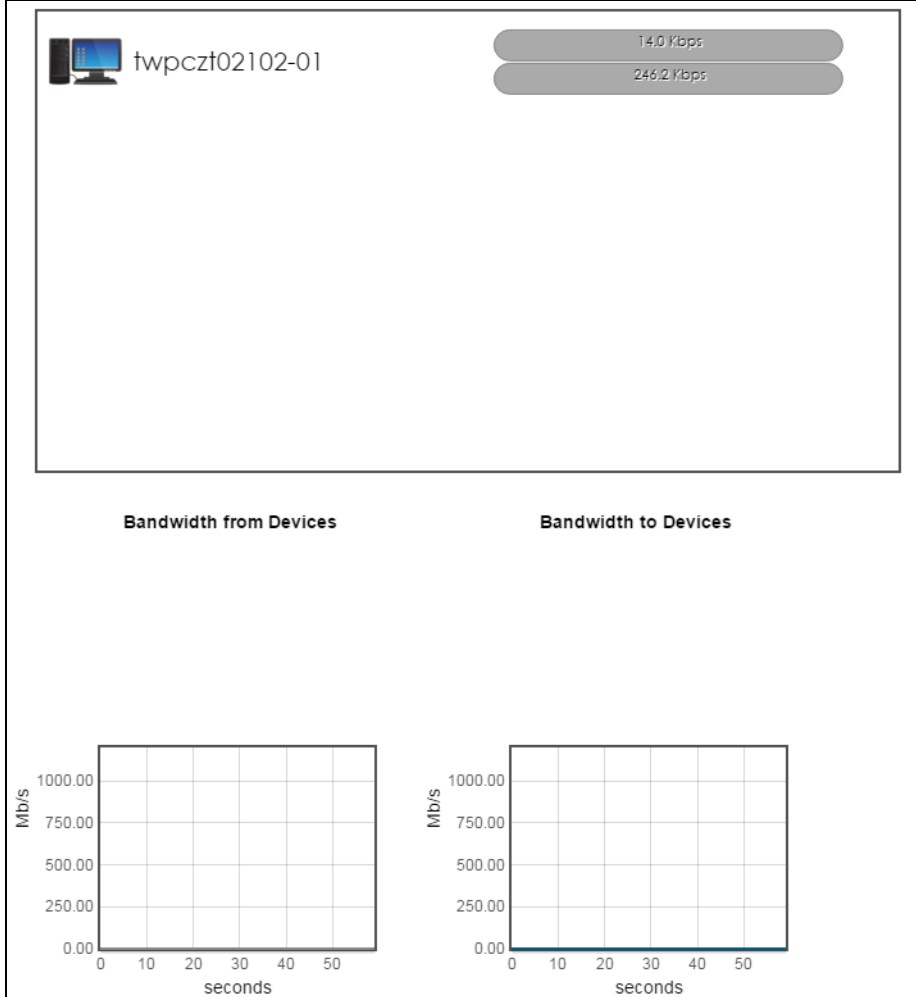
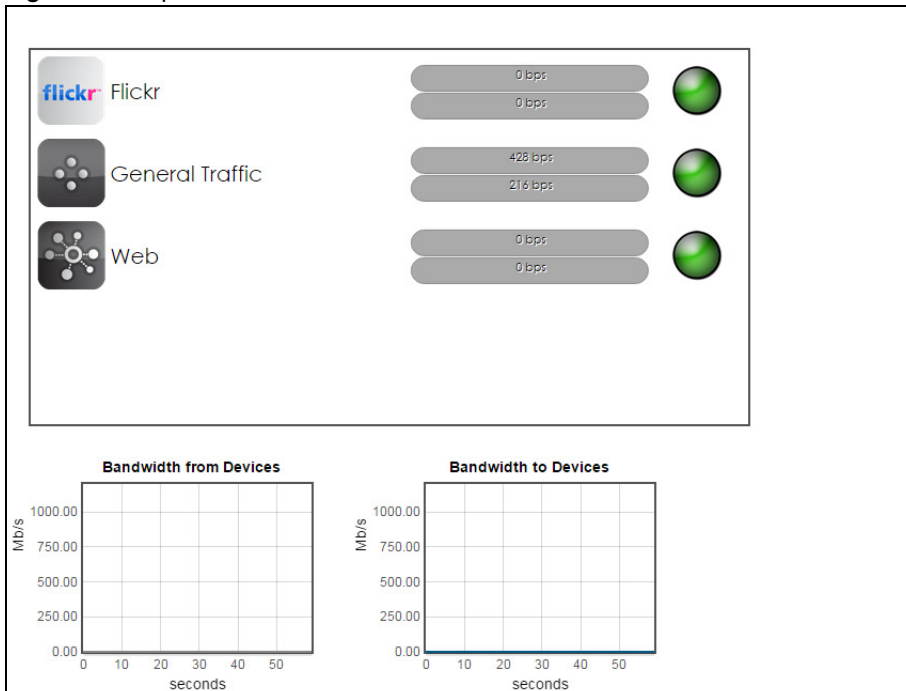


Figure 40 Expert Mode > Status > Live Network Monitor: Traffic Statistics (Connected Device)

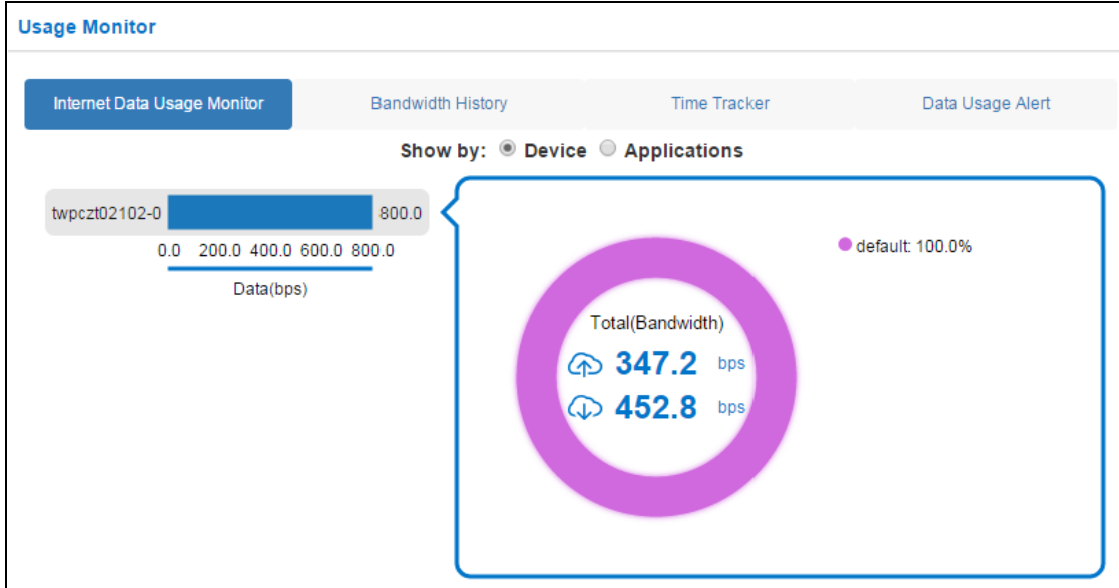
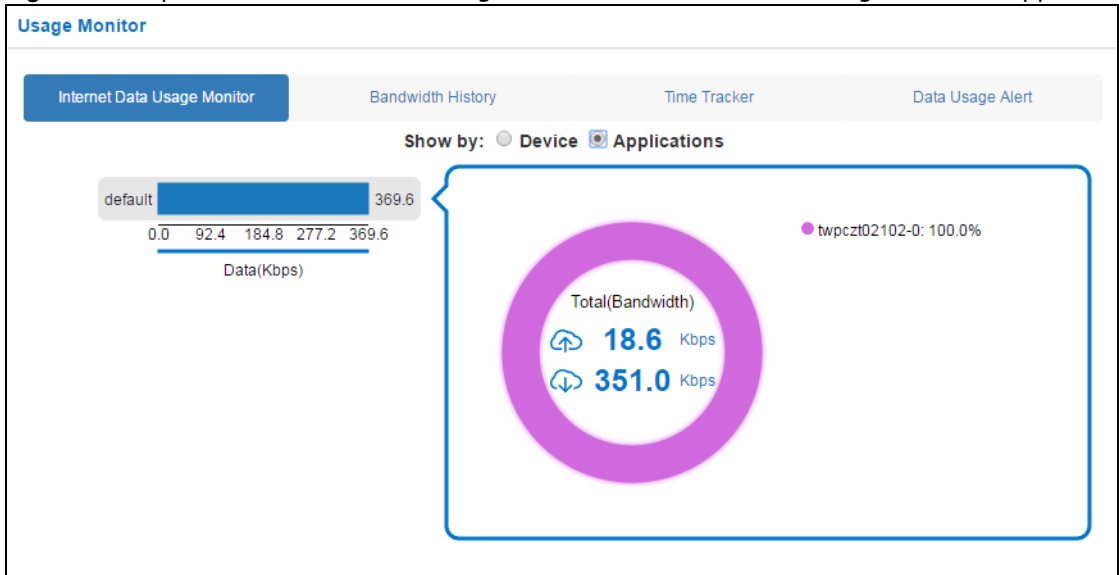
9.3 Usage Monitor Screens

- Use the **Internet Data Usage Monitor** screen to view the current amount of bandwidth being transmitted from/to the connected devices or applications ([Section 9.3.1 on page 63](#)).
- Use the **Bandwidth History** screen to view the upload/download peak being transmitted from/to the connected devices or applications ([Section 9.3.2 on page 64](#)).
- Use the **Time Tracker** screen to view the time period over which the traffic flow occurred from connected devices ([Section 9.3.3 on page 66](#)).
- Use the **Data Usage Alert** screen to view the amount of bandwidth and configure your data plan ([Section 9.3.4 on page 66](#)).

9.3.1 Internet Data Usage Monitor

Use this screen to view the current amount of bandwidth being transmitted from/to the connected LAN device(s) or applications. Select the device(s) or applications radio button to view the amount of uplink and downlink traffic by device(s) or applications.

Click **Expert Mode > Status > Usage Monitor > Internet Data Usage Monitor**. The following screen displays.

Figure 41 Expert Mode > Status > Usage Monitor > Internet Data Usage Monitor: Device**Figure 42** Expert Mode > Status > Usage Monitor > Internet Data Usage Monitor: Applications

9.3.2 Bandwidth History

Use this screen to view the peak upload (green) and download (blue) bandwidth in the past day, week, month, or quarter. Bandwidth history can be displayed by selecting the connected LAN device(s) or applications radio button. Select the time period and device(s) (or applications) from the drop-down list box to view the corresponding upload/download bandwidth. You can put your mouse in the gray bar and drag it to view the peak upload and download bandwidth. You can also put your cursor in the graph to view graph details.

Click **Expert Mode > Status > Usage Monitor > Bandwidth History**. The following screen displays.

Figure 43 Expert Mode > Status > Usage Monitor > Bandwidth History: Device

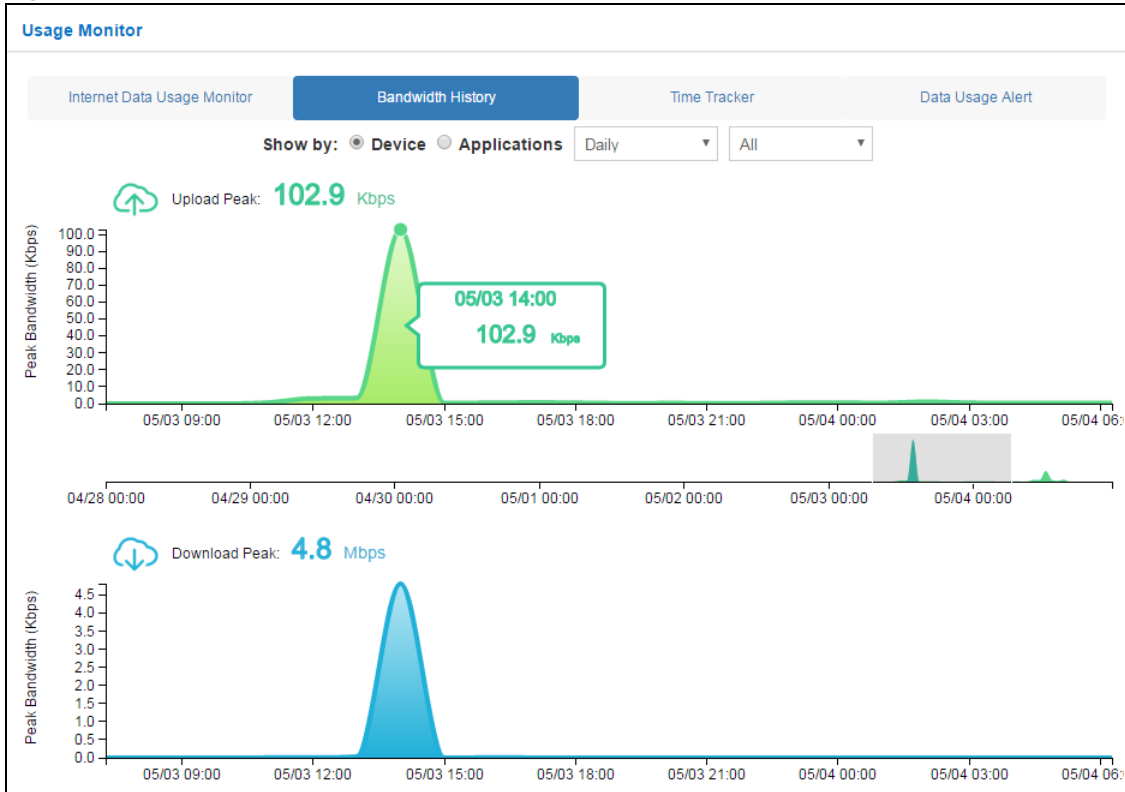
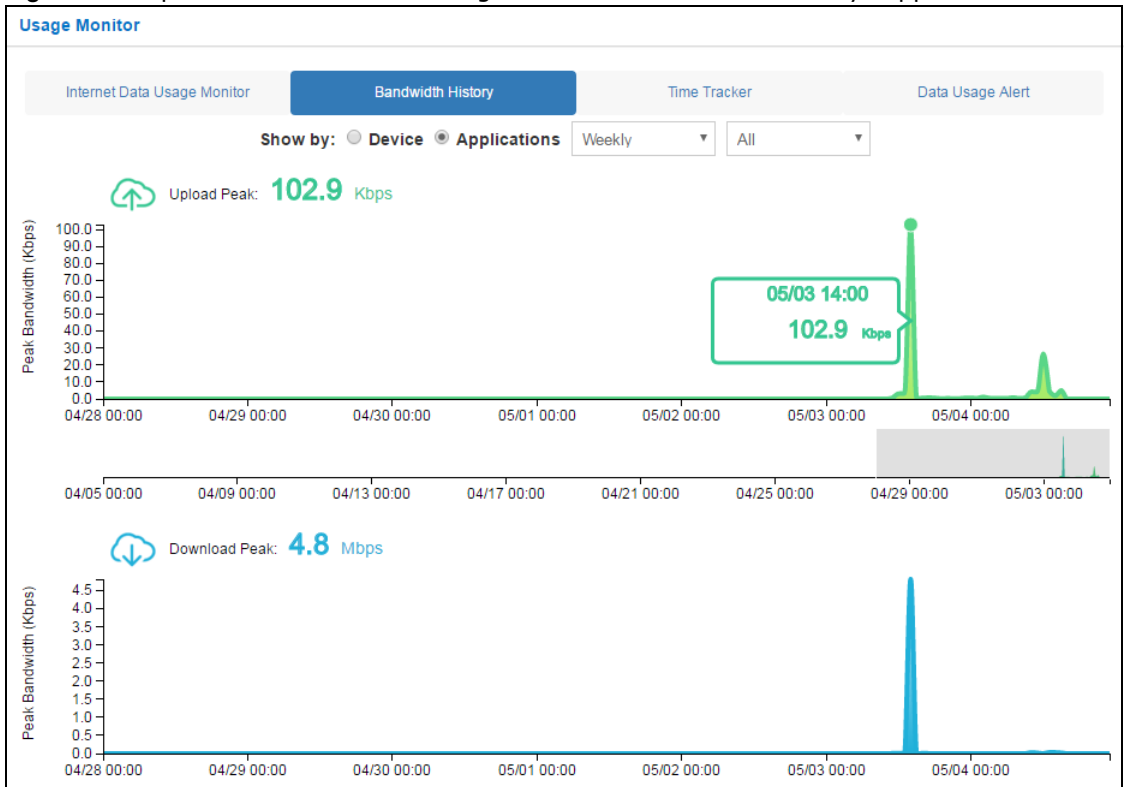



Figure 44 Expert Mode > Status > Usage Monitor > Bandwidth History: Applications

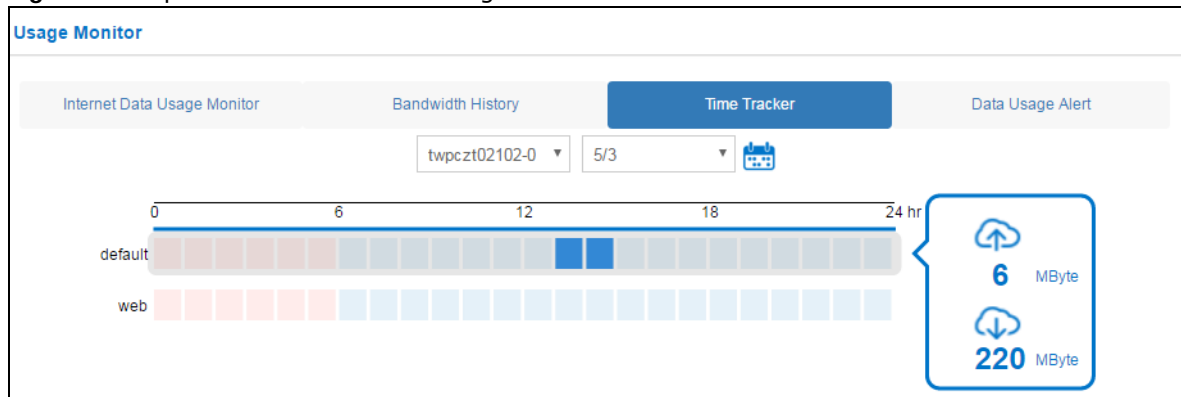


9.3.3 Time Tracker

Use this screen to view the time period over which the traffic flow occurred and the amount of uplink and downlink traffic generated in the past day, week, month, or quarter. Select the connected LAN device(s) from the drop-down list box and specify the time period to view the upload/download bandwidth. You can click the calendar icon () to choose the specified date.

Click **Expert Mode > Status > Usage Monitor > Time Tracker**. The following screen displays.

Figure 45 Expert Mode > Status > Usage Monitor > Time Tracker



9.3.4 Data Usage Alert

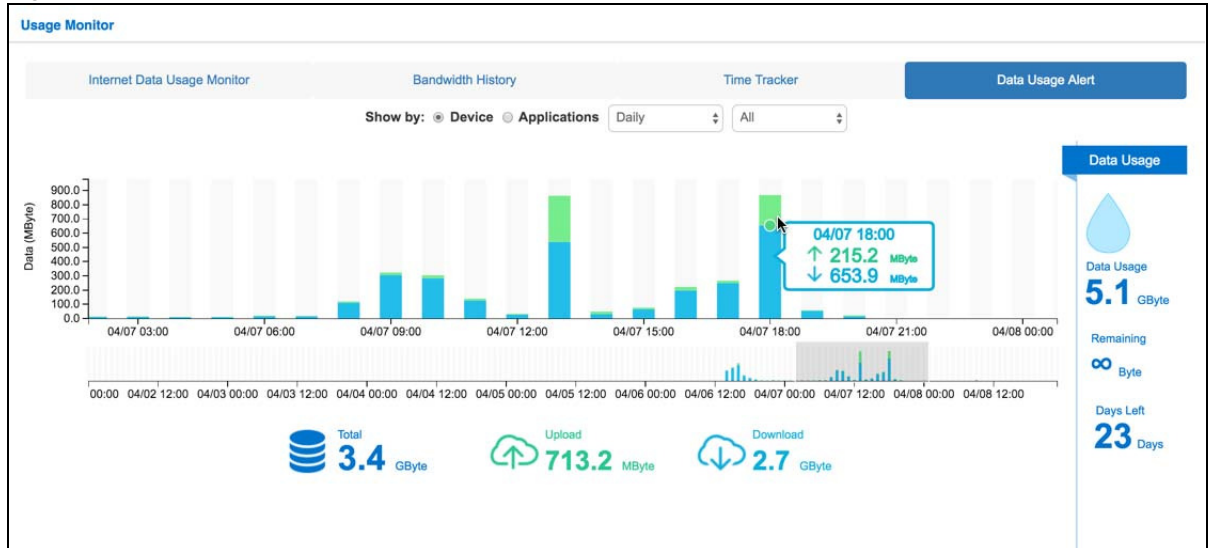
View data usage, data history and configure a data plan from this screen.

Data Usage Alert

Use this screen to view the upload (green) and download (blue) bandwidth in the past day, week, month, or quarter. Data usage can be displayed by selecting the connected LAN device(s) or applications radio button. Select the time period and device(s) (or applications) from the drop-down list box to view the corresponding upload/download bandwidth. You can put your mouse in the gray bar and drag it to view the upload and download bandwidth. You can also put your cursor in the graph to view graph details.

Click **Expert Mode > Status > Usage Monitor > Data Usage Alert**. The following screen displays.

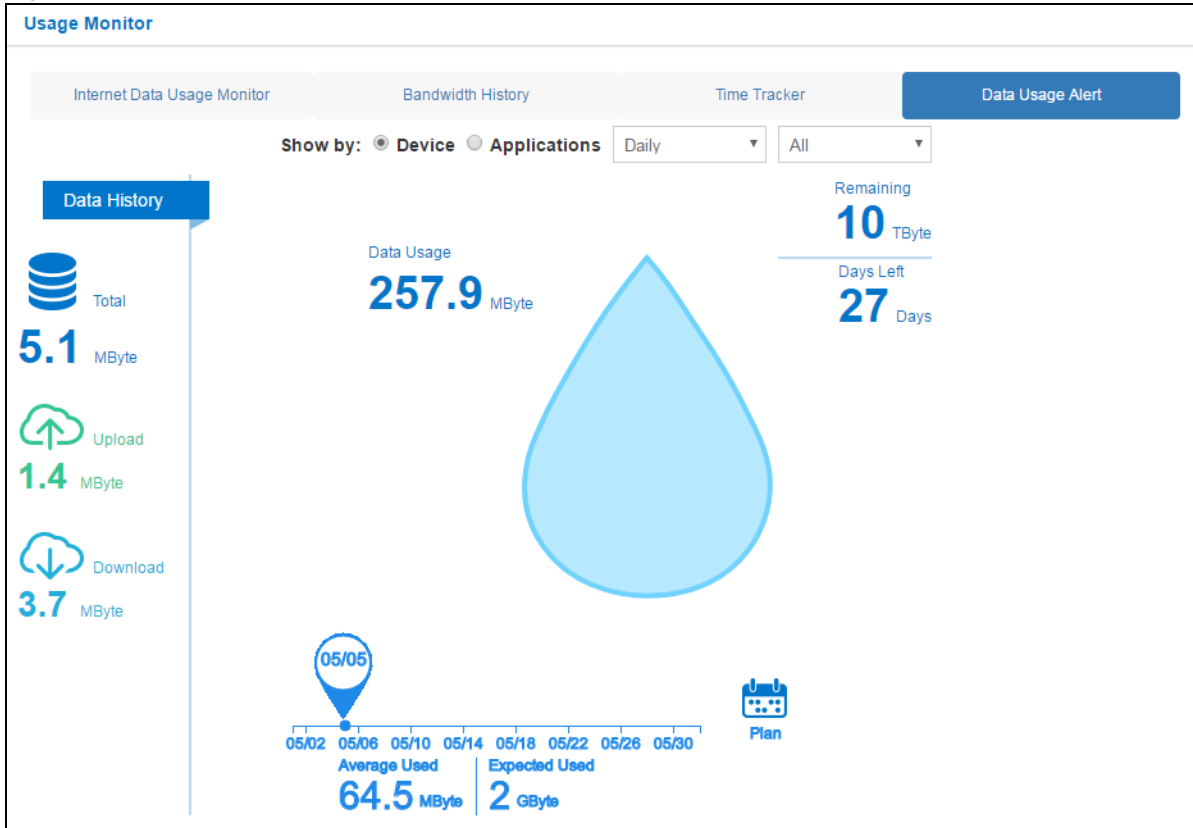
Figure 46 Expert Mode > Status > Usage Monitor > Data Usage Alert



Data History

Click **Data Usage** to view the remaining data usage allowed and remaining days to access the Internet. Use the **Data History** screen to view the upload (green) and download (blue) bandwidth in the past day, week, month, or quarter. Data history can be displayed by selecting the connected LAN device(s) or applications radio button. Select the time period and device(s) (or applications) from the drop-down list box to view the corresponding upload/download bandwidth. The following screen displays.

Figure 47 Expert Mode > Status > Usage Monitor > Data Usage Alert > Data Usage



Data Plan


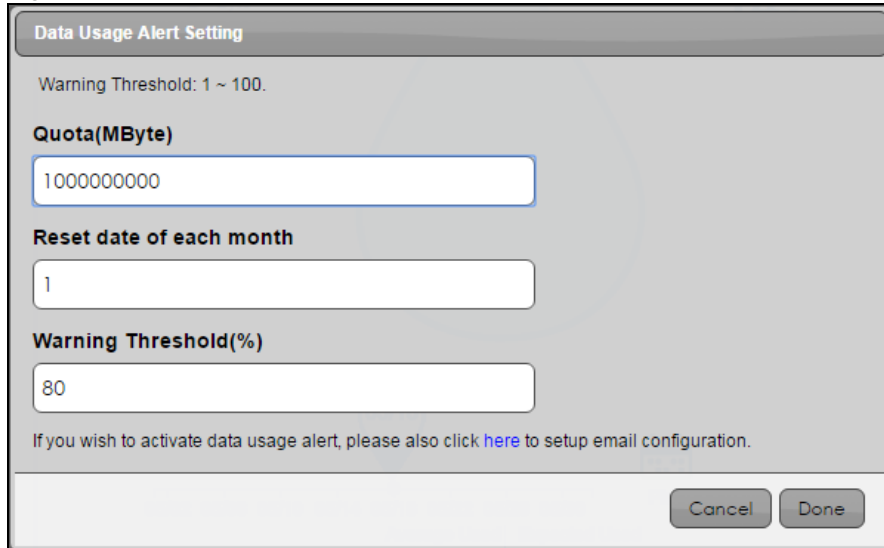
Click the data plan icon () to specify a data limit per month and the date data amounts used are reset. **Data Usage** displays the amount of data used from beginning. **Average Used** displays the average amount of data used from the beginning date to the current date, and **Expected Used** displays the expected amount data that will be used this month based on the **Average Used**. The following screen displays.

Figure 48 Expert Mode > Status > Usage Monitor > Data Usage Alert > Data Usage > Plan

The screenshot shows a dialog box titled "Data Usage Alert Setting". It contains the following fields and text:

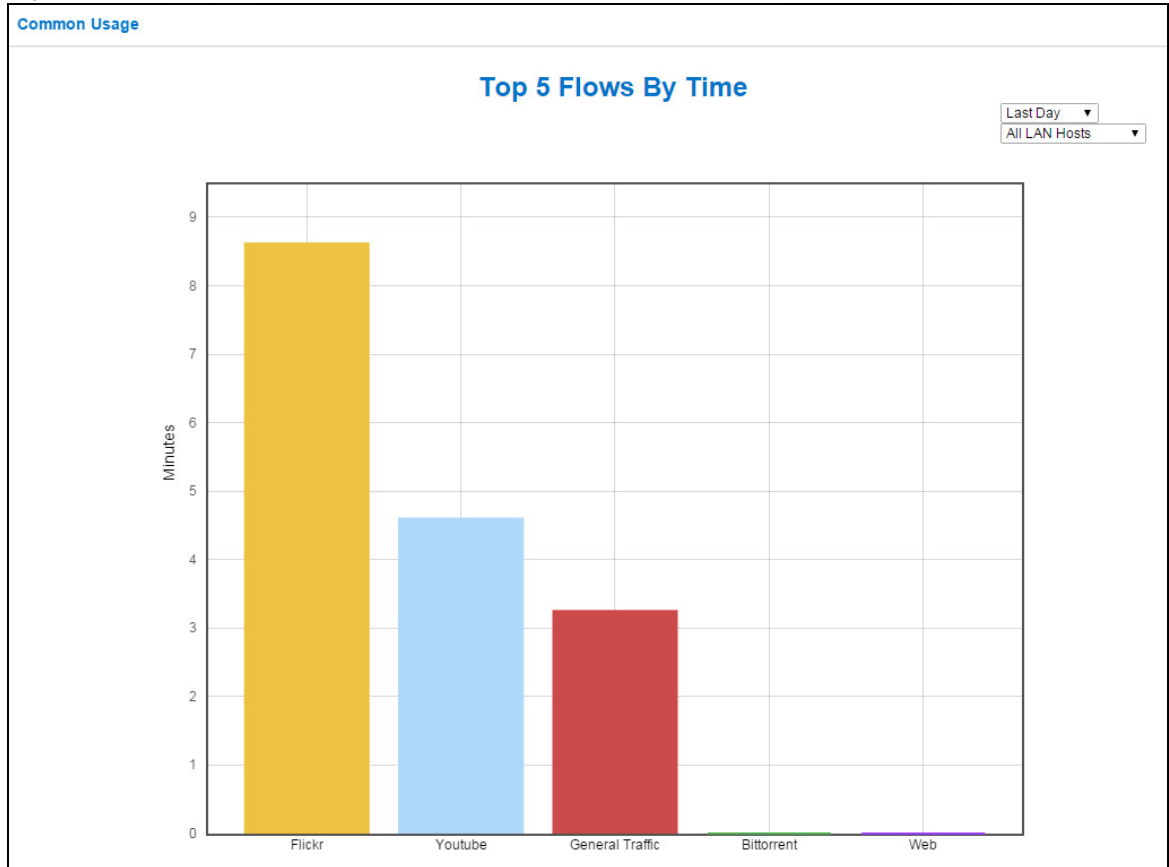
- Warning Threshold: 1 ~ 100.
- Quota(MByte)**: A text input field containing "100000000".
- Reset date of each month**: A text input field containing "1".
- Warning Threshold(%)**: A text input field containing "80".
- Text at the bottom: "If you wish to activate data usage alert, please also click [here](#) to setup email configuration."
- Buttons: "Cancel" and "Done".

9.4 Common Usage Screen

Use this screen to view the top five traffic flows transmitting from/to the selected LAN device(s) in the past day, week or month.

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

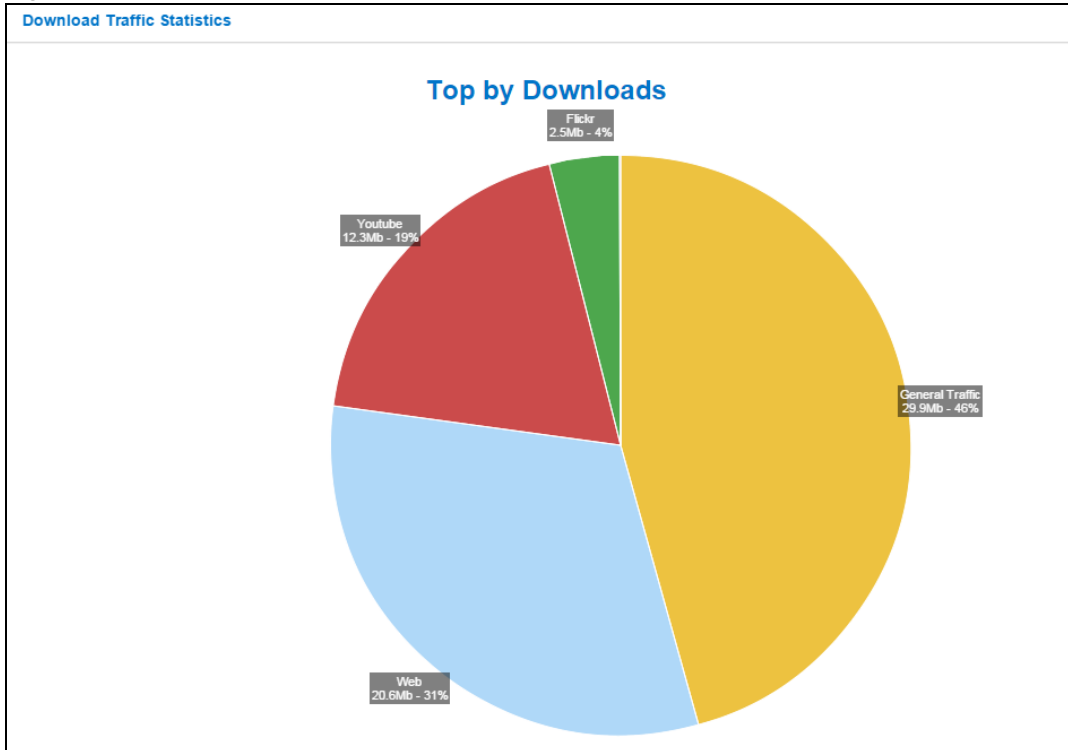
The y-axis shows the time period over which the traffic flow occurred. The x-axis shows the type of the traffic flow.

Figure 49 Expert Mode > Status > Common Usage

9.5 Download Traffic Statistics Screen

Use this screen to view the type and percentage of most download traffic on the NBG6817.

Click **Expert Mode > Status > Download Traffic Statistics** to open the **Download Traffic Statistics** screen.

Figure 50 Expert Mode > Status > Download Traffic Statistics

9.6 Client Tables Screen

You can configure the NBG6817's LAN as a DHCP server or disable it. When configured as a server, the NBG6817 assigns IP addresses to the clients. If DHCP service is disabled, you must have another DHCP server on that network, or else the computer must be manually configured.

Use this screen to view the online clients information (including Host Name, IP Address, MAC Address, Interface/Rssi, and Lease time) of all network clients using the NBG6817's DHCP server.

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

Figure 51 Expert Mode > Status > Client Tables

Client Tables								Apply	Cancel
Interface: <input type="text" value="ALL"/>									
DHCP Client Table									
#	Online	Host Name	IP Address	MAC Address	Interface/Rssi	Lease time	Reserve		
1		twpczt02102-01	192.168.1.88	c0:3f:d5:ba:9e:b7	LAN	2016-03-30 04:50	<input type="checkbox"/>		

The following table describes the labels in this screen.

Table 18 Expert Mode > Status > DHCP Table

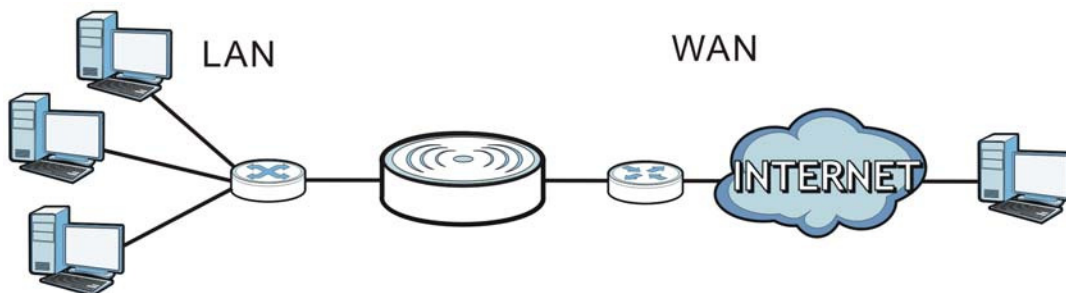
LABEL	DESCRIPTION
Interface	Select the interface from the drop-down list box to display current DHCP client information.
#	This is the index number of the host computer.
Online	This field displays whether the connection to the host computer is up (a yellow bulb) or down (a gray bulb).
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	This field shows the MAC address of the computer with the name in the Host Name field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Interface/Rssi	This field displays the device's interface type or received signal strength indicator (RSSI) that is currently connected to the NBG6817.
Lease time	This field displays the amount of time that the IP address is valid.
Reserve	Select this if you want to reserve the IP address for this specific MAC address.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to reload the previous configuration for this screen.

10.1 Overview

This chapter discusses the NBG6817's **WAN** screens. Use these screens to configure your NBG6817 for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 52 LAN and WAN



10.2 What You Can Do

- Use the **Internet Connection** screen to enter your ISP information and set how the computer acquires its IP, DNS and WAN MAC addresses ([Section 10.4 on page 76](#)).
- Use the **NAT > General** screen to enable NAT, set a default server and change your NBG6817's port forwarding settings ([Section 10.5.1 on page 88](#)).
- Use the **NAT > Port Trigger** screen to configure your NBG6817's trigger port settings ([Section 10.5.2 on page 90](#)).
- Use the **NAT > Passthrough** screen to configure your NBG6817's ALGs and VPN pass-through settings ([Section 10.5.3 on page 90](#)).
- Use the **Dynamic DNS** screen to change your NBG6817's DDNS settings ([Section 10.6 on page 92](#)).

10.3 What You Need To Know

The information in this section can help you configure the screens for your WAN connection, as well as enable/disable some advanced features of your NBG6817.

10.3.1 Configuring Your Internet Connection

Encapsulation Method

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

WAN IP Address

The WAN IP address is an IP address for the NBG6817, which makes it accessible from an outside network. It is used by the NBG6817 to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the NBG6817 tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The NBG6817 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 NBG6817's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

WAN MAC Address

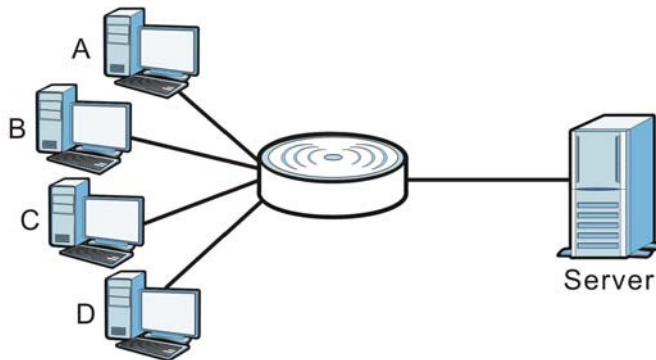
The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

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.

Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

Figure 53 Multicast Example



In the multicast example above, systems A and D comprise one multicast group. In multicasting, the server only needs to send one data stream and this is delivered to systems A and D.

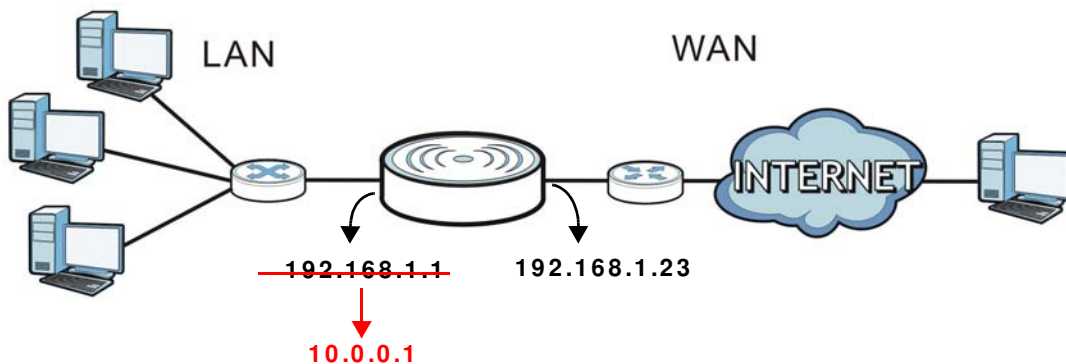
IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. The NBG6817 supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**).

At start up, the NBG6817 queries all directly connected networks to gather group membership. After that, the NBG6817 periodically updates this information. IP multicasting can be enabled/disabled on the NBG6817 WAN interface in the Web Configurator (**WAN**). Select **None** to disable IP multicasting on these interfaces.

Auto-IP Change

When the NBG6817 gets a WAN IP address or a DNS server IP address which is in the same subnet as the LAN IP address 192.168.1.1, Auto-IP-Change allows the NBG6817 to change its LAN IP address to 10.0.0.1 automatically. If the NBG6817'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 NBG6817 switches to use 192.168.1.1 as its LAN IP address.

Figure 54 Auto-IP-Change Example



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

- The NBG6817 must be in **Router Mode** (see [Section 15.12 on page 160](#) for more information) for Auto-IP-Change to become active.
- The NBG6817 is set to receive a dynamic WAN IP address.

10.4 Internet Connection Screen

Use this screen to change your NBG6817's Internet access settings. Click **Expert Mode > WAN > Internet Connection**.

10.4.1 IPoE Encapsulation

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

Figure 55 Expert Mode > WAN > Internet Connection: IPoE Encapsulation (IPv4 Only)

Internet Connection		Apply	Cancel
ISP Parameters for Internet Access			
Encapsulation :	IPoE ▼		
IPv4 / IPv6 :	IPv4 Only ▼		
<hr/>			
IP Address			
<input checked="" type="radio"/> Obtain an IP Address Automatically(DHCP) <input type="radio"/> Static IP Address			
IP Address :	<input type="text"/>		
Subnet Mask :	<input type="text"/>		
Default Gateway :	<input type="text"/>		
MTU Size :	1500		
<hr/>			
DNS Server			
First DNS Server :	Obtained From ISP ▼	<input type="text"/>	
Second DNS Server :	Obtained From ISP ▼	<input type="text"/>	
Third DNS Server :	Obtained From ISP ▼	<input type="text"/>	
<hr/>			
WAN MAC Address			
<input checked="" type="radio"/> Factory default <input type="radio"/> Clone the computer's MAC address - IP Address <input type="text"/> <input type="radio"/> Set WAN MAC Address <input type="text"/>			
<hr/>			
IPv6 Tunneling			
IPv6 Tunneling :	6RD ▼		
<input type="radio"/> Automatically configured by DHCPC <input checked="" type="radio"/> Manually Configured			
Border Relay IPv4 Address:	<input type="text"/>		
Service Provider IPv6 Prefix:	<input type="text"/>		
Service Provider IPv6 Prefix length:	32	32~64	
IPv4 mask length:	0	0~32	
<hr/>			
IPv6 DNS Server			
First DNS Server :	<input type="text"/>		
Second DNS Server :	<input type="text"/>		
Third DNS Server :	<input type="text"/>		
<hr/>			
Multicast Setup			
Multicast Setup :	IGMPv1/v2 ▼		
<hr/>			
Auto-Subnet Configuration			
<input checked="" type="checkbox"/> Enable Auto-IP-Change Mode			

The following table describes the labels in this screen.

Table 19 Network > WAN > Internet Connection: IPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the IPoE option when the WAN port is used as a regular Ethernet.
IPv4 / IPv6	Select IPv4 Only if you want the NBG6817 to run IPv4 only. Select Dual Stack to allow the NBG6817 to run IPv4 and IPv6 at the same time. Select IPv6 Only if you want the NBG6817 to run IPv6 only.
IP Address	
Obtain an IP Address Automatically (DHCP)	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected Static IP Address .
Subnet Mask	Enter the Subnet Mask in this field.
Default 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 NBG6817 divides it into smaller fragments.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the NBG6817's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	
Once the WAN MAC address is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file.	
Factory default	Select this option to have the WAN interface use the factory assigned default MAC address. By default, the NBG6817 uses the factory assigned MAC address to identify itself.
Clone the computer's MAC address - IP 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.
IPv6 Tunneling	
Use IPv6 tunneling when the local network uses IPv6 and the ISP has an IPv4 network. When the NBG6817 has an IPv4 WAN address and you set IPv4/IPv6 mode to IPv4 Only , you can enable IPv6 tunneling to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network.	

Table 19 Network > WAN > Internet Connection: IPoE Encapsulation (continued)

LABEL	DESCRIPTION
IPv6 Tunneling	<p>Select None to not allow IPv6 packets to cross IPv4 networks.</p> <p>Select 6RD to enable 6RD. IPv6 Rapid Deployment (6RD) is an IPv6 transitioning process for stateless tunneling of IPv6 over IPv4. Enable 6RD to allow tunneling across an ISP's IPv4 only access network.</p> <p>Select 6to4 to transmit IPv6 packets over an IPv4 network. A 6to4 relay router is required to route 6to4 packets to a native IPv6 network.</p> <p>Select 6in4 if the NBG6817 has a public IPv4 address and you want to transmit your IPv6 packets to one and only one remote site whose LAN network is also an IPv6 network. You must know the WAN IP address of the remote gateway.</p>
6RD	<p>The NBG6817 generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router to connect to the native IPv6 Internet. The local network can also use IPv4 services. The NBG6817 uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.</p> <p>This is available only when you select IPv4 Only in the IPv4/IPv6 field.</p>
Automatically configured by DHCP	Select this to have the NBG6817 detect the relay server's IP address automatically through DHCP.
Manually Configured	Select this if you have the IPv4 address of the relay server.
Border Relay IPv4 Address	Specify the relay server's IPv4 address.
Service Provider IPv6 Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's Border Relay router and connecting to the native IPv6 Internet.
Service Provider IPv6 Prefix length	<p>Enter the IPv6 prefix length.</p> <p>An IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address.</p>
IPv4 mask length	Enter the subnet mask number (1~32) for the IPv4 network.
6to4	<p>The NBG6817 should get a public IPv4 address for the WAN. The NBG6817 adds an IPv4 IP header to an IPv6 packet when transmitting the packet to the Internet. In reverse, the NBG6817 removes the IPv4 header from an IPv6 packet when receiving it from the Internet.</p> <p>This is available only when you select IPv4 Only in the IPv4/IPv6 field.</p>
Relay Server IPv4 Address	Enter the IPv4 address of a 6to4 relay server which helps forward packets between 6to4 networks and native IPv6 networks.
6in4	<p>The NBG6817 encapsulates IPv6 packets within IPv4 packets across the Internet. You must know the WAN IP address of the remote gateway device. This mode is normally used for a site-to-site application such as two branch offices.</p> <p>This is available only when you select IPv4 Only in the IPv4/IPv6 field.</p>
Remote IPv4 Address	Enter the IPv4 address of the remote gateway to which this interface tunnels traffic.
Remote IPv6 Address	Enter the IPv6 address of the remote gateway to which this interface tunnels traffic.
Local IPv6 Address	Enter the IPv6 address assigned by your ISP.
IPv6 Prefix	Enter the IPv6 prefix for this interface if you want to use a static IP address.

Table 19 Network > WAN > Internet Connection: IPoE Encapsulation (continued)

LABEL	DESCRIPTION
IPv6 DNS Server	This is available only when you select IPv4 Only in the IPv4/ IPv6 field and set IPv6 Tunneling to 6RD , 6in4 or 6to4 .
First DNS Server Second DNS Server Third DNS Server	Specify the DNS server IPv6 address assigned by the ISP.
IPv6 Address	This section is NOT available when you select IPv4 Only in the IPv4/ IPv6 field.
Obtain an IP Address Automatically(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 NBG6817 use DUID-LL (DUID Based on Link-layer Address) for identification when exchanging DHCPv6 messages. • Select DUID-LLT to have the NBG6817 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.
IPv6 Default 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 is available only when you select Dual Stack or IPv6 Only in the IPv4/ IPv6 field.
First DNS Server Second DNS Server Third DNS Server	Select Obtained From ISP to have the NBG6817 get the IPv6 DNS server addresses from the ISP automatically. Select User-Defined and enter the IPv6 DNS server address assigned by the ISP to have the NBG6817 use the IPv6 DNS server addresses you configure manually. Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IPv6 address of a computer in order to access it.
Multicast Setup	Select IGMPv1/ v2 to enable multicasting. This applies to traffic routed from the WAN to the LAN. Select None to disable this feature. This may cause incoming traffic to be dropped or sent to all connected network devices.
Auto-Subnet Configuration	Select this option to have the NBG6817 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG6817 gets a dynamic WAN IP address in the same subnet as the LAN IP address. Select this option to have the NBG6817 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG6817 gets a DNS server IP address in the same subnet as the LAN IP address. The NAT, DHCP server and firewall functions on the NBG6817 are still available in this mode.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

10.4.2 PPPoE Encapsulation

The NBG6817 supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** option is for a dial-up connection using PPPoE.

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

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

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the NBG6817 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG6817 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 56 Network > WAN > Internet Connection: PPPoE Encapsulation (IPv4 Only)

Internet Connection		Apply	Cancel
ISP Parameters for Internet Access			
Encapsulation :	PPPoE ▼		
IPv4 / IPv6 :	IPv4 Only ▼		
PPP Information			
PPP Username :	<input type="text"/>		
PPP Password :	<input type="password"/>		
MTU Size :	1454		
PPP Auto Connect :	<input checked="" type="checkbox"/>		
IDLE Timeout [second] :	300		
PPPoE Service Name :	<input type="text"/>		
WAN IP Address Assignment			
<input type="radio"/> Get automatically from ISP			
<input checked="" type="radio"/> Use Fixed IP Address			
	<input type="text"/>		
DNS Server			
First DNS Server :	User-Defined ▼	<input type="text"/>	
Second DNS Server :	User-Defined ▼	<input type="text"/>	
Third DNS Server :	User-Defined ▼	<input type="text"/>	
WAN MAC Address			
<input checked="" type="radio"/> Factory default			
<input type="radio"/> Clone the computer's MAC address - IP Address			
	<input type="text"/>		
<input type="radio"/> Set WAN MAC Address			
	<input type="text"/>		
IPv6 Tunneling			
IPv6 Tunneling :	6in4 ▼		
Remote IPv4 Address:	<input type="text"/>		
Remote IPv6 Address:	<input type="text"/>		
Local IPv6 Address:	<input type="text"/>		
IPv6 Prefix:	<input type="text"/>		
IPv6 DNS Server			
First DNS Server :	<input type="text"/>		
Second DNS Server :	<input type="text"/>		
Third DNS Server :	<input type="text"/>		
Multicast Setup			
Multicast Setup :	IGMPv1/V2 ▼		
Auto-Subnet Configuration			
<input checked="" type="checkbox"/> Enable Auto-IP-Change Mode			

The following table describes the labels in this screen.

Table 20 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select PPPoE if you connect to your Internet via dial-up.
IPv4 / IPv6	Select IPv4 Only if you want the NBG6817 to run IPv4 only. Select Dual Stack to allow the NBG6817 to run IPv4 and IPv6 at the same time. Select IPv6 Only if you want the NBG6817 to run IPv6 only.
PPP Information	
PPP Username	Type the user name given to you by your ISP.
PPP Password	Type the password associated with the user name above.
MTU Size	Enter the Maximum Transmission Unit (MTU) or the largest packet size per frame that your NBG6817 can receive and process.
PPP Auto Connect	Select this option if you do not want the connection to time out.
IDLE Timeout (second)	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
PPPoE Service Name	Enter the PPPoE service name specified in the ISP account.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option and enter your WAN IP address if the ISP assigned a fixed IP address.
DNS Server	
First DNS Server	Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the NBG6817'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 None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	
The MAC address section allows users to configure the WAN port's MAC address by using the NBG6817's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.	
Factory default	Select Factory default to use the factory assigned default MAC Address.
Clone the computer's MAC address - IP Address	Select Clone the computer's MAC address - IP Address and enter the IP address of the computer on the LAN whose MAC you are cloning.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
IPv6 Tunneling	
Use IPv6 tunneling when the local network uses IPv6 and the ISP has an IPv4 network. When the NBG6817 has an IPv4 WAN address and you set IPv4 / IPv6 mode to IPv4 Only , you can enable IPv6 tunneling to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network.	

Table 20 Network > WAN > Internet Connection: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
IPv6 Tunneling	<p>Select None to not allow IPv6 packets to cross IPv4 networks.</p> <p>Select 6RD to enable 6RD. IPv6 Rapid Deployment (6RD) is an IPv6 transitioning process for stateless tunneling of IPv6 over IPv4. Enable 6RD to allow tunneling across an ISP's IPv4 only access network.</p> <p>Select 6to4 to transmit IPv6 packets over an IPv4 network. A 6to4 relay router is required to route 6to4 packets to a native IPv6 network.</p> <p>Select 6in4 if the NBG6817 has a public IPv4 address and you want to transmit your IPv6 packets to one and only one remote site whose LAN network is also an IPv6 network. You must know the WAN IP address of the remote gateway.</p>
6RD	<p>The NBG6817 generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router to connect to the native IPv6 Internet. The local network can also use IPv4 services. The NBG6817 uses its configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.</p> <p>This is available only when you select IPv4 Only in the IPv4/IPv6 field.</p>
Automatically configured by DHCP	Select this to have the NBG6817 detect the relay server's IP address automatically through DHCP.
Manually Configured	Select this if you have the IPv4 address of the relay server.
Border Relay IPv4 Address	Specify the relay server's IPv4 address.
Service Provider IPv6 Prefix	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's Border Relay router and connecting to the native IPv6 Internet.
Service Provider IPv6 Prefix length	<p>Enter the IPv6 prefix length.</p> <p>An IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address.</p>
IPv4 mask length	Enter the subnet mask number (1~32) for the IPv4 network.
6to4	<p>The NBG6817 should get a public IPv4 address for the WAN. The NBG6817 adds an IPv4 IP header to an IPv6 packet when transmitting the packet to the Internet. In reverse, the NBG6817 removes the IPv4 header from an IPv6 packet when receiving it from the Internet.</p> <p>This is available only when you select IPv4 Only in the IPv4/IPv6 field.</p>
Relay Server IPv4 Address	Enter the IPv4 address of a 6to4 relay server which helps forward packets between 6to4 networks and native IPv6 networks.
6in4	<p>The NBG6817 encapsulates IPv6 packets within IPv4 packets across the Internet. You must know the WAN IP address of the remote gateway device. This mode is normally used for a site-to-site application such as two branch offices.</p> <p>This is available only when you select IPv4 Only in the IPv4/IPv6 field.</p>
Remote IPv4 Address	Enter the IPv4 address of the remote gateway to which this interface tunnels traffic.
Remote IPv6 Address	Enter the IPv6 address of the remote gateway to which this interface tunnels traffic.
Local IPv6 Address	Enter the IPv6 address assigned by your ISP.
IPv6 Prefix	Enter the IPv6 prefix for this interface if you want to use a static IP address.

Table 20 Network > WAN > Internet Connection: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
IPv6 DNS Server	This is available only when you select IPv4 Only in the IPv4/IPv6 field and set IPv6 Tunneling to 6RD , 6in4 or 6to4 .
First DNS Server Second DNS Server Third DNS Server	Specify the DNS server IPv6 address assigned by the ISP.
IPv6 DNS Server	This is available only when you select Dual Stack or IPv6 Only in the IPv4/IPv6 field.
First DNS Server Second DNS Server Third DNS Server	<p>Select Obtained From ISP to have the NBG6817 get the IPv6 DNS server addresses from the ISP automatically.</p> <p>Select User-Defined and enter the IPv6 DNS server address assigned by the ISP to have the NBG6817 use the IPv6 DNS server addresses you configure manually.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IPv6 address of a computer in order to access it.</p>
Multicast Setup	
Multicast Setup	<p>Select IGMPv1/v2 to enable multicasting. This applies to traffic routed from the WAN to the LAN.</p> <p>Select None to disable this feature. This may cause incoming traffic to be dropped or sent to all connected network devices.</p>
Auto-Subnet Configuration	
Enable Auto-IP-Change Mode	<p>Select this option to have the NBG6817 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG6817 gets a dynamic WAN IP address in the same subnet as the LAN IP address.</p> <p>Select this option to have the NBG6817 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG6817 gets a DNS server IP address in the same subnet as the LAN IP address.</p> <p>The NAT, DHCP server and firewall functions on the NBG6817 are still available in this mode.</p>
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

10.4.3 PPTP Encapsulation

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

Figure 57 Expert Mode > WAN > Internet Connection: PPTP Encapsulation (IPv4 Only)

Internet Connection	Apply	Cancel
ISP Parameters for Internet Access		
Encapsulation :	PPTP ▾	
IPv4 / IPv6 :	IPv4 Only ▾	
PPTP Information		
PPTP Username :	<input type="text"/>	
PPTP Password :	<input type="text"/>	
PPTP Encryption Type :	Auto ▾	
MTU Size :	1492	
PPTP Auto Connect :	<input checked="" type="checkbox"/>	
IDLE Timeout [second] :	300	
PPTP CONFIGURATION		
PPTP Server IP Address :	<input type="text"/>	
<input checked="" type="radio"/> Obtain an IP Address Automatically(DHCP) <input type="radio"/> Static IP Address		
IP Address :	<input type="text"/>	
Subnet Mask :	<input type="text"/>	
Default Gateway :	<input type="text"/>	
WAN IP Address Assignment		
<input checked="" type="radio"/> Get automatically from ISP <input type="radio"/> Use Fixed IP Address		
IP Address :	<input type="text"/>	
DNS Server		
First DNS Server :	Obtained From ISP ▾	<input type="text" value="172.21.65.1"/>
Second DNS Server :	Obtained From ISP ▾	<input type="text" value="172.23.5.2"/>
Third DNS Server :	Obtained From ISP ▾	<input type="text"/>
WAN MAC Address		
<input checked="" type="radio"/> Factory default <input type="radio"/> Clone the computer's MAC address - <input type="text"/> <input type="radio"/> Set WAN MAC Address <input type="text"/>		
IPv6 Tunneling		
IPv6 Tunneling :	None ▾	
Multicast Setup		
Multicast Setup :	IGMPv1/v2 ▾	
Auto-Subnet Configuration		
<input checked="" type="checkbox"/> Enable Auto-IP-Change Mode		

The following table describes the labels in this screen.

Table 21 Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select PPTP if you want to connect the Internet via point to point tunneling protocol.
IPv4 / IPv6	This field is greyed out. The PPTP encapsulation only supports IPv4.
PPTP Information	
PPTP Username	Enter the user name given to you by your ISP.
PPTP 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. No Encryption - This ISP account does not use MPPE. MPPE 40 - This ISP account uses 40-bit MPPE. MPPE 128 - This ISP account uses 128-bit MMPE.
MTU Size	Enter the MTU (Maximum Transmission Unit) size for each packet. If a larger packet arrives, the NBG6817 divides it into smaller fragments.
PPTP Auto Connect	Select this option if you do not want the connection to time out.
IDLE Timeout [second]	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server. 0 means no timeout.
PPTP CONFIGURATION	
PPTP Server IP Address	Enter the IP address of the PPTP server.
Obtain an IP Address Automatically(DHCP)	Select this radio button if the PPTP server did not assign you a fixed IP address.
Static IP Address	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.
Subnet Mask	Enter the IP subnet mask in this field.
Default Gateway	Enter the gateway IP address in this field.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected Static IP Address .
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the NBG6817's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.

Table 21 Network > WAN > Internet Connection: PPTP Encapsulation (continued)

LABEL	DESCRIPTION
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 NBG6817 uses the factory assigned MAC address to identify itself.
Clone the 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.
Multicast Setup	
Multicast Setup	Select IGMPv1 / v2 to enable multicasting. This applies to traffic routed from the WAN to the LAN. Select None to disable this feature. This may cause incoming traffic to be dropped or sent to all connected network devices.
Auto-Subnet Configuration	
Enable Auto-IP-Change Mode	Select this option to have the NBG6817 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG6817 gets a dynamic WAN IP address in the same subnet as the LAN IP address. Select this option to have the NBG6817 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG6817 gets a DNS server IP address in the same subnet as the LAN IP address. The NAT, DHCP server and firewall functions on the NBG6817 are still available in this mode.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

10.5 NAT

Use this screen to change your NBG6817's NAT (Network Address Translation) settings. Click **Expert Mode > WAN > NAT**.

10.5.1 General Screen

Use this screen to enable NAT, set a default server and configure your NBG6817's port forwarding settings to forward incoming service requests to the server(s) on your local network. Click **Expert Mode > WAN > NAT > General**.

Figure 58 Expert Mode > WAN > NAT > General

General		Apply	Cancel		
Network Address Translation(NAT): <input checked="" type="radio"/> Enable <input type="radio"/> Disable					
Default Server Setup					
<input checked="" type="radio"/> Default Server:		192.168.1.1			
<input type="radio"/> Change To Server:		twpczt02102-01	192.168.1.88		
Port Forwarding (Max Limit : 32)					
#	Name	Protocol	External Port	Server IP Address	Internal Port
	WWW	TCP_UDI	80	twpczt02102-01	192.168.1.88
1	HTTPS	TCP	443	192.168.1.100	443
2	User define	TCP_UDP	20	192.168.1.88	20
Note: If you want to forward a Port Range to LAN client, just leave the Internal Port empty.					

The following table describes the labels in this screen.

Table 22 Expert Mode > WAN > NAT > General

LABEL	DESCRIPTION
General	
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.
Default 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 (Max Limit : 32)	
#	This is the number of an individual port forwarding server entry.
Name	Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will be displayed in the port forwarding summary table. Otherwise, select User define to manually enter the port number/range and select the Protocol .
Protocol	Select the transport layer protocol supported by this virtual server. Choices are TCP , UDP , or TCP_UDP . If you have chosen a pre-defined service in the Name field, the protocol will be configured automatically.
External Port	This shows the port number(s) that identifies the service if you select a pre-defined service. If you select User define in the Name field, enter the port number(s) manually.
Server IP Address	Select User define to manually enter the inside IP address of the virtual server here.
Internal Port	This shows the port number(s) that identifies the service if you select a pre-defined service. If you select User define in the Name field, enter an internal port number manually or leave the field blank for port range forwarding.

Table 22 Expert Mode > WAN > NAT > General (continued)

LABEL	DESCRIPTION
Add	Click + to add the rule in the port forwarding summary table.
Delete	Click - to remove a rule.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

10.5.2 Port Trigger Screen

To change your NBG6817's trigger port settings, click **Expert Mode > WAN > NAT > Port Trigger**. The screen appears as shown.

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

Figure 59 Expert Mode > WAN > NAT > Port Trigger

The following table describes the labels in this screen.

Table 23 Expert Mode > WAN > NAT > Port Trigger

LABEL	DESCRIPTION
Port Trigger Rules (Max Limit : 32)	
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming 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 NBG6817 forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger Port	The trigger port is a port (or a range of ports) that causes (or triggers) the NBG6817 to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Add	Click + to add the rule in the port trigger summary table.
Delete	Click - to remove a rule.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

10.5.3 Passthrough Screen

ALG Overview

Application Layer Gateway (ALG) allows the following applications to operate properly through the NBG6817'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 NBG6817's NAT.

To change your NBG6817's ALGs and VPN pass-through settings, click **Expert Mode > WAN > NAT > Passthrough**. The screen appears as shown.

Figure 60 Expert Mode > WAN > NAT > Passthrough

Passthrough		Apply	Cancel
ALG Setup :			
FTP :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
H.323 :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
SIP :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
SNMP :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
RTSP :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
IRC :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
VPN Passthrough :			
PPTP :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
L2TP :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
IPSEC :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		

The following table describes the labels in this screen.

Table 24 Expert Mode > WAN > NAT > 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 NBG6817 through the network via SNMP.

Table 24 Expert Mode > WAN > NAT > Passthrough (continued)

LABEL	DESCRIPTION
RTSP	Select Enable to have the NBG6817 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 NBG6817 and the NBG6817 will drop the request. When PPTP is enabled, the NBG6817 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 NBG6817 and the NBG6817 will drop the request. When L2TP is enabled, the NBG6817 will forward the reply from the VPN server to the client that initiated the request, and the connection will establish successfully.
IPSEC	Select Enable to allow VPN clients to make outbound IPsec connections. It is required in order to connect to a IPsec VPN account. If IPSEC is disabled, then when a client sends a request to a VPN server, the server will reply to the NBG6817 and the NBG6817 will drop the request. When IPSEC is enabled, the NBG6817 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 NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

10.6 Dynamic DNS Screen

To change your NBG6817's DDNS, click **Expert Mode > WAN > Dynamic DNS**. The screen appears as shown.

Figure 61 Expert Mode > WAN > Dynamic DNS

Dynamic DNS [Apply] [Cancel]

Dynamic DNS Setup

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.

Register at <https://mycloud.zyxel.com/> and get a free accessible-from-anywhere network name as well as other ZyXEL services.

Dynamic DNS: Enable Disable

Service Provider: [DynDNS](#)

Host Name:

Username:

Password:

The following table describes the labels in this screen.

Table 25 Expert Mode > WAN > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Dynamic DNS	Select Enable to use dynamic DNS. Select Disable to turn this feature off.
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Enter a host names in the field provided. You can specify up to two host names in the field separated by a comma (",").
Username	Enter your user name.
Password	Enter the password assigned to you.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

Wireless LAN

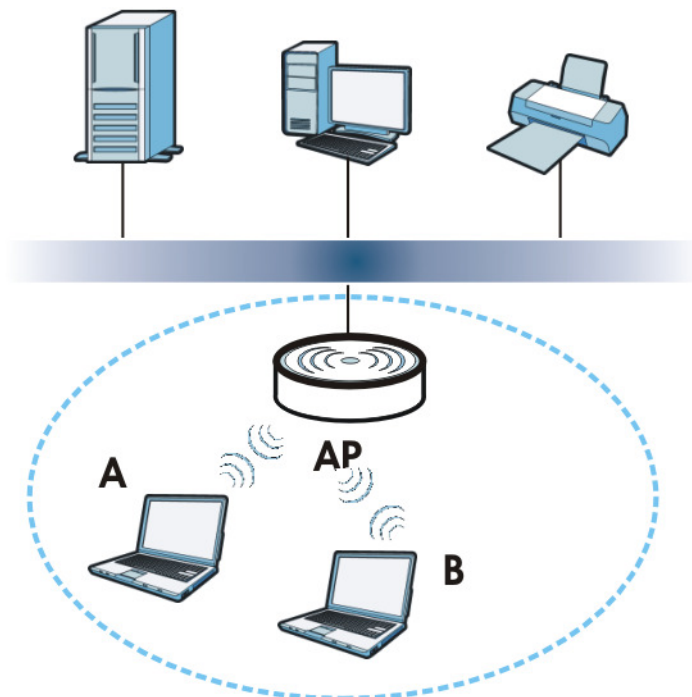
11.1 Overview

This chapter discusses how to configure the wireless network settings in your NBG6817. The NBG6817 is able to function both 2.4GHz and 5GHz network at the same time. You can have different wireless and wireless security settings for 2.4GHz and 5GHz wireless LANs. Click **Expert Mode > Wireless** to configure **wireless LAN 2.4G** or **wireless LAN 5G**.

See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 62 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your NBG6817 is the AP.

11.1.1 What You Can Do

- Use the **Wireless** screen to enable or disable the 2.4GHz or 5GHz wireless LAN, set up wireless security between the NBG6817 and the wireless clients, and make other basic configuration changes ([Section 11.2 on page 99](#)).
- Use the **Guest Wireless** screen to set up multiple wireless networks on your NBG6817 ([Section 11.4 on page 105](#)).
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the NBG6817 ([Section 11.5 on page 108](#)).
- Use the **Advanced** screen to allow intra-BSS networking and set the RTS/CTS Threshold ([Section 11.6 on page 109](#)).
- Use the **WPS** screen to quickly set up a wireless network with strong security, without having to configure security settings manually ([Section 11.7 on page 110](#)).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off ([Section 11.8 on page 112](#)).

11.1.2 What You Should Know

Every wireless network must follow these basic guidelines.

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

Wireless Security Overview

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

SSID

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

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

MAC Address Filter

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

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

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

User Authentication

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

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

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

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

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

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

Encryption

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

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

Table 26 Types of Encryption for Each Type of Authentication

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

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

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

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless clients. Device A only supports WPA, and device B supports WPA and WPA2. Therefore, you should set up **WPA** or **WPA-PSK** in the wireless network.

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

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

When you select **WPA2** or **WPA2-PSK** in your NBG6817, you can also select an option (**WPA/WPA-PSK Compatible**) to support WPA/WPA-PSK as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA/WPA-PSK Compatible** option in the NBG6817.

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

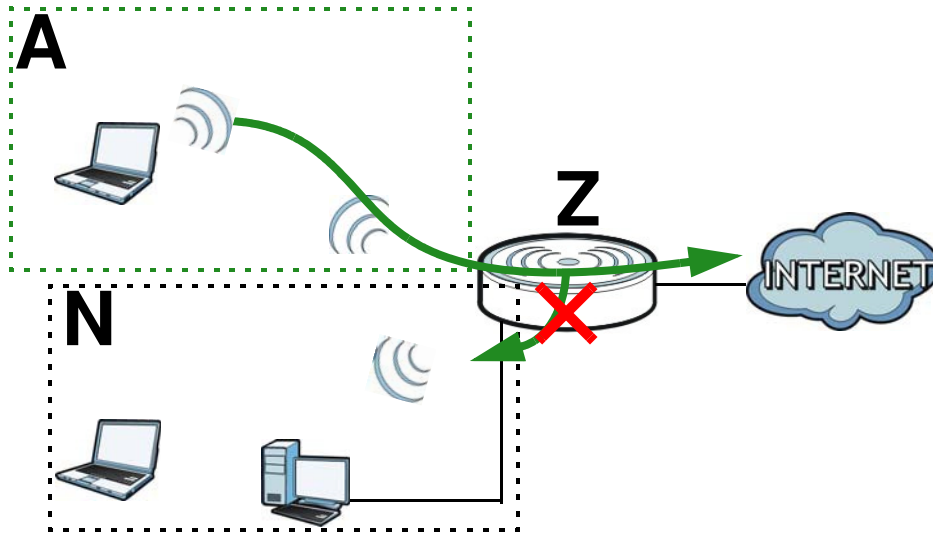
Guest WLAN

Guest WLAN allows you to set up a wireless network where users can access to Internet via the NBG6817 (**Z**), but not other networks connected to the **Z**. In the following figure, a guest user can access the Internet from the guest wireless network **A** via **Z** but not the home or company network **N**.

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

Note: Only Router mode supports guest WLAN.

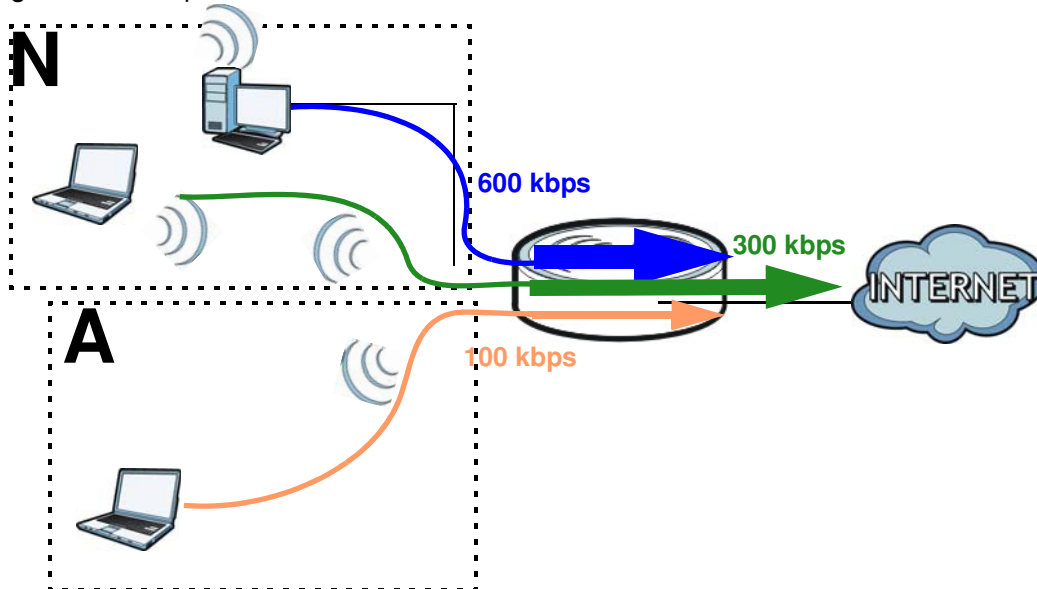
Figure 63 Guest Wireless LAN Network



Guest WLAN Bandwidth

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

Figure 64 Example: Bandwidth for Different Networks



WPS

WiFi Protected Setup (WPS) is an industry standard specification, defined by the WiFi Alliance. WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification

Number) in the devices. Then, they connect and set up a secure network by themselves. See how to set up a secure wireless network using WPS in the [Section 8.2 on page 49](#).

11.2 Wireless Screen

Use this screen to configure the SSID and wireless security of the NBG6817's default wireless LAN.

Note: If you are configuring the NBG6817 from a computer connected to the wireless LAN and you change the NBG6817's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the NBG6817's new settings.

Click **Expert Mode > Wireless**.

Figure 65 Expert Mode > Wireless

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

Table 27 Expert Mode > Wireless

LABEL	DESCRIPTION
Wireless Setup	
Band	Select the frequency band to set whether you want to apply the wireless and security settings to the default 2.4GHz or 5GHz wireless LAN.
Wireless LAN	Select Enable to activate the 2.4GHz and/or 5GHz wireless LAN. Select Disable to turn it off. You can enable or disable both 2.4GHz and 5GHz wireless LANs by using the WiFi button located on the rear panel of the NBG6817.

Table 27 Expert Mode > Wireless (continued)

LABEL	DESCRIPTION
Name (SSID)	The SSID (Service Set Identity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	<p>Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in.</p> <p>This option is only available if Auto Channel Selection is disabled.</p>
Operating Channel	This displays the channel the NBG6817 is currently using.
Channel Width	<p>Select the wireless channel width used by NBG6817.</p> <p>A standard 20MHz channel offers transfer speeds of up to 144Mbps (2.4GHz) or 217Mbps (5GHZ) whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps (2.4GHz) or 450Mbps (5GHZ). An IEEE 802.11ac-specific 80MHz channel offers speeds of up to 1.3 Gbps.</p> <p>The following are available only when you set Band to 2.4GHz.</p> <p>Because not all devices support 40 MHz channels, select Auto 20/ 40MHz to allow the NBG6817 to adjust the channel bandwidth automatically.</p> <p>40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.</p> <p>Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.</p> <p>The following are available only when you set Band to 5GHz.</p> <p>Because not all devices support 40 MHz and/or 80 MHz channels, select Auto to allow the NBG6817 to adjust the channel bandwidth automatically.</p> <p>80+ 80MHz bonds two non-adjacent 80MHz channels to increase throughput. The wireless clients may transmit/receive on both channels and use for the same purpose simultaneously.</p> <p>40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. A 80 MHz channel consists of two adjacent 40 MHz channels. The wireless clients must also support 40 MHz or 80 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal.</p> <p>Select 20MHz if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.</p>

Table 27 Expert Mode > Wireless (continued)

LABEL	DESCRIPTION
802.11 Mode	<p>If you set Band to 2.4GHz, you can select from the following:</p> <ul style="list-style-type: none"> • 802.11b: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the NBG6817. In this mode, all wireless devices can only transmit at the data rates supported by IEEE 802.11b. • 802.11g: allows IEEE 802.11g compliant WLAN devices to associate with the Device. IEEE 802.11b compliant WLAN devices can associate with the NBG6817 only when they use the short preamble type. • 802.11bg: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the NBG6817. The NBG6817 adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. • 802.11n: allows IEEE 802.11n compliant WLAN devices to associate with the NBG6817. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the NBG6817. • 802.11gn: allows either IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the NBG6817. The transmission rate of your NBG6817 might be reduced. • 802.11 bgn: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the NBG6817. The transmission rate of your NBG6817 might be reduced. <p>If you set Band to 5GHz, you can select from the following:</p> <ul style="list-style-type: none"> • 802.11a: allows only IEEE 802.11a compliant WLAN devices to associate with the NBG6817. • 802.11a/ an: allows both IEEE802.11n and IEEE802.11a compliant WLAN devices to associate with the NBG6817. The transmission rate of your NBG6817 might be reduced. • 802.11a/ an/ ac: allows IEEE802.11n, IEEE802.11a and IEEE 802.11ac compliant WLAN devices to associate with the NBG6817.
Security	
Security Mode	<p>Select WPA2-PSK to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See Section 11.3 on page 101 for detailed information on different security modes. Or you can select No Security to allow any client to associate this network without authentication.</p> <p>Note: If the WPS function is enabled (default), only No Security and WPA2-PSK are available in this field.</p>
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to reload the previous configuration for this screen.

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

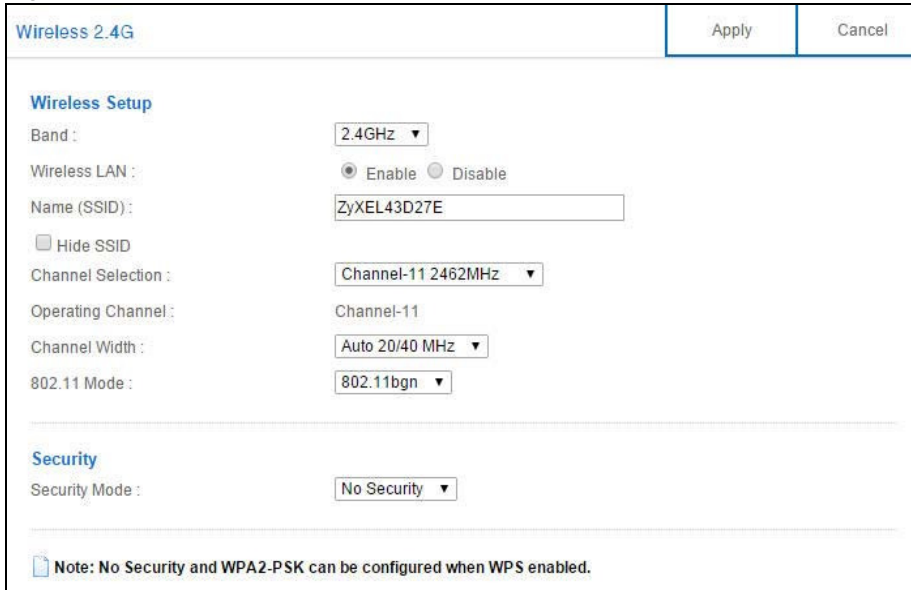
11.3 Wireless Security

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

11.3.1 No Security

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

Note: If you do not enable any wireless security on your NBG6817, your network is accessible to any wireless networking device that is within range.

Figure 66 Expert Mode > Wireless > Security Mode: No Security


The following table describes the labels in this screen.

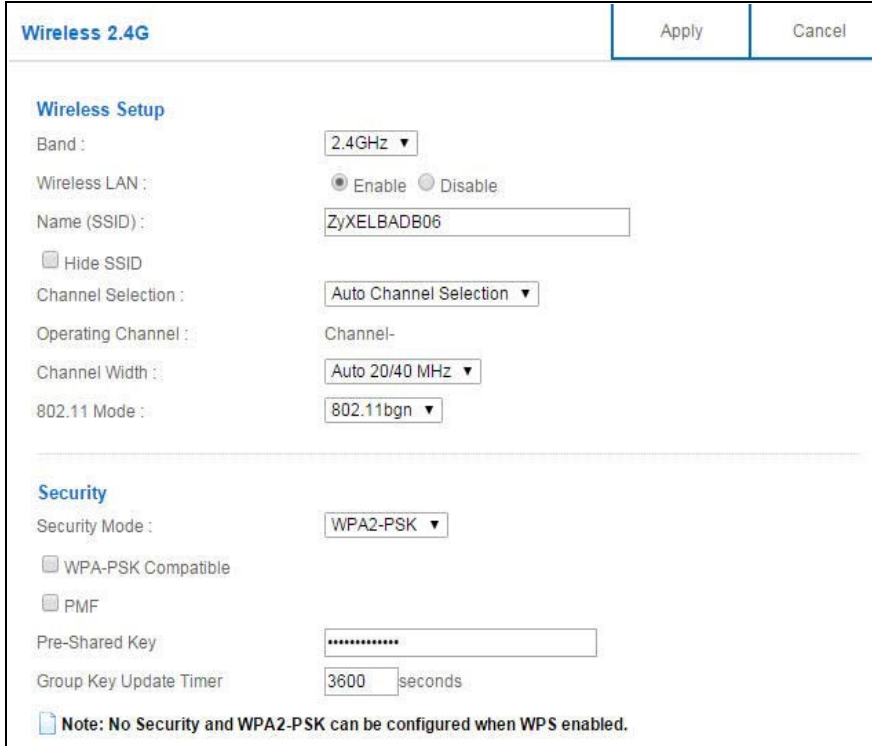
Table 28 Expert Mode > Wireless > Security Mode: No Security

LABEL	DESCRIPTION
Security Mode	Choose No Security from the drop-down list box.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to reload the previous configuration for this screen.

11.3.2 WPA-PSK/WPA2-PSK

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

Note: WPA-PSK is not available if you enable WPS before you configure WPA-PSK in the **Expert Mode > Wireless > Wireless** screen.

Figure 67 Expert Mode > Wireless > Security Mode: WPA-PSK/WPA2-PSK


The following table describes the labels in this screen.

Table 29 Expert Mode > Wireless > Security Mode: WPA-PSK/WPA2-PSK

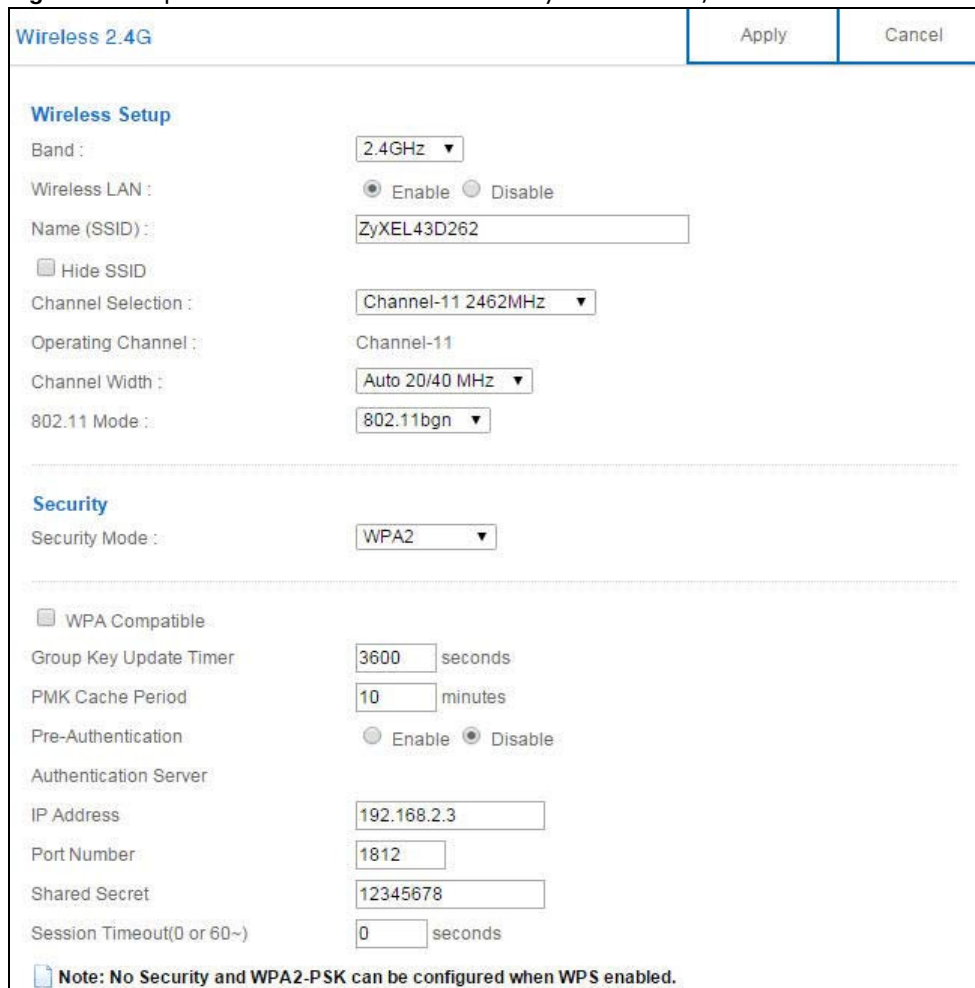
LABEL	DESCRIPTION
Security Mode	Select WPA2-PSK to enable data encryption.
WPA-PSK Compatible	This field appears when you choose WPA2-PSK as the Security Mode . Check this field to allow wireless devices using WPA-PSK security mode to connect to your NBG6817.
PMF	Protected Management Frames (PMF) is a protection mechanism of action management frames. Check this field to allow wireless devices using the PMF protection mechanism to connect to your NBG6817.
Pre-Shared Key	WPA-PSK/ WPA2-PSK uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive keyboard characters.
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP sends a new group key out to all clients. The default is 3600 seconds (60 minutes).
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to reload the previous configuration for this screen.

11.3.3 WPA/WPA2

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

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

Figure 68 Expert Mode > Wireless > Security Mode: WPA/WPA2



The following table describes the labels in this screen.

Table 30 Expert Mode > Wireless > Security Mode: WPA/WPA2

LABEL	DESCRIPTION
Security Mode	Select WPA2 to enable data encryption.
WPA Compatible	This check box is available only when you select WPA2-PSK or WPA2 in the Security Mode field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the NBG6817 even when the NBG6817 is using WPA2-PSK or WPA2.
Group Key Update Timer	The Group Key Update Timer is the rate at which the AP (if using WPA-PSK/ WPA2-PSK key management) or RADIUS server (if using WPA/ WPA2 key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the Group Key Update Timer is also supported in WPA-PSK/ WPA2-PSK mode.

Table 30 Expert Mode > Wireless > Security Mode: WPA/WPA2 (continued)

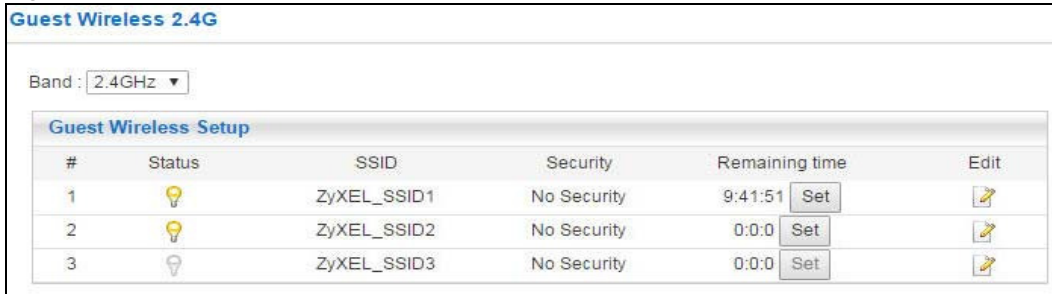
LABEL	DESCRIPTION
PMK Cache Period	This field is available only when you select WPA2 . Specify how often wireless clients have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 999999 minutes. Note: If wireless client authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Pre-Authentication	This field is available only when you select WPA2 . Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it. Select Enable to turn on preauthentication in WAP2. Otherwise, select Disable .
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 127 alphanumeric characters) as the key to be shared between the external authentication server and the NBG6817. The key must be the same on the external authentication server and your NBG6817. The key is not sent over the network.
Session Timeout	The NBG6817 automatically disconnects a wireless client from the wireless and wired networks after a period of inactivity. The wireless client needs to send the username and password again before it can use the wireless and wired networks again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again. Enter the time in seconds from 0 to 999999.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to reload the previous configuration for this screen.

11.4 Guest Wireless Screen

This screen allows you to enable and configure multiple guest wireless network settings on the NBG6817.

You can configure up to four SSIDs to enable multiple BSSs (Basic Service Sets) on the NBG6817. This allows you to use one access point to provide several BSSs simultaneously. You can then assign varying security types to different SSIDs. Wireless clients can use different SSIDs to associate with the same access point.

Click **Expert Mode > Wireless > Guest Wireless**. The following screen displays.

Figure 69 Expert Mode > Wireless > Guest Wireless

The following table describes the labels in this screen.

Table 31 Expert Mode > Wireless > Guest Wireless

LABEL	DESCRIPTION
Band	Use 2.4GHz or 5GHz to set up the NBG6817's guest Wi-Fi network.
#	This is the index number of each SSID profile.
Status	This shows whether the SSID profile is active (a yellow bulb) or not (a gray bulb).
SSID	An SSID profile is the set of parameters relating to one of the NBG6817's BSSs. The SSID (Service Set Identifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Remaining time	If the user is currently not permitted to access the Internet, you can click Set to allow access for a specified period of time. A screen then displays allowing you to set how long (in hours) the user is allowed to access the Internet. This field displays the amount of Internet access time that remains for each user before the NBG6817 blocks the user from accessing the Internet. 0:0:0 means there is no extra Internet access time.
Edit	Click the Edit icon to configure the SSID profile.

11.4.1 Guest Wireless Edit

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

Figure 70 Expert Mode > Wireless > Guest Wireless > Guest Wireless Setup: Edit


The following table describes the labels in this screen.

Table 32 Expert Mode > Wireless > Guest Wireless > Guest Wireless Setup: Edit

LABEL	DESCRIPTION
Active	Select this to activate the SSID profile.
Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Intra-BSS Traffic Blocking	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless clients can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless clients can still access the wired network but cannot communicate with each other.
WMM QoS	Check this to have the NBG6817 automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Enable Bandwidth Management for Guest WLAN	Select this to turn on bandwidth management for the Guest Wi-Fi network.
Maximum Bandwidth	Enter a number to specify maximum bandwidth the Guest Wi-Fi network can use.
Security Mode	Select WPA-PSK or WPA2-PSK to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See Section 11.3 on page 101 for detailed information on different security modes. Or you can select No Security to allow any client to associate this network without authentication. Note: If the WPS function is enabled (default), only No Security and WPA2-PSK are available in this field.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to reload the previous configuration for this screen.

11.5 MAC Filter Screen

The MAC filter screen allows you to configure the NBG6817 to give exclusive access to devices (**Allow**) or exclude devices from accessing the NBG6817 (**Deny**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your NBG6817's MAC filter settings, click **Expert Mode > Wireless > MAC Filter**. The screen appears as shown.

Figure 71 Expert Mode > Wireless > MAC Filter

The screenshot shows the 'MAC Filter 2.4G' configuration interface. At the top right are 'Apply' and 'Cancel' buttons. The configuration options are:

- Band: 2.4GHz (dropdown menu)
- SSID Select: ZyXEL3333C2 (text field)
- MAC Address Filter: Enable Disable
- Filter Action: Allow Deny

 Below the configuration options is a 'MAC Filter Summary (Max Limit : 64)' table. The table has three columns: '#', 'MAC Address', and 'Add/Delete'. The first row shows '# 1' and 'MAC Address AC:AC:AB:CC:BA:AC'. The 'Add/Delete' column contains a '+' icon for adding and a '-' icon for deleting. A 'User Defined' dropdown is visible above the table.

The following table describes the labels in this menu.

Table 33 Expert Mode > Wireless > MAC Filter

LABEL	DESCRIPTION
Band	Select the frequency band to set whether you want to apply the wireless and security settings to the default 2.4GHz or 5GHz wireless LAN.
SSID Select	This shows the SSID for which you are configuring MAC filtering.
MAC Address Filter	Select to turn on (Enable) or off (Disable) MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the MAC Filter Summary table. Select Allow to permit access to the NBG6817, MAC addresses not listed will be denied access to the NBG6817. Select Deny to block access to the NBG6817, MAC addresses not listed will be allowed to access the NBG6817.
MAC Filter Summary (Max Limit : 64)	
#	This is the index number of the MAC address. Select Auto Detection to automatically detect the MAC address of the wireless station that are allowed or denied access to the NBG6817. Otherwise, select User define to enter the MAC address of the wireless station in the MAC Address field that are allowed or denied access to the NBG6817.
MAC Address	This field displays the MAC address of the wireless station. If you select User define in the # field, enter the MAC address(es) manually.
Add/Delete	Click to add the rule in the MAC filter summary table. Click to remove a rule.

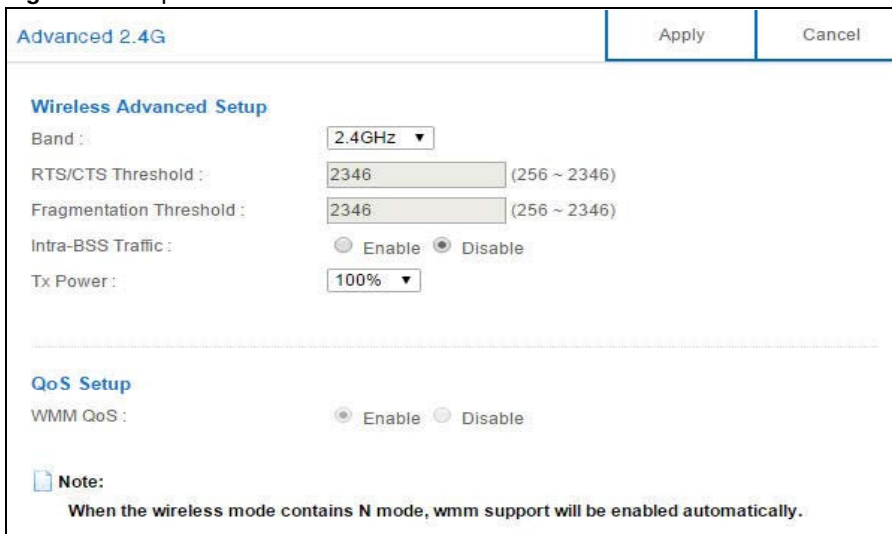
Table 33 Expert Mode > Wireless > MAC Filter

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to reload the previous configuration for this screen.

11.6 Advanced Screen

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

Click **Expert Mode > Wireless > Advanced**. The screen appears as shown.

Figure 72 Expert Mode > Wireless > Advanced


The following table describes the labels in this screen.

Table 34 Expert Mode > Wireless > Advanced

LABEL	DESCRIPTION
Wireless Advanced Setup	
Band	Select the frequency band to set whether you want to apply the wireless and security settings to the default 2.4GHz or 5GHz wireless LAN.
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. This field is not configurable and the NBG6817 automatically changes to use the maximum value if you select 802.11n , 802.11an , 802.11gn or 802.11bgn in the Expert > Wireless screen.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. This field is not configurable and the NBG6817 automatically changes to use the maximum value if you select 802.11n , 802.11an , 802.11gn or 802.11bgn in the Expert > Wireless screen.

Table 34 Expert Mode > Wireless > Advanced (continued)

LABEL	DESCRIPTION
Intra-BSS Traffic	<p>A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).</p> <p>Intra-BSS traffic is traffic between wireless clients in the BSS. When you Enable Intra-BSS, wireless clients can access the wired network and communicate with each other. When you Disable Intra-BSS, wireless clients can still access the wired network but cannot communicate with each other.</p>
Tx Power	<p>Set the output power of the NBG6817 in this field. If there is a high density of APs in an area, decrease the output power of the NBG6817 to reduce interference with other APs. Select one of the following 100% , 90% , 75% , 50% , 25% or 10% .</p>
QoS Setup	
WMM QoS	<p>Select Enable to have the NBG6817 automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.</p> <p>This field is not configurable and the NBG6817 automatically enables WMM QoS if you select 802.11n , 802.11an , 802.11gn or 802.11bgn in the Expert > Wireless screen.</p>
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to reload the previous configuration for this screen.

11.7 WPS Screen

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

Note: With WPS, wireless clients can only connect to the wireless network using the first SSID on the NBG6817.

Figure 73 Expert Mode > Wireless > WPS

WPS 2.4G
Apply
Cancel

WPS Setup

Band : 2.4GHz ▾

WPS : Enable Disable

PIN Code : Enable Disable

PIN Number : Generate

Click the Push Button to add WPS stations to wireless network. Push Button

Or input station's PIN number : Start

Note:

1. The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.
2. You may find the PIN number in the station's utility.

WPS Status

Status : Configured Release Configuration

802.11 Mode : 802.11bgn

SSID : ZyXEL43D27E

Security : WPA2-PSK

Note:

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

The following table describes the labels in this screen.

Table 35 Expert Mode > Wireless > WPS

LABEL	DESCRIPTION
WPS Setup	
Band	Select the frequency band to set whether you want to apply the wireless and security settings to the default 2.4GHz or 5GHz wireless LAN.
WPS	Select Enable to turn on the WPS feature. Otherwise, select Disable .
PIN Code	Select Enable and click Apply to allow the PIN Configuration method. If you select Disable , you cannot create a new PIN number.
PIN Number	This is the WPS PIN (Personal Identification Number) of the NBG6817. Enter this PIN in the configuration utility of the device you want to connect to the NBG6817 using WPS. The PIN is not necessary when you use WPS push-button method. Click Generate to generate a new PIN number.
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.

Table 35 Expert Mode > Wireless > WPS (continued)

LABEL	DESCRIPTION
Or input station's PIN number	Use this button when you use the PIN Configuration method to configure wireless station's wireless settings. Type the same PIN number generated in the wireless station's utility. Then click Start to associate to each other and perform the wireless security information synchronization.
WPS Status	
Status	This displays Configured when the NBG6817 has connected to a wireless network using WPS or when WPS Enable is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays Unconfigured if WPS is disabled and there are no wireless or wireless security changes on the NBG6817 or you click Release Configuration to remove the configured wireless and wireless security settings.
Release Configuration	This button is only available when the WPS status displays Configured . Click this button to remove all configured wireless and wireless security settings for WPS connections on the NBG6817.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the NBG6817.
SSID	This is the name of the wireless network (the NBG6817's first SSID).
Security	This is the type of wireless security employed by the network.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to reload the previous configuration for this screen.

11.8 Scheduling Screen

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

Figure 74 Expert Mode > Wireless > Scheduling

Scheduling 2.4G Apply Cancel

Band:

Wireless LAN Scheduling: Enable Disable

Internet Access Schedule

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Sun	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block
Mon	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block
Tue	Block	Block	Block	Block	Allow	Allow	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	
Wed	Block	Block	Block	Block	Block	Block	Block	Block	Block	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow
Thu	Block	Block	Block	Block	Block	Block	Block	Block	Block	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow	Allow
Fri	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block
Sat	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block	Block

Allow Block

The following table describes the labels in this screen.

Table 36 Expert Mode > Wireless > Scheduling

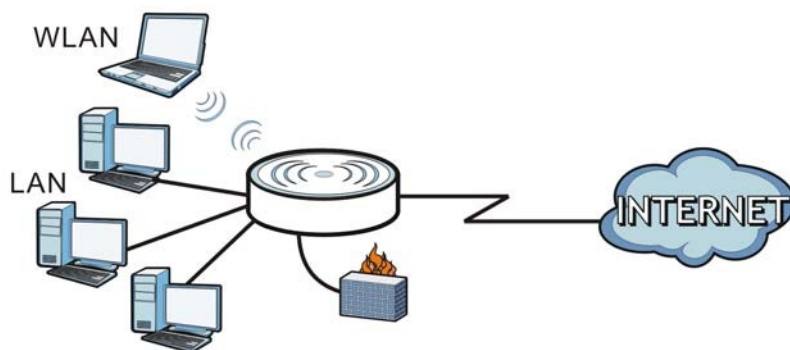
LABEL	DESCRIPTION
Band	Select the frequency band to set whether you want to apply the wireless and security settings to the default 2.4GHz or 5GHz wireless LAN.
Wireless LAN Scheduling	Select Enable to activate the wireless LAN scheduling feature. Select Disable to turn it off.
Internet Access Schedule	The y-axis shows the time period in days. The x-axis shows the time period in hours. Click Select All or click gray blocks to specify days and times to turn the Wireless LAN on or off. If you click Select All you can not select any specific days and times. Click Clean All to remove all the wireless LAN scheduling.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to reload the previous configuration for this screen.

12.1 Overview

This chapter describes how to configure LAN settings.

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

Figure 75 LAN Example



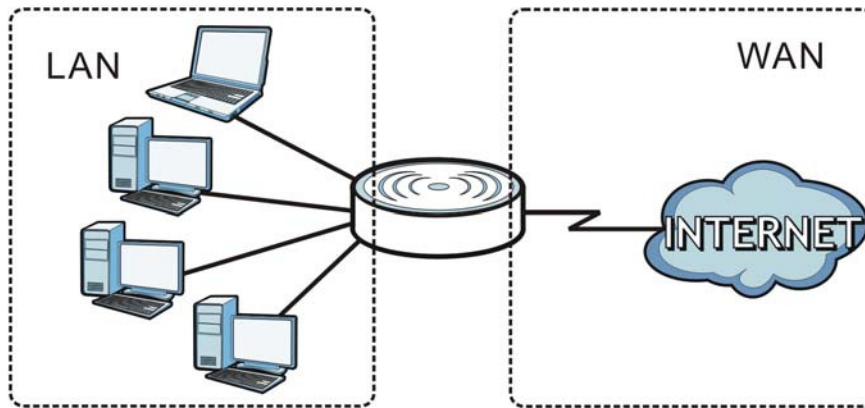
The LAN screens can help you configure a manage IP address, and partition your physical network into logical networks.

12.2 What You Can Do

- Use the **LAN IP** screen to configure the IPv4 and IPv6 addresses for your NBG6817 on the LAN ([Section 12.4 on page 115](#)).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses ([Section 12.5 on page 116](#)).
- Use the **IPv6 LAN** screen to configure the IPv6 address for your NBG6817 on the LAN ([Section 12.6 on page 117](#)).

12.3 What You Need To Know

The actual physical connection determines whether the NBG6817 ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 76 LAN and WAN IP Addresses

The LAN parameters of the NBG6817 are preset in the factory with the following values:

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

These parameters should work for the majority of installations.

12.4 LAN IP Screen

Use this screen to change the IP address for your NBG6817. Click **Expert Mode > LAN > LAN IP**.

Figure 77 Expert Mode > LAN > LAN IP

LAN IP		Apply	Cancel
IP Address :	<input type="text" value="192.168.1.1"/>		
IP Subnet Mask :	<input type="text" value="255.255.255.0"/>		
<hr/>			
DHCP Server :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
IP Pool Starting Address :	<input type="text" value="192.168.1.33"/>		
Pool Size :	<input type="text" value="32"/>		

The following table describes the labels in this screen.

Table 37 Expert Mode > LAN > LAN IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your NBG6817 in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG6817 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 NBG6817.

Table 37 Expert Mode > LAN > LAN IP (continued)

LABEL	DESCRIPTION
DHCP Server	Select Enable to activate DHCP for LAN. DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Enable the DHCP server unless your ISP instructs you to do otherwise. Select Disable to stop the NBG6817 acting as a DHCP server. When configured as a server, the NBG6817 provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool for LAN.
Pool Size	This field specifies the size, or count of the IP address pool for LAN.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

12.5 Static DHCP Screen

This screen allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses.

To change your NBG6817's static DHCP settings, click **Expert Mode > LAN > Static DHCP**.

Figure 78 Expert Mode > LAN > Static DHCP

#	MAC Address	IP Address	Add/Delete
1	c0:3f:d5:ba:9e:b7	192.168.1.88	+

The following table describes the labels on this screen.

Table 38 Expert Mode > LAN > Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the static IP table entry (row). Select Auto Detection to automatically detect the MAC address of a computer on your LAN. Otherwise, select User define 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 define in the # field, enter the MAC address(es) manually.
IP Address	This field displays the LAN IP address of a computer on your LAN. If you select User define in the # field, enter the IP address(es) manually.
Add/Delete	Click + to add the rule in the MAC filter summary table. Click - to remove a rule.

Table 38 Expert Mode > LAN > Static DHCP (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes with the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

12.6 IPv6 LAN Screen

Use this screen to configure the IP address for your NBG6817 on the LAN. Click **Expert Mode > LAN > IPv6 LAN**.

Figure 79 Expert Mode > LAN > IPv6 LAN

The following table describes the labels in this screen.

Table 39 Expert Mode > LAN > IPv6 LAN

LABEL	DESCRIPTION
LAN IPv6 Address Assignment	
Enable_DHCPv6-PD	Select this option to use DHCPv6 prefix delegation. The NBG6817 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 IP addresses that this address object represents.
IPv6 Address range (End)	Enter the end of the range of IP address that this address object represents.

Table 39 Expert Mode > LAN > IPv6 LAN (continued)

LABEL	DESCRIPTION
IPv6 Lifetime	Enter the IPv6 lifetime in the LAN.
Static IP Address	
Select this option to manually enter an IPv6 address if you want to use a static IP address.	
LAN IPv6 Address	Enter the LAN IPv6 address you want to assign to your NBG6817 in hexadecimal notation.
LAN IPv6 Prefix Length (48~64)	Enter the 48 to 64 address prefix length to specify in an IPv6 address compose the network address.
Prefix Preferred Lifetime	Enter the preferred lifetime for the prefix.
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 NBG6817 interfaces in the LAN.	
ULA	
Select this option to identify a unique local address of the NBG6817 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 NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

Applications

13.1 Overview

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

13.1.1 What You Can Do

- Use the **Parental Control** screens to enable parental control, configure the parental control rules and schedules, and send e-mail notifications. ([Section 13.2 on page 121](#)).
- Use the **Bandwidth Management** screen to configure bandwidth management and the device priority ([Section 13.3 on page 127](#)).
- Use the **USB Media Sharing** screen to use the NBG6817 as a media server and allow DLNA-compliant devices to play media files stored in the attached USB device ([Section 13.4 on page 130](#)).
- Use the **UPnP** screen to enable UPnP on your NBG6817 ([Section 13.5 on page 132](#)).
- Use the **File Sharing** screen to allow file sharing via the NBG6817 using Windows Explorer, the workgroup name or FTP ([Section 13.6 on page 133](#)).
- Use the **One Connect** screen to enable or disable Wi-Fi auto-configuration ([Section 13.7 on page 140](#)).

13.1.2 What You Need To Know

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

Keyword Blocking URL Checking

The NBG6817 checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

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

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

Since the NBG6817 checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the NBG6817 would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path ([news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php)) but it would not find "tw/news".

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 NBG6817 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 NBG6817 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 NBG6817 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 NBG6817. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

Samba

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

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

File Transfer Protocol

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

Universal Plug-and-Play (UPnP)

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

13.1.3 Before You Begin

Make sure the NBG6817 is connected to your network and turned on.

- 1 Connect the USB device to one of the NBG6817's USB ports.
- 2 The NBG6817 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 NBG6817, see the troubleshooting for suggestions.

13.2 Parental Control

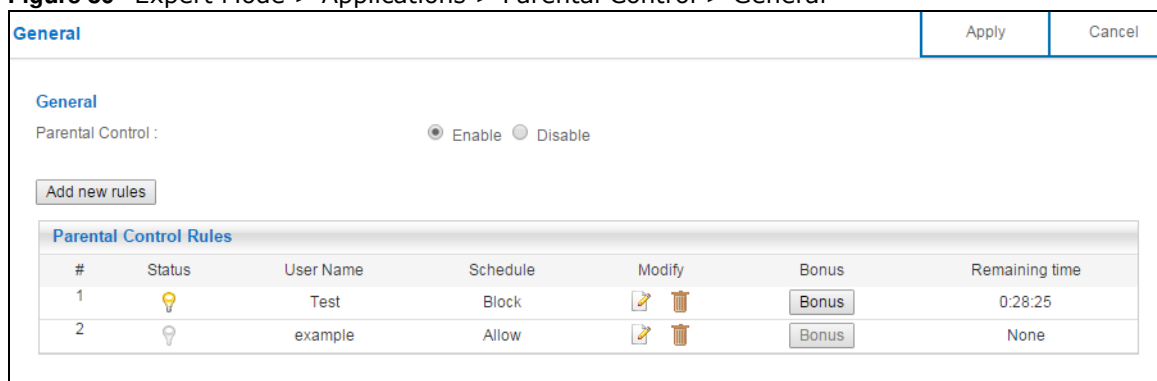
Parental Control allows you to block specific URLs. You can also define time periods and days during which the NBG6817 performs parental control on a specific user.

13.2.1 General Screen

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

In **Expert** mode, click **Applications > Parental Control > General** to open the following screen.

Figure 80 Expert Mode > Applications > Parental Control > General



#	Status	User Name	Schedule	Modify	Bonus	Remaining time
1	💡	Test	Block	✏️ 🗑️	Bonus	0:28:25
2	💡	example	Allow	✏️ 🗑️	Bonus	None

The following table describes the fields in this screen.

Table 40 Expert Mode > Applications > Parental Control > General

LABEL	DESCRIPTION
General	
Parental Control	Select Enable to activate parental control. Otherwise, select Disable to turn it off.
Add new rules	Click this if you want to configure a new parental control rule.
Parental Control Rules	
#	This shows the index number of the rule.
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
User Name	This shows the name of the user to which this rule applies.
Schedule	This shows whether the user is able to access the Internet through the NBG6817 (Allow) or not (Block) at the moment.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Delete icon to delete an existing rule.
Bonus	If the user is currently not permitted to access the Internet, you can click the Bonus to allow access for a specified period of time. A screen then displays allowing you to set how long (in minutes) the user is allowed to access the Internet. This button is grayed out if the user is now able to access the Internet.
Remaining Time	This field displays the amount of Internet access time that remains for each user before the NBG6817 blocks the user from accessing the Internet. None means there is no extra Internet access time.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

13.2.1.1 Add/Edit a Parental Control Rule

Click **Add new rules** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain web sites.

Figure 81 Expert Mode > Applications > Parental Control > General: Add/Edit new rules

The following table describes the fields in this screen.

Table 41 Expert Mode > Applications > Parental Control > General: Add/Edit new rules

LABEL	DESCRIPTION
General	
Active	Select the checkbox to activate this parental control rule.
User Name	Enter a descriptive name for the user.
Device List	The left text box lists the system name of the LAN user device which is connected to the NBG6817 and assigned an IP address. From the left text box, select the LAN user device to which you want to apply this rule and click Add to move it to the right text box. To remove a user device, select it from the right text box and click Delete .
Internet Access Schedule	The y-axis shows the days that you want the NBG6817 to perform parental control and allow the user to access the Internet. The x-axis shows the time period during which the LAN user is allowed access. A blue block signifies that this rule is active. A gray block signifies that this rule is not active.
Clean All	Click Clean All to remove blocks you selected.
Select All	Click Select All to choose all blocks.

Table 41 Expert Mode > Applications > Parental Control > General: Add/Edit new rules (continued)

LABEL	DESCRIPTION
Network Service	
Network Service Setting	If you select Block , the NBG6817 prohibits the users from using the services listed below. If you select Allow , the NBG6817 blocks all services except ones listed below.
Add new service	Click this to show a screen in which you can add a new service rule. You can configure the Service Name , Protocol , and Port of the new rule.
#	This shows the index number of the rule. Select the checkbox next to the rule to activate it.
Service Name	This shows the name of the service.
Protocol:Port	This shows the protocol and the port of the service.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Delete icon to delete an existing rule.
Block Site/URL Keyword	
Keyword	Enter a keyword and click Add to add it to the keyword list. This has the NBG6817 block access to the website URLs that contain the keyword.
Keyword List	Select a keyword and click Delete to remove it. Click Clear All to remove all keywords from the keyword list.
Apply	Click Apply to save your settings back to the NBG6817.
Back	Click Back to return to the previous screen.

13.2.1.2 Add/Edit a Service

Click **Add new service** in the **Parental Control > Add new rules** screen to add a new entry or click the **Edit** icon next to an existing entry to edit it. Use this screen to configure a service rule.

Figure 82 Expert Mode > Applications > Parental Control > General: Add/Edit new rules: Add new service

The screenshot shows a web interface titled 'parental control edit'. At the top right, there are two buttons: 'Apply' and 'Back'. Below the title bar, there are three main input fields:

- Service Name :** A dropdown menu currently showing 'UserDefined'.
- Protocol :** A dropdown menu currently showing 'TCP'.
- Port :** A text input field.

Below the Port field, there is a note: '(Example:4091,5091-6892)'.

The following table describes the fields in this screen.

Table 42 Expert Mode > Applications > Parental Control > General: Add/Edit new rules: Add new service

LABEL	DESCRIPTION
Service Name	Select the name of the service. Otherwise, select UserDefined and manually specify the protocol and the port of the service. If you have chosen a pre-defined service in the Service Name field, this field will not be configurable.
Protocol	Select the transport layer protocol used for the service. Choices are TCP , UDP , or TCP/UDP .

Table 42 Expert Mode > Applications > Parental Control > General: Add/Edit new rules: Add new service (continued)

LABEL	DESCRIPTION
Port	Enter the port of the service. If you have chosen a pre-defined service in the Service Name field, this field will not be configurable.
Apply	Click Apply to save your settings with the NBG6817.
Back	Click Back to return to the previous screen.

13.2.2 Notification Screen

Use this screen to have the NBG6817 send e-mail notifications when the user(s) is connected to the NBG6817 for Internet access during the specified time periods.

In **Expert** mode, click **Applications > Parental Control > Notification** to open the following screen.

Figure 83 Expert Mode > Applications > Parental Control > Notification

The following table describes the fields in this screen.

Table 43 Expert Mode > Applications > Parental Control > Notification

LABEL	DESCRIPTION
General	
E-mail Notification	Select Enable to activate e-mail notifications.
Add new rules	Click this if you want to configure a new parental monitor rule.
Notification Rules	
#	This shows the index number of the rule.

Table 43 Expert Mode > Applications > Parental Control > Notification (continued)

LABEL	DESCRIPTION
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
User Name	This shows the name of the user to which this rule applies.
Notification	This shows the e-mail address to which the notification is sent.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Delete icon to delete an existing rule.
Email Notification Configuration	
Mail Server	Select the mail server. Otherwise, select UserDefined and manually specify the mail server address and the port of the mail server.
Mail Server Address	Type the name or IP address of the outgoing SMTP server.
Mail Server Port	Enter the same port number here as is on the mail server for mail traffic.
Authentication Username	Type the user name to provide to the SMTP server for authentication when the notification is e-mailed.
Authentication Password	Type the password to provide to the SMTP server for authentication when the notification is e-mailed.
Mail From	Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies.
E-Mail	Type the e-mail address (or addresses) to which the outgoing e-mail is delivered.
Apply	Click Apply to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

13.2.2.1 Add/Edit a Notification Rule

Click **Add new rules** in the **Notification** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to set a schedule and have the NBG6817 send a notification when the specified user connects to the NBG6817 at the scheduled time.

Figure 84 Expert Mode > Applications > Notification: Add/Edit new rules

Notification Edit

Apply
Back

Notification

Active

Home Network User: TEST

Schedule

Day: Monday Tuesday Wednesday Thursday
 Friday Saturday Sunday

Time (Begin ~ End): 00 (hour) 00 (min) ~ 24 (hour) 00 (min)

Note:

1. Please add a user profile rule at Parental Control > General first.
2. You need to configure the e-mail settings before the system can send notifications.

The following table describes the fields in this screen.

Table 44 Expert Mode > Applications > Notification: Add/Edit new rules

LABEL	DESCRIPTION
Notification	
Active	Select the checkbox to activate this notification rule.
Home Network User	Select the user that you want to apply this rule to from the drop-down list box. Note: You should have configured a parental control rule already for the specified user.
Schedule	
Day	Select check boxes for the days that you want the NBG6817 to perform notification.
Time (Begin ~ End)	Define the time period during that you want the NBG6817 to perform notification.
Apply	Click Apply to save your settings back to the NBG6817.
Back	Click Back to return to the previous screen.

13.3 Bandwidth Management

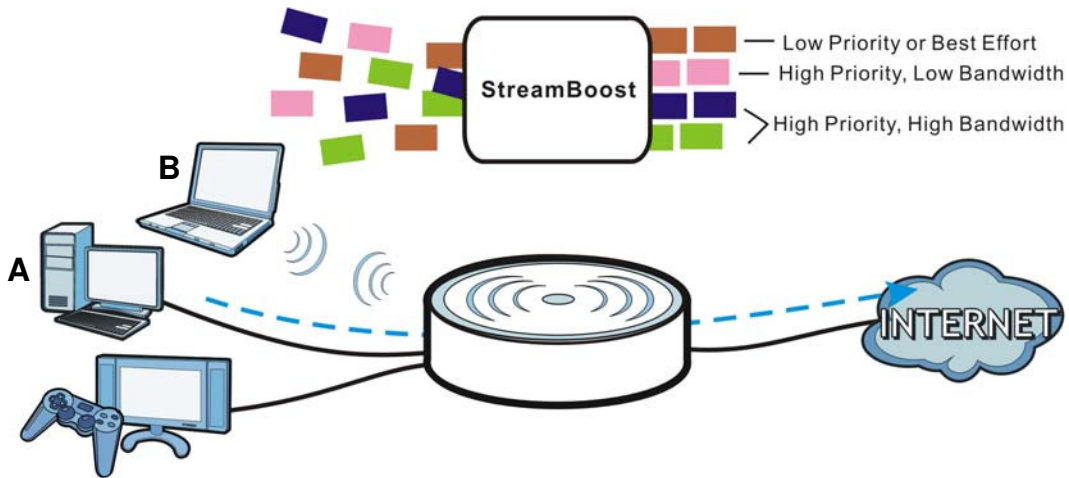
The NBG6817 supports the new StreamBoost technology, introduced by Qualcomm, to redistribute traffic over the NBG6817 for the best possible performance in a home network.

Streamboost is smart Quality of Service (QoS). Streamboost detects traffic flow and applies traffic shaping policies automatically. It gives each device and each application priority and provides the exact amount of bandwidth they need at a given time. This helps free up bandwidth for other applications or connected devices. If there is not enough bandwidth for optimal performance, Streamboost makes sure the application or device has the minimum acceptable bandwidth which is determined according to StreamBoost's cloud-based database.

Real-time application traffic (such as on-line games or communications) and video/audio streaming are given the highest priority. Downloads or torrent files are classified as best effort and placed lower than general network traffic (general browsing).

In the figure below, the StreamBoost-enabled NBG6817 differentiates incoming traffic flow going from the LAN device (**A**) or wireless device (**B**) to the Internet. It shapes traffic and gives priority and allocates bandwidth according to traffic types.

Figure 85 StreamBoost Management Example



13.3.1 Bandwidth Screen

Use this screen to configure the maximum allowable bandwidth on the NBG6817 and allow the NBG6817 to get StreamBoost database updates automatically.

In **Expert** mode, click **Applications > Bandwidth Management > Bandwidth** to open the following screen.

Figure 86 Expert Mode > Applications > Bandwidth Management > Bandwidth

Bandwidth		Apply	Cancel
Streamboost			
<input checked="" type="checkbox"/> Enable StreamBoost			
Up Limit (Mbps)	<input type="text" value="1000"/>		
Down Limit (Mbps)	<input type="text" value="1000"/>		
Automatic Update Agreement			
<p>Check below to enable your router to receive automatic StreamBoost updates during your initial 3-year manufacturer service term (extendable through the manufacturer). StreamBoost updates may help improve its Internet traffic management capabilities. In exchange, your StreamBoost enabled router will send Qualcomm Atheros Inc. anonymous information from your router. If you decline, you can find updates through software or firmware postings from your router's manufacturer.</p> <p>Your StreamBoost enabled router will provide Qualcomm Atheros Inc. with anonymous data transmitted through the router. Such anonymous data may include small amountsof information when you launch a streaming service (such as video, audio, or gaming) for</p>			
<input type="checkbox"/> Enable Automatic Update			

The following table describes the labels in this screen.

Table 45 Expert Mode > Applications > Bandwidth Management > Bandwidth

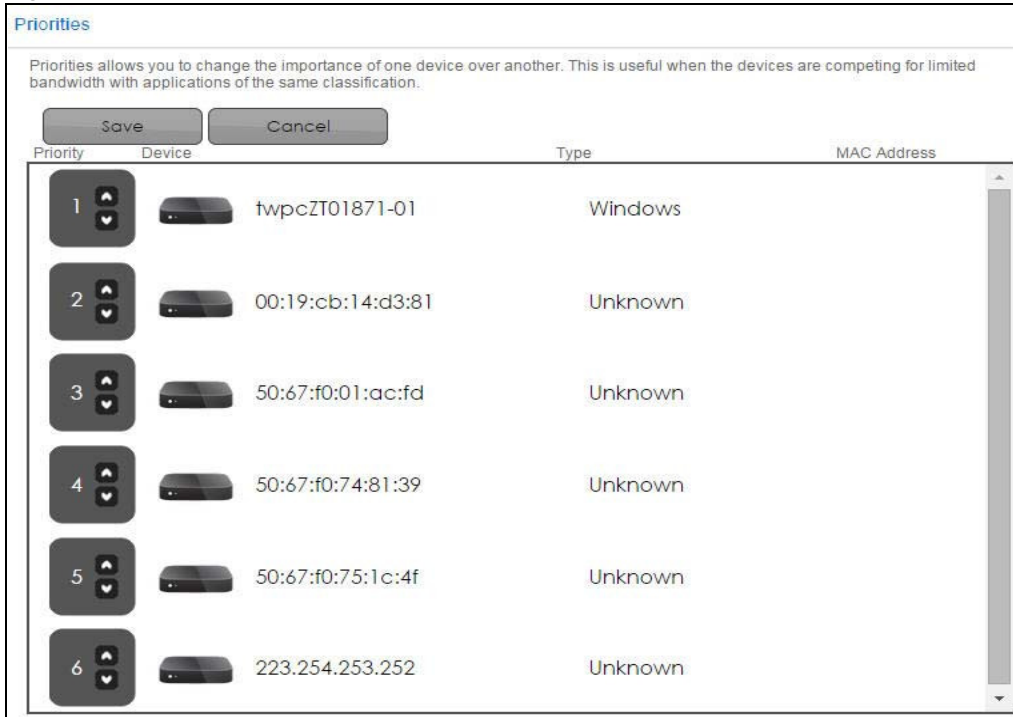
LABEL	DESCRIPTION
Enable StreamBoost	Select this option to turn on Streamboost management on the NBG6817.
Up Limit (Mbps)	<p>If you select Automatic Bandwidth Detection, this automatically displays the total amount of bandwidth that you can dedicate to uplink (or outgoing) traffic.</p> <p>If you don't select Automatic Bandwidth Detection, set the total amount of bandwidth that you want to dedicate to uplink (or outgoing) traffic.</p> <p>This is traffic from LAN/WLAN to WAN.</p>
Down Limit (Mbps)	<p>If you select Automatic Bandwidth Detection, this automatically displays the total amount of bandwidth that you can dedicate to downlink (or incoming) traffic.</p> <p>If you don't select Automatic Bandwidth Detection, set the total amount of bandwidth that you want to dedicate to downlink (or incoming) traffic.</p> <p>This is traffic from WAN to LAN/WLAN.</p>
Enable Automatic Update	<p>StreamBoost provides a cloud-based service to learn any new type of traffic which is not in its database and update the table in the NBG6817 for traffic detection and policies.</p> <p>Select this option to have the NBG6817 automatically receives the StreamBoost table updates. When there is a new type of traffic which is not in the NBG6817's table, the NBG6817 will capture some packets and send them to the StreamBoost cloud for analysis and database update.</p>
Apply	Click Apply to save your customized settings.
Cancel	Click Cancel to begin configuring this screen afresh.

13.3.2 Priorities Screen

The StreamBoost engine on the NBG6817 can identify the types of connected devices (such as PC, smart phone, tablet, TV or game console) in your network. When there is not enough bandwidth to support traffic of the same priority, the NBG6817 refers to the connected device priority. Traffic from the device with the lowest priority is classified as best-effort traffic.

Use this screen to prioritize the connected devices by clicking a device's arrow button to change its position in the list. Click **Save** to apply your settings. Otherwise, click **Cancel** to return the screen to its last-saved settings.

In **Expert** mode, click **Applications > Bandwidth Management > Priorities** to open the following screen.

Figure 87 Expert Mode > Applications > Bandwidth Management > Priorities

13.4 USB Media Sharing Screen

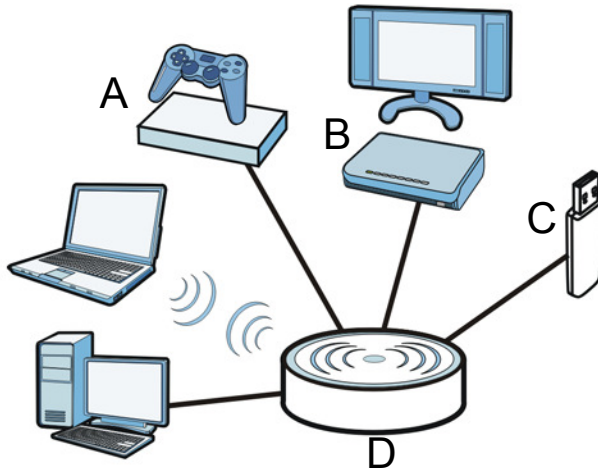
You can set up your NBG6817 to act as a media server to provide media (like video) to DLNA-compliant players, such as Windows Media Player, ZyXEL DMAs (Digital Media Adapters), Xboxes or PS3s. The media server and clients must have IP addresses in the same subnet.

The NBG6817 media server enables you to:

- Publish all folders for everyone to play media files in the USB storage device connected to the NBG6817.
- Use hardware-based media clients like the DMA-2500 to play the files.

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

The following figure is an overview of the NBG6817's media server feature. DLNA devices **A** and **B** can access and play files on a USB device (**C**) which is connected to the NBG6817 (**D**).

Figure 88 Media Server Overview

Use this screen to have the NBG6817 act as a DLNA-compliant media server that lets DLNA-compliant media clients on your network play video, music, and photos from the NBG6817 (without having to copy them to another computer).

In **Expert** mode, click **Applications** > **USB Media Sharing** to open the following screen.

Figure 89 Expert Mode > Applications > USB Media Sharing

USB Media Sharing		Apply	Cancel
DLNA Setup			
Enable DLNA	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Enable Shared Media Types			
USB1 :	<input checked="" type="checkbox"/> Photo	<input checked="" type="checkbox"/> Music	<input checked="" type="checkbox"/> Video
USB2 :	<input checked="" type="checkbox"/> Photo	<input checked="" type="checkbox"/> Music	<input checked="" type="checkbox"/> Video
Rescan Media Contents			
<input type="button" value="Rescan"/>			
Note: Maximum of 60,000 media files can be loaded.			

The following table describes the labels in this screen.

Table 46 Expert Mode > Applications > USB Media Sharing

LABEL	DESCRIPTION
DLNA Setup	
Enable DLNA	Select this to have the NBG6817 function as a DLNA-compliant media server.
Enable Shared Media Types	
USB1/USB2	Select the media type that you want to share on the USB device connected to the NBG6817's USB port.
Rescan Media Contents	
Rescan	Click this button to have the NBG6817 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.

Table 46 Expert Mode > Applications > USB Media Sharing (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

13.5 UPnP Screen

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

Use this screen to enable UPnP on your NBG6817.

In **Expert** mode, click **Applications > UPnP** to open the following screen.

Figure 90 Expert Mode > Applications > UPnP

#	Protocol	In Port	Out Port	IP Address
1	tcp	548	548	192.168.77.55
2	tcp	445	445	192.168.77.55
3	tcp	21	21	192.168.77.55
4	tcp	8000	80	192.168.77.55
5	tcp	8082	8082	192.168.77.55
6	udp	50657	50657	192.168.77.97
7	udp	59530	59530	192.168.77.46
8	udp	34851	34851	172.20.10.3
9	udp	18166	18166	172.20.10.3
10	tcp	34851	34851	172.20.10.3

The following table describes the fields in this screen.

Table 47 Expert Mode > Applications > UPnP

LABEL	DESCRIPTION
UPnP	Select Enable to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the NBG6817's IP address (although you must still enter the password to access the web configurator).
Display	Select the page number from the drop-down list box to display the UPnP port mapping rules.
UPnP Portmap Table	
#	This is the number of an individual UPnP entry.
Protocol	This is the transport layer protocol used for the service.
In Port	In Port 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.

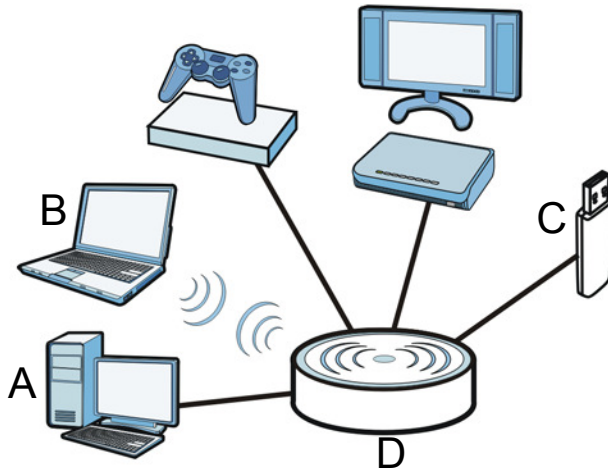
Table 47 Expert Mode > Applications > UPnP (continued)

LABEL	DESCRIPTION
Out Port	<p>Out Port is the well-known port that the WAN server uses to reply to the LAN computer that made the request using In Port.</p> <p>In the below example, In Port 8000 is paired with Out Port 80. A user on the WAN could enter http://A.B.C.D:8000 to access the internal computer with private IP address 192.168.77.55 where A.B.C.D is the WAN IP address or URL of the NBG6817.</p> <p>This field displays the port number of the UPnP entry.</p>
IP Address	This field displays the IP address of this UPnP entry.
Apply	Click Apply to save the setting to the NBG6817.
Cancel	Click Cancel to return to the previously saved settings.

13.6 File Sharing

You can also share files on a USB memory stick or hard drive connected to your NBG6817 with users on your network.

The following figure is an overview of the NBG6817's file-sharing server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the NBG6817 (**D**).

Figure 91 File Sharing Overview

Note: The read and write performance may be affected by amount of file-sharing traffic on your network, type of connected USB device and your USB version (3.0 or 2.0).

13.6.1 SAMBA Server Screen

Use this screen to set up file-sharing via the NBG6817 using Windows Explorer or the workgroup name. You can also configure the workgroup name and create file-sharing user accounts.

In **Expert** mode, click **Applications > File Sharing > SAMBA** to open the following screen.

Figure 92 Expert Mode > Applications > File Sharing > SAMBA

#	Enable	User Name	Password	USB1	USB2
1	<input type="checkbox"/>			None	None
2	<input type="checkbox"/>			None	None
3	<input type="checkbox"/>			None	None
4	<input type="checkbox"/>			None	None
5	<input type="checkbox"/>			None	None

The following table describes the labels in this screen.

Table 48 Expert Mode > Applications > File Sharing > SAMBA

LABEL	DESCRIPTION
SAMBA Setup	
Enable SAMBA	Select this to enable file sharing through the NBG6817 using Windows Explorer or by browsing to your work group.
Name	Specify the name to identify the NBG6817 in a work group.
Work Group	You can add the NBG6817 to an existing or a new workgroup on your network. Enter the name of the workgroup which your NBG6817 automatically joins. You can set the NBG6817's workgroup name to be exactly the same as the workgroup name to which your computer belongs to. Note: The NBG6817 will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.
Description	Enter the description of the NBG6817 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.
#	This is the index number of the user account.
Enable	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	Enter a user name that will be allowed to access the shared files. You can enter up to 20 characters. Only letters and numbers allowed.
Password	Enter the password used to access the shared files. You can enter up to 20 characters. Only letters and numbers are allowed. The password is case sensitive.

Table 48 Expert Mode > Applications > File Sharing > SAMBA

LABEL	DESCRIPTION
USB1/USB2	Specify the user's access rights to the USB storage device which is connected to the NBG6817's USB port. Read & Write - The user has read and write rights, meaning that the user can create and edit the files on the connected USB device. Read - The user has read rights only and can not create or edit the files on the connected USB device.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

13.6.2 FTP Server Screen

Use this screen to set up file sharing via the NBG6817 using FTP and create user accounts.

In **Expert** mode, click **Applications > File Sharing > FTP** to open the following screen.

Figure 93 Expert Mode > Applications > File Sharing > FTP

The screenshot shows the FTP Setup screen. At the top right are 'Apply' and 'Cancel' buttons. The 'FTP Setup' section has 'Enable FTP' with a radio button selected for 'Enable' and 'Disable' unselected. The 'Port' is set to 21. Below is a 'User Accounts' table with the following data:

#	Enable	User Name	Password	USB1	USB2	Upstream Bandwidth	Downstream Bandwidth
1	<input checked="" type="checkbox"/>	TEST	****	Read	Read	1000 KBytes	1000 KBytes
2	<input type="checkbox"/>			None	None		
3	<input type="checkbox"/>			None	None		
4	<input type="checkbox"/>			None	None		
5	<input type="checkbox"/>			None	None		

The following table describes the labels in this screen.

Table 49 Expert Mode > Applications > File Sharing > FTP

LABEL	DESCRIPTION
Enable FTP	Select this to enable the FTP server on the NBG6817 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.
#	This is the index number of the user account.
Enable	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	Enter a user name that will be allowed to access the shared files. You can enter up to 20 characters. Only letters and numbers allowed.
Password	Enter the password used to access the shared files. You can enter up to 20 characters. Only letters and numbers are allowed. The password is case sensitive.

Table 49 Expert Mode > Applications > File Sharing > FTP

LABEL	DESCRIPTION
USB1/USB2	Specify the user's access rights to the USB storage device which is connected to the NBG6817's USB port. Read & Write - The user has read and write rights, meaning that the user can create and edit the files on the connected USB device. Read - The user has read rights only and can not create or edit the files on the connected USB device. None - The user cannot access the files on the USB device(s) connected to the USB port.
Upstream Bandwidth	Enter the maximum bandwidth (in Kbps) allowed for incoming FTP traffic.
Downstream Bandwidth	Enter the maximum bandwidth (in Kbps) allowed for outgoing FTP traffic.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

13.6.3 Example of Accessing Your Shared Files From a Computer

You can use Windows Explorer or FTP to access the USB storage devices connected to the NBG6817.

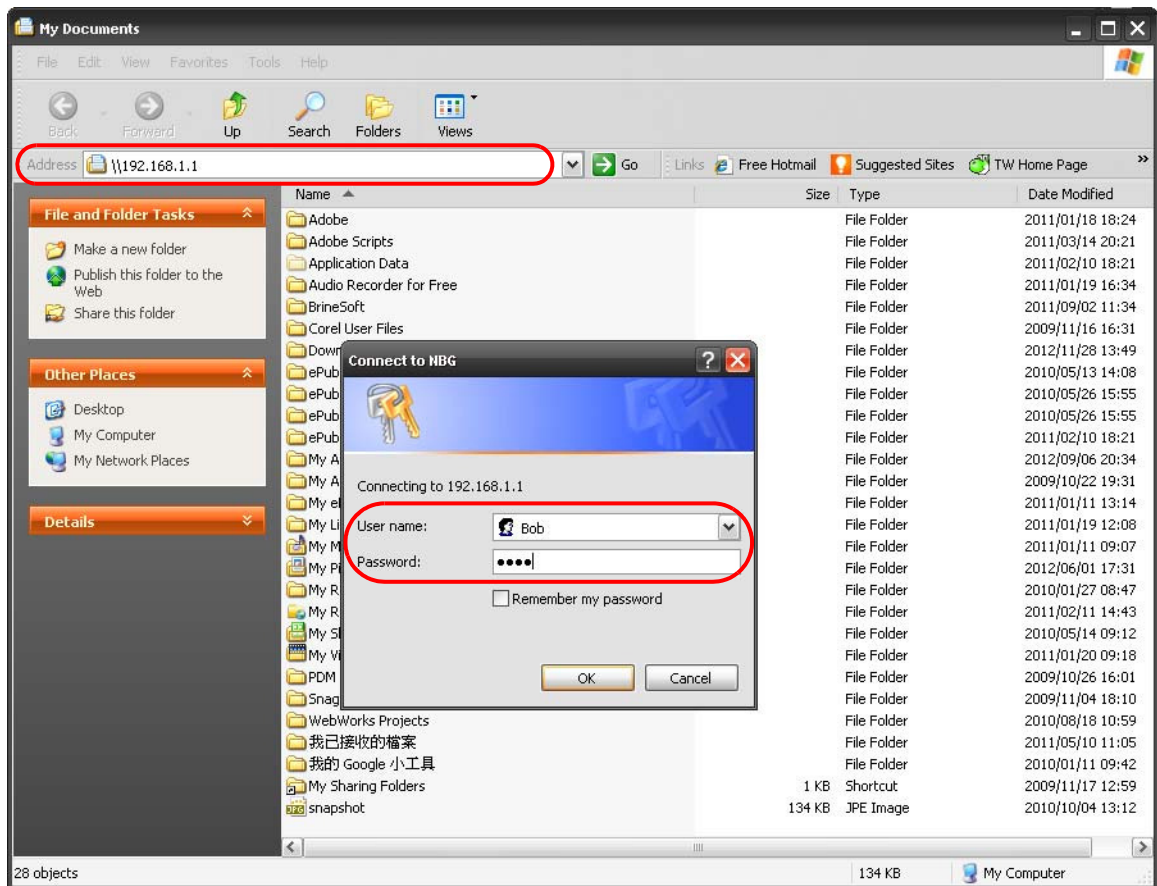
This example shows you how to use Microsoft's Windows XP to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

Use Windows Explorer to Share Files

You should have enabled file sharing and create a user account (Bob/1234 for example) with read and write access to USB 1 in the **Applications > File Sharing > SAMBA** screen.

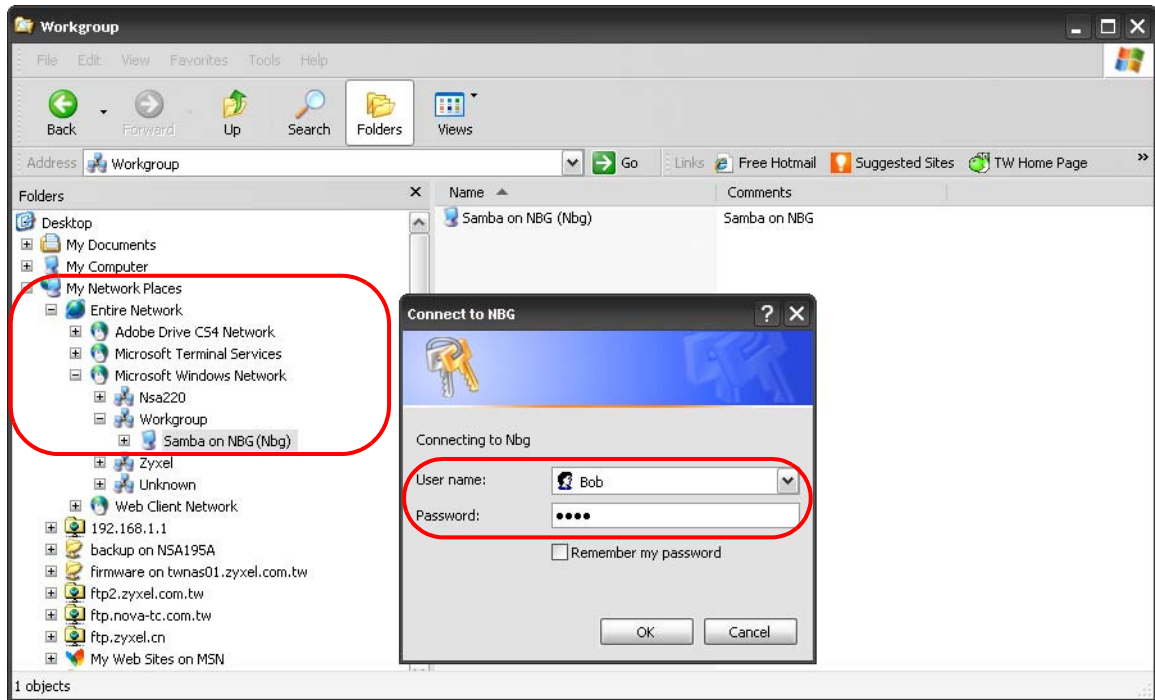
Open Windows Explorer to access the connected USB device using either Windows Explorer browser or by browsing to your workgroup.

- 1 In Windows Explorer's Address bar type a double backslash "\\ " followed by the IP address of the NBG6817 (the default IP address of the NBG6817 in router mode is 192.168.1.1) and press [ENTER]. A screen asking for password authentication appears. Type the user name and password (Bob and 1234 in this example) and click **OK**.



Note: Once you log into the shared folder via your NBG6817, you do not have to relogin unless you restart your computer.

- 2 You can also use the workgroup name to access files by browsing to the workgroup folder using the folder tree on the left side of the screen. It is located under **My Network Places**. In this example the workgroup name is the default "Workgroup".



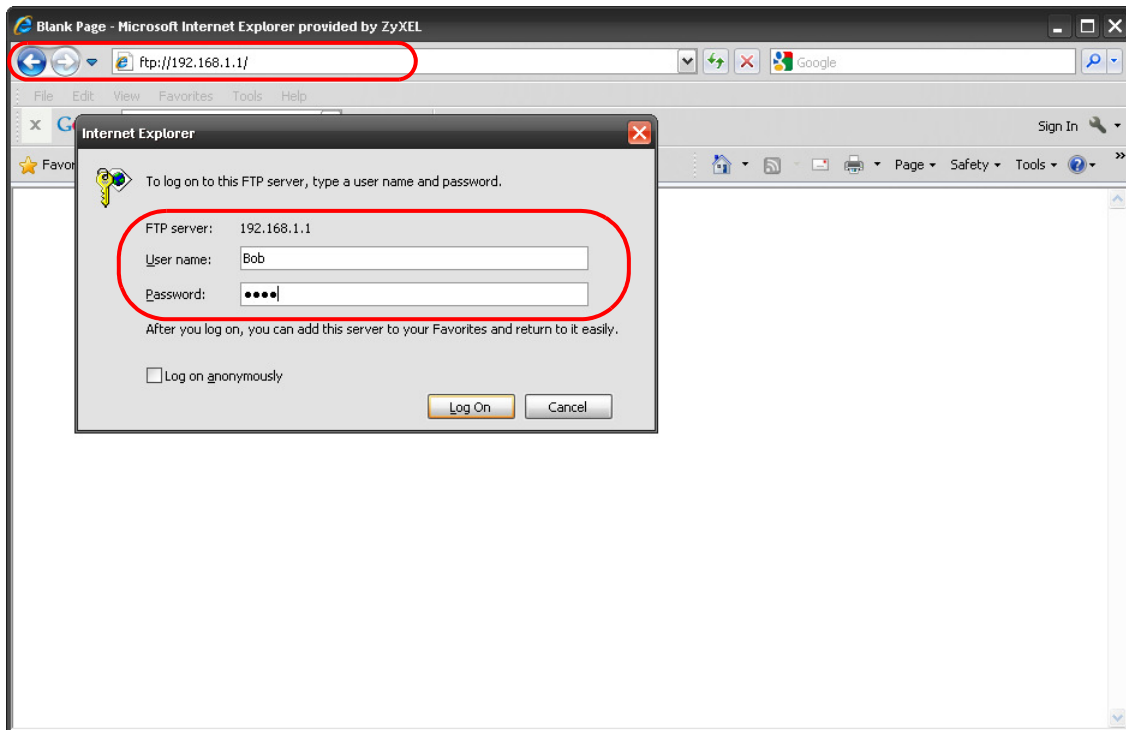
Use FTP to Share Files

You can use FTP to access the USB storage devices connected to the NBG6817. In this example, we use the web browser to share files via FTP from the LAN. The way or screen you log into the FTP server (on the NBG6817) varies depending on your FTP client. See your FTP client documentation for more information.

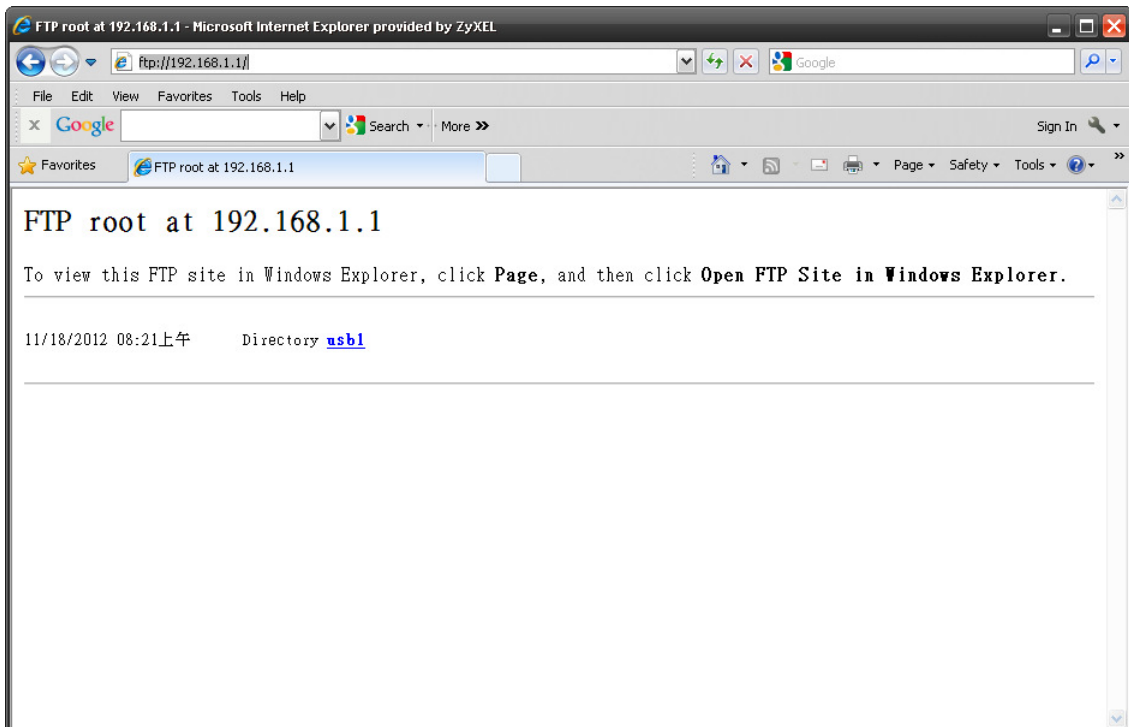
You should have enabled file sharing and create a user account (Bob/1234 for example) with read and write access to USB 1 in the **Applications > File Sharing > FTP** screen.

- 1 In your web browser's address or URL bar type "ftp://" followed by the IP address of the NBG6817 (the default LAN IP address of the NBG6817 in router mode is 192.168.1.1) and click **Go** or press [ENTER].

- 2 A screen asking for password authentication appears. Enter the user name and password (you configured in the **Applications > File Sharing > FTP** screen) and click **Log On**.



- 3 The screen changes and shows you the folder for the USB storage device connected to your NBG6817. Double-click the folder to display the contents in it.



13.7 ONE Connect Screen

One Connect is a ZyXEL-proprietary feature. It complies with the IEEE 1905.1 standard and allows auto-detection and auto-configuration.

If your wireless router supports ZyXEL ONE Connect, NBG6817 for example, you can download and install the ZyXEL ONE Connect App in your mobile device to check the connection status, do speed test, turn on or turn off the devices in your network, block or allow a device's access and set up a guest Wi-Fi network from the mobile device. You can even use the App to access the NBG6817's web configurator. The mobile device with the App installed must be connected to the NBG6817 wirelessly.

Note: You have to go to <https://mycloud.zyxel.com> and pair your device again when you reset the NBG6817.

Figure 94 ZyXEL ONE Connect App



Use this screen to enable or disable Wi-Fi auto-configuration on the NBG6817.

In **Expert** mode, click **Applications** > **ONE Connect** to open the following screen.

Figure 95 Expert Mode > Applications > ONE Connect



The following table describes the labels in this screen.

Table 50 Expert Mode > Applications > ONE Connect

LABEL	DESCRIPTION
ONE Connect	
QR Code	Scan the QR code and go to a website to download the ZyXEL ONE Connect App in your mobile device. One is for the iTunes App Store, and the other is for Google Play.

Table 50 Expert Mode > Applications > ONE Connect

LABEL	DESCRIPTION
ONE Connect Compatible Devices	
Automatically Update AP/ Repeater Wi-Fi Settings	Select Enable to allow the NBG6817 to automatically update the wireless settings on the APs or wireless repeaters (which also support ZyXEL One Connect) in its network. Select Disable to turn this feature off if you want to have the APs or repeaters in the network use different wireless settings.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

13.8 Technical Reference

The following section contains additional technical information about the NBG6817 features described in this chapter.

Customizing Keyword Blocking URL Checking

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

Domain Name or IP Address URL Checking

By default, the NBG6817 checks the URL's domain name or IP address when performing keyword blocking.

This means that the NBG6817 checks the characters that come before the first slash in the URL.

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

Full Path URL Checking

Full path URL checking has the NBG6817 check the characters that come before the last slash in the URL.

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

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

File Name URL Checking

Filename URL checking has the NBG6817 check all of the characters in the URL.

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

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

NAT Traversal

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

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

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

See the NAT chapter for more information on NAT.

Cautions with UPnP

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

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the NBG6817 allows multicast messages on the LAN only.

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

14.1 Overview

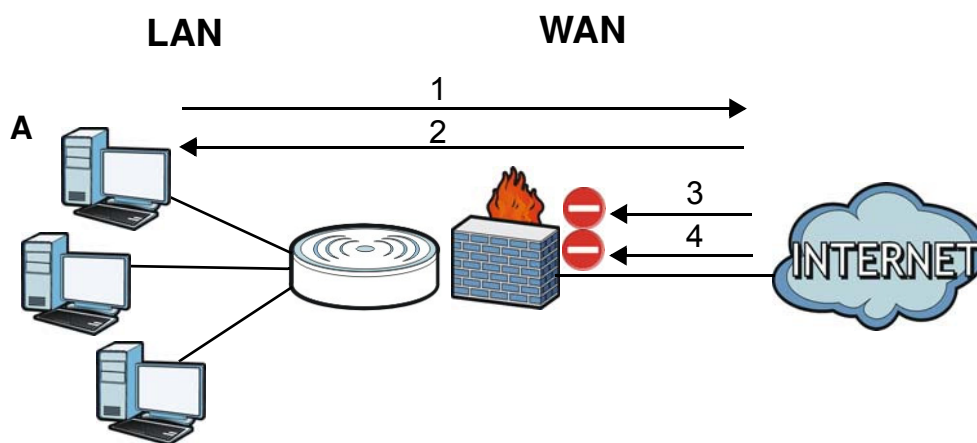
Use these screens to enable and configure the firewall that protects your NBG6817 and your LAN from unwanted or malicious traffic.

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 96 Default Firewall Action



14.1.1 What You Can Do

- Use the **IPv4 Firewall** screen to enable or disable the NBG6817's IPv4 firewall ([Section 14.2 on page 144](#)).
- Use the **IPv6 Firewall** screen to enable or disable the NBG6817's IPv6 firewall ([Section 14.3 on page 146](#)).

14.1.2 What You Need To Know

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

About the NBG6817 Firewall

The NBG6817'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 NBG6817's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG6817 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 NBG6817 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 NBG6817 has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas. The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

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

Guidelines For Enhancing Security With Your Firewall

- 1 Change the default password via Web Configurator.
- 2 Think about access control before you connect to the network in any way, including attaching a modem to the port.
- 3 Limit who can access your router.
- 4 Don't enable any local service (such as NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- 5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- 6 Protect against IP spoofing by making sure the firewall is active.
- 7 Keep the firewall in a secured (locked) room.

14.2 IPv4 Firewall Screen

Use this screen to enable or disable the NBG6817's IPv4 firewall. Click **Expert Mode > Security > IPv4 Firewall** to open the firewall setup screen.

Figure 97 Expert Mode > Security > IPv4 Firewall

IPv4 Firewall Apply Cancel

ICMP
Respond to Ping on:

Firewall Setup
Enable Firewall

Enable Firewall Rule
Enable Firewall Rule
Filter table type DROP ACCEPT

Add Firewall Rule
Service Name :
MAC Address :
Dest IP Address :
Source IP Address :
Protocol :
Dest Port Range : -
Source Port Range : -

Firewall Rule (Max Limit : 64)


#	Service Name	MAC Address	Dest IP	Source IP	Protocol	Dest Port Range	Source Port Range
1	TEST	00:AC:AB:AA:00:AA	192.168.1.100	0.0.0.0	TCP	-	-

The following table describes the labels in this screen.

Table 51 Expert Mode > Security > 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 NBG6817 will not respond to any incoming Ping requests when Disable is selected. Select LAN to reply to incoming LAN Ping requests. Select WAN to reply to incoming WAN Ping requests. Otherwise select LAN&WAN to reply to all incoming LAN and WAN Ping requests.
Firewall Setup	
Enable Firewall	Select this check box to activate the firewall. The NBG6817 performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Enable Firewall Rule	
Enable Firewall Rule	Select this check box to activate the firewall rules that you define (see Add Firewall Rule below).
Filter table type	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.

Table 51 Expert Mode > Security > IPv4 Firewall (continued)

LABEL	DESCRIPTION
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.
Dest IP Address	Enter the IP address of the computer to which traffic for the application or service is entering. The NBG6817 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 NBG6817 applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol (TCP , UDP or ICMP) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Add Rule	Click Add Rule to save the firewall rule.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Service Name	This is a name that identifies or describes the firewall rule.
MAC address	This is the MAC address of the computer for which the firewall rule applies.
Dest IP	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP	This is the IP address of the computer from which traffic for the application or service is initialized.
Protocol	This is the protocol (TCP , UDP or ICMP) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Delete	Click  to remove the firewall rule.
Apply	Click Apply to save the settings.
Cancel	Click Cancel to start configuring this screen again.

14.3 IPv6 Firewall Screen

This chapter shows you how to enable and create IPv6 firewall rules to filter IPv6 traffic.

Click **Expert Mode > Security > IPv6 Firewall**. The **IPv6 Firewall** screen appears as shown.


Figure 98 Expert Mode > Security > IPv6 Firewall

The following table describes the labels in this screen.

Table 52 Expert Mode > Security > IPv6 Firewall

LABEL	DESCRIPTION
Enable Firewall Rule	
Enable Firewall Rule	Select this check box to activate the firewall rules that you define (see Add Firewall Rule below).
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.
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.
Dest IP Address	Enter the IPv6 address of the computer to which traffic for the application or service is entering. The NBG6817 applies the firewall rule to traffic destined for this computer.
Source IP Address	Enter the IPv6 address of the computer that initializes traffic for the application or service. The NBG6817 applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol (TCP , UDP or ICMPv6) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	Enter the port number/range of the destination that defines the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	Enter the port number/range of the source that defines the traffic type, for example TCP port 80 defines web traffic.

Table 52 Expert Mode > Security > IPv6 Firewall (continued)

LABEL	DESCRIPTION
Add Rule	Click Add Rule to save the firewall rule.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
ServiceName	This is a name that identifies or describes the firewall rule.
MAC Address	This is the MAC address of the computer for which the firewall rule applies.
Dest IP	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP	This is the IP address of the computer to which traffic for the application or service is initialized.
Protocol	This is the protocol (TCP , UDP or ICMPv6) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	This is the port number/range of the destination that defines the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	This is the port number/range of the source that defines the traffic type, for example TCP port 80 defines web traffic.
Delete	Click  to remove the firewall rule.
Apply	Click Apply to save the settings.
Cancel	Click Cancel to restore your previously saved settings.

Maintenance

15.1 Overview

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

15.2 What You Can Do

- Use the **General** screen to set the timeout period of the management session ([Section 15.3 on page 149](#)).
- Use the **Password** screen to change your NBG6817's system password ([Section 15.4 on page 150](#)).
- Use the **Time** screen to change your NBG6817's time and date ([Section 15.5 on page 151](#)).
- Use the **Firmware Upgrade** screen to upload firmware to your NBG6817 ([Section 15.6 on page 153](#)).
- Use the **Backup/ Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration ([Section 15.7 on page 154](#)).
- Use the **Restart** screen to reboot the NBG6817 without turning the power off ([Section 15.8 on page 155](#)).
- Use the **Language** screen to change the language for the Web Configurator ([Section 15.9 on page 155](#)).
- Use the **Remote Management** screen to configure the interface/s from which the NBG6817 can be managed remotely and specify a secure client that can manage the NBG6817. ([Section 15.10 on page 156](#)).
- Use the **Log** screen to see the logs for the activity on the NBG6817 ([Section 15.11 on page 159](#)).
- Use the **Operation Mode** screen to select how you want to use your NBG6817 ([Section 15.13 on page 161](#)).

15.3 General Screen

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

Figure 99 Expert Mode > Maintenance > General

General		Apply	Cancel
System Name :	<input type="text" value="NBG6817"/>		
Domain Name :	<input type="text" value="local"/>		
Administrator Inactivity Timer :	<input type="text" value="0"/>		(minutes, 0 means no timeout)

The following table describes the labels in this screen.

Table 53 Expert Mode > Maintenance > General

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the NBG6817 in an Ethernet network.
Domain Name	Enter the domain name you want to give to the NBG6817.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

15.4 Password Screen

It is strongly recommended that you change your NBG6817's password.

If you forget your NBG6817's password (or IP address), you will need to reset the device. See [Section 15.8 on page 155](#) for details.

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

Figure 100 Expert Mode > Maintenance > Password

Password		Apply	Cancel
Old Password :	<input type="text"/>		
New Password :	<input type="text"/>		
Retype to Confirm :	<input type="text"/>		

The following table describes the labels in this screen.

Table 54 Expert Mode > Maintenance > Password

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.

Table 54 Expert Mode > Maintenance > Password (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

15.5 Time Screen

Use this screen to configure the NBG6817's time based on your local time zone. To change your NBG6817's time and date, click **Expert Mode > Maintenance > Time**. The screen appears as shown.

Figure 101 Expert Mode > Maintenance > Time

The following table describes the labels in this screen.

Table 55 Expert Mode > Maintenance > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your NBG6817. Each time you reload this page, the NBG6817 synchronizes the time with the time server.
Current Date	This field displays the date of your NBG6817. Each time you reload this page, the NBG6817 synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.

Table 55 Expert Mode > Maintenance > Time (continued)

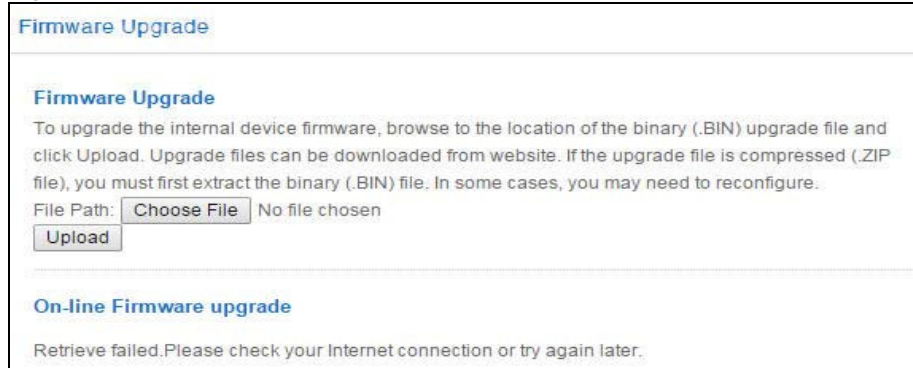
LABEL	DESCRIPTION
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you select Manual , enter the new time in this field and then click Apply .
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you select Manual , enter the new date in this field and then click Apply .
Get from Time Server	Select this radio button to have the NBG6817 get the time and date from the time server you specified below.
User Defined Time Server Address	Select User Defined Time Server Address and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected Daylight Savings . The at field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and select 2 in the at field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March . The time you select in the at field depends on your time zone. In Germany for instance, you would select 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected Daylight Savings . The at field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and select 2 in the at field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October . The time you select in the at field depends on your time zone. In Germany for instance, you would select 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

15.6 Firmware Upgrade Screen

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

Click **Expert Mode > Maintenance > Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your NBG6817.

Figure 102 Expert Mode > Maintenance > Firmware Upgrade



The following table describes the labels in this screen.

Table 56 Expert Mode > Maintenance > Firmware Upgrade

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

Note: Do not turn off the NBG6817 while firmware upload is in progress!

After you see the **Firmware Upload In Progress** screen, wait two minutes before logging into the NBG6817 again.

The NBG6817 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 103 Network Temporarily Disconnected



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

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

15.7 Backup/Restore Screen

Backup configuration allows you to back up (save) the NBG6817's current configuration to a file on your computer. Once your NBG6817 is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NBG6817.

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

Figure 104 Expert Mode > Maintenance > Backup/Restore

Backup/Restore

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

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

File Path : No file chosen

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

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

The following table describes the labels in this screen.

Table 57 Expert Mode > Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup	Click Backup to save the NBG6817's current configuration to your computer.
File Path	Click Choose File to find the location of the file you want to upload in this field.
Choose File	Click Choose File to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.

Table 57 Expert Mode > Maintenance > Backup/Restore (continued)

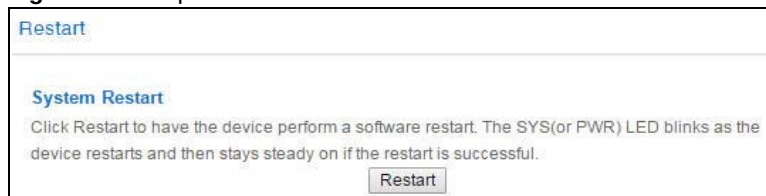
LABEL	DESCRIPTION
Upload	<p>Click Upload to begin the upload process.</p> <p>Note: Do not turn off the NBG6817 while configuration file upload is in progress.</p> <p>After you see a "configuration upload successful" screen, you must then wait one minute before logging into the NBG6817 again. The NBG6817 automatically restarts in this time causing a temporary network disconnect.</p> <p>If you see an error screen, click Back to return to the Backup/Restore screen.</p>
Reset	<p>Pressing the Reset button in this section clears all user-entered configuration information and returns the NBG6817 to its factory defaults.</p> <p>You can also press the RESET button on the rear panel to reset the factory defaults of your NBG6817. Refer to the chapter about introducing the Web Configurator for more information on the RESET button.</p>

Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default NBG6817 IP address (192.168.1.1). See [Appendix B on page 176](#) for details on how to set up your computer's IP address.

15.8 Restart Screen

System restart allows you to reboot the NBG6817 without turning the power off.

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

Figure 105 Expert Mode > Maintenance > Restart

Click **Restart** to have the NBG6817 reboot. This does not affect the NBG6817's configuration.

15.9 Language Screen

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

Select the language you prefer and click **Apply**. The Web Configurator language changes after a while without restarting the NBG6817. Click **Expert Mode > Maintenance > Language** to open the following screen.

Figure 106 Expert Mode > Maintenance > Language

The screenshot shows a web interface for language selection. At the top, the word "Language" is displayed in blue. To its right are two buttons: "Apply" and "Cancel". Below this, the text "Language selection :" is followed by a dropdown menu currently set to "English".

15.10 Remote Management Screen

Remote Management allows you to manage your NBG6817 from a remote location through the LAN/WLAN or WAN interface.

15.10.1 Remote Access

Use this screen to change your NBG6817's remote management settings. You can use Telnet, HTTP or HTTPS to access and manage the NBG6817.

Click **Expert Mode > Maintenance > Remote Management > Remote Access** to open the following screen.

Figure 107 Expert Mode > Maintenance > Remote Management > Remote Access

Remote Access
Apply
Cancel

WWW

Port:

Access Status:

Secured Client IP Address: All Selected

Note:

1. For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.
2. You may also need to create a Firewall rule.

Telnet

Port:

Access Status:

Secured Client IP Address: All Selected

Note:

You may also need to create a Firewall rule.

HTTPS

Port:

Access Status:

Secured Client IP Address: All Selected

Note:

You may also need to create a Firewall rule.

The following table describes the labels in this screen.

Table 58 Expert Mode > Maintenance > Remote Management > WAN Access

LABEL	DESCRIPTION
WWW	
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the NBG6817 using this service.
Secured Client IP Address	Select All to allow all computers to access the NBG6817. Otherwise, check Selected and specify the IP address of the computer that can access the NBG6817.
Telnet	

Table 58 Expert Mode > Maintenance > Remote Management > WAN Access

LABEL	DESCRIPTION
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the NBG6817 using this service.
Secured Client IP Address	Select All to allow all computes to access the NBG6817. Otherwise, check Selected and specify the IP address of the computer that can access the NBG6817.
HTTPS	
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the NBG6817 using this service.
Secured Client IP Address	Select All to allow all computes to access the NBG6817. Otherwise, check Selected and specify the IP address of the computer that can access the NBG6817.
Apply	Click Apply to save your changes back to the NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

15.10.2 Wake On LAN

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

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

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

Figure 108 Expert Mode > Maintenance > Remote Management > Wake On LAN

Wake On LAN [Apply] [Cancel]

Wake On LAN over WAN Settings

Enable Wake On Lan over WAN Enable Disable

Port:

Wake On LAN

Wake MAC Address: [Start]

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

The following table describes the labels in this screen.

Table 59 Expert Mode > Maintenance > Remote Management > Wake On LAN

LABEL	DESCRIPTION
Wake On LAN over WAN Settings	
Enable Wake On LAN over WAN	Select Enable to have the NBG6817 forward a WoL "Magic Packet" to all devices on the LAN if the packet comes from the WAN or remote network and uses the port number specified in the Port field. A LAN device whose hardware supports Wake on LAN then will be powered on if it is turned off previously.
Port	Type a port number from which a WoL packet is forwarded to the LAN.
Wake On LAN	
Wake MAC Address	This field displays the hostname and MAC address of the LAN device by default. Otherwise, select User define 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 NBG6817 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 NBG6817.
Cancel	Click Cancel to begin configuring this screen afresh.

15.11 Log Screen

The Web Configurator allows you to look at all of the NBG6817's logs in one location.

You can configure which logs to display in the Log screen. Select the logs you wish to display. Click **Apply** to save your settings. Click **Cancel** to start the screen afresh.

Use this screen to see the logged messages for the NBG6817. The log wraps around and deletes the old entries after it fills. Select what logs you want to see from the **Display** drop list. The log choices depend on your settings above this screen. Click **Refresh** to renew the log screen. Click **Clear Log** to delete all the logs.

Figure 109 Expert Mode > Maintenance > Log

The screenshot shows the 'Log' configuration page. At the top right are 'Apply' and 'Cancel' buttons. Under 'Active Log and Alert', there are three checkboxes: 'System Errors' (unchecked), 'On-line Firmware upgrade' (unchecked), and 'Access Control' (checked). Below this is a 'Display:' dropdown menu set to 'All Logs', with 'Refresh' and 'Clear Log' buttons. A 'Summary' table is displayed below, showing log entries with columns for '#', 'Time', and 'Message'.

#	Time	Message
1	2015 Jan 29 17:16:54	user.notice netprobe: netprb_info_collect: Enter
2	2015 Jan 29 17:16:44	user.notice netprobe: netprb_info_collect: Enter
3	2015 Jan 29 17:16:34	user.notice netprobe: netprb_info_collect: Enter
4	2015 Jan 29 17:16:29	daemon.info aperture-controller.sh: Sleeping 300 seconds...
5	2015 Jan 29 17:16:29	daemon.info aperture-controller.sh: Test returned -1, bw up 0 / down 0
6	2015 Jan 29 17:16:28	daemon.info aperture[14833]: (INFO) Aperture shutting down.
7	2015 Jan 29 17:16:28	daemon.info aperture[14833]: (INFO) Discarding outlier

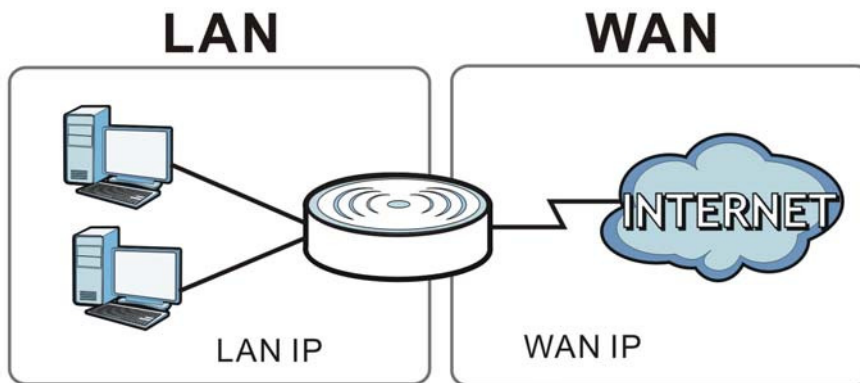
15.12 System Operation Mode Overview

The **Sys OP Mode** (System Operation Mode) function lets you configure your NBG6817 as a router or access point. You can choose between **Router Mode**, and **Access Point Mode** depending on your network topology and the features you require from your device.

The following describes the device modes available in your NBG6817.

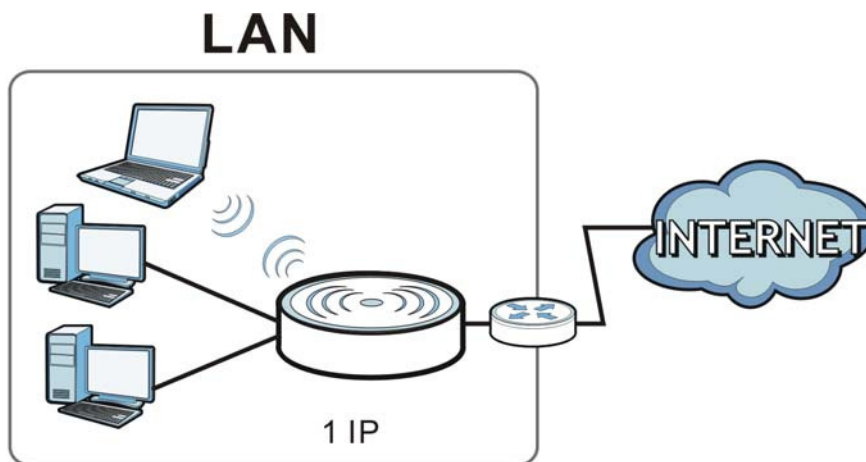
Router

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

Figure 110 LAN and WAN IP Addresses in Router Mode

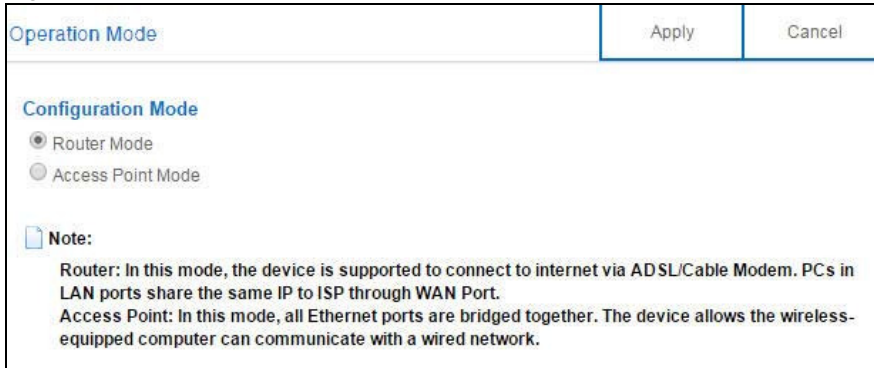
Access Point

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

Figure 111 Access Point Mode

15.13 Operation Mode Screen

Use this screen to select how you want to use your NBG6817.

Figure 112 Expert Mode > Maintenance > Operation Mode


Operation Mode Apply Cancel

Configuration Mode

Router Mode
 Access Point Mode

Note:

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

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

The following table describes the labels in the **Operation Mode** screen.

Table 60 Expert Mode > Maintenance > Operation Mode

LABEL	DESCRIPTION
Configuration Mode	
Router Mode	Select Router Mode if your device routes traffic between a local network and another network such as the Internet. This mode offers services such as a firewall or bandwidth management. You can configure the IP address settings on your WAN port. Contact your ISP or system administrator for more information on appropriate settings.
Access Point Mode	Select Access Point Mode if your device bridges traffic between clients on the same network. <ul style="list-style-type: none"> • In Access Point Mode, all Ethernet ports have the same IP address. • All ports on the rear panel of the device are LAN ports, including the port labeled WAN. There is no WAN port. • The DHCP server on your device is disabled. • Router functions (such as NAT, bandwidth management, remote management, firewall and so on) are not available when the NBG6817 is in Access Point Mode. • The IP address of the device on the local network is set to 192.168.1.2.
Apply	Click Apply to save your settings.
Cancel	Click Cancel to return your settings to the default (Router).

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

Troubleshooting

16.1 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](#)
- [NBG6817 Access and Login](#)
- [Internet Access](#)
- [Resetting the NBG6817 to Its Factory Defaults](#)
- [Wireless Connections](#)
- [USB Device Problems](#)

16.2 Power, Hardware Connections, and LEDs

The NBG6817 does not turn on. None of the LEDs turn on.

- 1 Make sure you are using the power adaptor or cord included with the NBG6817.
- 2 Make sure the power adaptor or cord is connected to the NBG6817 and plugged in to an appropriate power source. Make sure the power source is turned on.
- 3 Disconnect and re-connect the power adaptor or cord to the NBG6817.
- 4 If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.7 on page 12](#).
- 2 Check the hardware connections. See the Quick Start Guide.
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Disconnect and re-connect the power adaptor to the NBG6817.

- 5 If the problem continues, contact the vendor.

16.3 NBG6817 Access and Login

I don't know the IP address of my NBG6817.

- 6 The default IP address of the NBG6817 in **Router Mode** is **192.168.1.1**. If the NBG6817 obtains a WAN IP address in the same subnet as the LAN IP address 192.168.1.1, the default LAN IP address will be changed to 10.0.0.1 automatically. See [Auto-IP Change on page 75](#) for more information. The default IP address of the NBG6817 in **Access Point Mode** is **192.168.1.2**.
- 7 If you changed the IP address and have forgotten it, you might get the IP address of the NBG6817 in **Router Mode** by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the NBG6817 (it depends on the network), so enter this IP address in your Internet browser.
- 8 If your NBG6817 in **Access Point Mode** is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.
- 9 Reset your NBG6817 to change all settings back to their default. This means your current settings are lost. See [Section 16.5 on page 167](#) in the **Troubleshooting** for information on resetting your NBG6817.

I forgot the password.

- 1 The default password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 16.5 on page 167](#).

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

- 1 Make sure you are using the correct IP address.
- 2 The default IP address of the NBG6817 in **Router Mode** is **192.168.1.1**. If the NBG6817 obtains a WAN IP address in the same subnet as the LAN IP address 192.168.1.1, the default LAN IP address will be changed to 10.0.0.1 automatically. See [Auto-IP Change on page 75](#) for more information. The default IP address of the NBG6817 in **Access Point Mode** is **192.168.1.2**.
 - If you changed the IP address ([Section 12.4 on page 115](#)), use the new IP address.

- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I don't know the IP address of my NBG6817](#).
- 3 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
 - 4 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See [Appendix B on page 171](#).
 - 5 Make sure your computer is in the same subnet as the NBG6817. (If you know that there are routers between your computer and the NBG6817, skip this step.)
 - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See [Section 12.4 on page 115](#).
 - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG6817. See [Section 12.4 on page 115](#).
 - 6 Reset the device to its factory defaults, and try to access the NBG6817 with the default IP address. See [Section 1.5 on page 11](#).
 - 7 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the NBG6817 using another service, such as Telnet. If you can access the NBG6817, check the remote management settings and firewall rules to find out why the NBG6817 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 NBG6817.

- 1 Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.
- 2 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.
- 3 Disconnect and re-connect the power adaptor or cord to the NBG6817.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 16.5 on page 167](#).

16.4 Internet Access

I cannot access the Internet.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
- 2 Go to **Expert > Maintenance > Operation Mode**. Check your System Operation Mode setting.
 - If the NBG6817 is in **Router Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access. Your computer and the NBG6817 should be in the same subnet.
 - If the NBG6817 is in **Access Point Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access and your computer is set to obtain an dynamic IP address.
- 3 If the NBG6817 is in **Router Mode**, make sure you entered your ISP account information correctly in the wizard or the WAN screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 4 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
- 5 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 6 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NBG6817), but my Internet connection is not available anymore.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.7 on page 12](#).
- 2 Reboot the NBG6817.
- 3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

- 1 There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.7 on page 12](#). If the NBG6817 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Check the signal strength. If the signal strength is low, try moving the NBG6817 closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
- 3 Reboot the NBG6817.
- 4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestion

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

16.5 Resetting the NBG6817 to Its Factory Defaults

If you reset the NBG6817, you lose all of the changes you have made. The NBG6817 re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

You will lose all of your changes when you push the **RESET** button.

To reset the NBG6817:

- 1 Make sure the power LED is on.
- 2 Press the **RESET** button for one to four seconds to restart/reboot the NBG6817.
- 3 Press the **RESET** button for longer than five seconds to set the NBG6817 back to its factory-default configurations.

If the NBG6817 restarts automatically, wait for the NBG6817 to finish restarting, and log in to the Web Configurator. The password is "1234".

If the NBG6817 does not restart automatically, disconnect and reconnect the NBG6817's power. Then, follow the directions above again.

16.6 Wireless Connections

I cannot access the NBG6817 or ping any computer from the WLAN.

- 1 Make sure the wireless LAN is enabled on the NBG6817.
- 2 Make sure the wireless adapter on your computer is working properly.
- 3 Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the NBG6817.
- 4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG6817.
- 5 Check that both the NBG6817 and the wireless adapter on your computer are using the same wireless and wireless security settings.
- 6 Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the NBG6817.

- 7 Make sure you allow the NBG6817 to be remotely accessed through the WLAN interface. Check your remote management settings.
 - See the chapter on [Wireless LAN](#) in the User's Guide for more information.

I set up URL keyword blocking, but I can still access a website that should be blocked.

Make sure that you enable parental control in the **Parental Control** screen, set up rules and turn on the rules. Make sure that the keywords that you type are listed in the rule's **Keyword List**.

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

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

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

Refer to [Appendix B on page 176](#) for instructions on how to change your computer's IP address.

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

The following factors may cause interference:

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

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

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

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

16.7 USB Device Problems

I cannot access or see a USB device that is connected to the NBG6817.

- 1 Disconnect the problematic USB device, then reconnect it to the NBG6817.
- 2 Ensure that the USB device has power.
- 3 Check your cable connections.
- 4 Restart the NBG6817 by disconnecting the power and then reconnecting it.
- 5 If the USB device requires a special driver, install the driver from the installation disc that came with the device. After driver installation, reconnect the USB device to the NBG6817 and try to connect to it again with your computer.
- 6 If the problem persists, contact your vendor.

What kind of USB devices do the NBG6817 support?

- 1 It is strongly recommended to use version 2.0 or higher USB storage devices (such as NTFS or FAT32 file system, USB hard drives) and/or USB devices. Other USB products are not guaranteed to function properly with the NBG6817.
- 2 The NBG6817 do not support 3G/4G USB dongles.