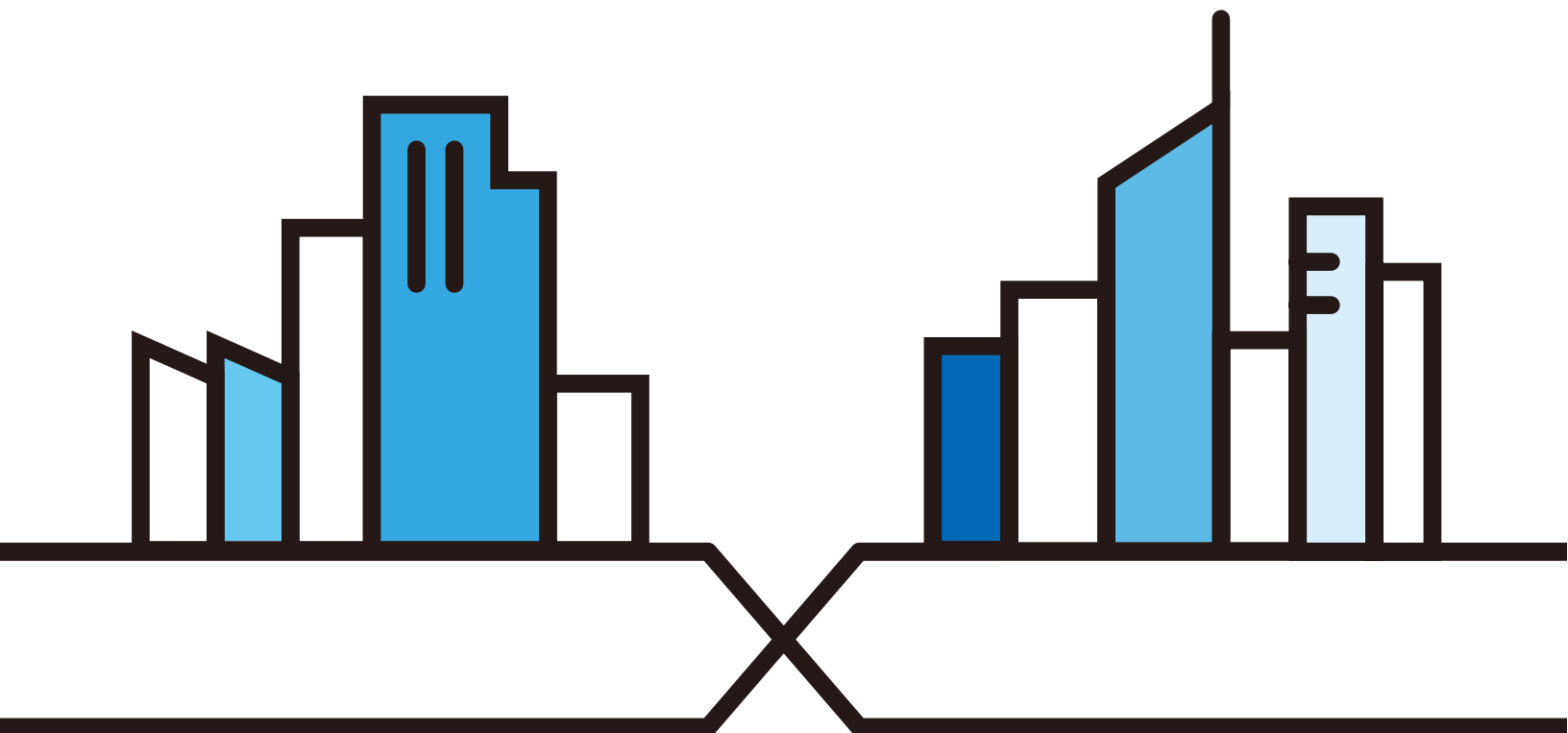# ZYXEL

Your Networking Ally

User's Guide

NBG6604

AC1200 Dual-Band Wireless Router

Default Login Details	
LAN IP Address	http://myrouter (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 NBG6604 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 NBG6604.

Document Conventions

Warnings and Notes

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

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

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

Syntax Conventions

- The NBG6604 may be referred to as the "NBG6604" or the "device" in this guide.

- Product labels, screen names, field labels and field choices are all in **bold** font.

- A right angle bracket (>) within a screen name denotes a mouse click. For example, **WAN** > **Internet Connection**: **IPoE Encapsulation** means you first click **WAN** in the navigation panel, then the **Internet Connection** sub menu and finally select the **IPoE Encapsulation** field option to display the **WAN** > **Internet Connection** screen for **IPoE Encapsulation** connection type.

Icons Used in Figures

Figures in this user guide may use the following generic icons. The NBG6604 icon is not an exact representation of your device.

NBG6604	Generic Router or Modem	Wireless Signal
Switch	Firewall	Printer
Server		

Table of Contents

CHAPTER 1
Introduction

1.1 Overview

This chapter introduces the main features and applications of the NBG6604.

The NBG6604 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 NBG6604 is able to use both 2.4GHz and 5GHz bands at the same time.

A range of services such as a firewall are also available for secure Internet access.

1.2 Applications

You can have the following networks with the NBG6604:

- **Wired**. You can connect network devices via the Ethernet ports of the NBG6604 so that they can communicate with each other and access the Internet.
- **Wireless**. Wireless clients can connect to the NBG6604 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 NBG6604

Use any of the following methods to manage the NBG6604:

- 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 NBG6604.
- Web Configurator. This is recommended for everyday management of the NBG6604 using a (supported) web browser.
- Zyxel ONE Connect App. See .

1.4 Good Habits for Managing the NBG6604

Do the following things regularly to make the NBG6604 more secure and to manage the NBG6604 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 NBG6604 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG6604. You could simply restore your last configuration.

1.5 Resetting the NBG6604

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 NBG6604 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 NBG6604.

3   Press the **RESET** button for longer than five seconds to set the NBG6604 back to its factory-default configurations.

1.6 The WPS Button

Your NBG6604 supports Wi-Fi Protected Setup (WPS), which is a quick way to set up a secure wireless network. WPS is an industry standard specification defined by the Wi-Fi Alliance.

WPS allows you to 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 top panel of the NBG6604 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 NBG6604.

Note: You must activate WPS in the NBG6604 and in the other wireless device within two minutes of each other.

1.7 LEDs

Figure 1 Top Panel
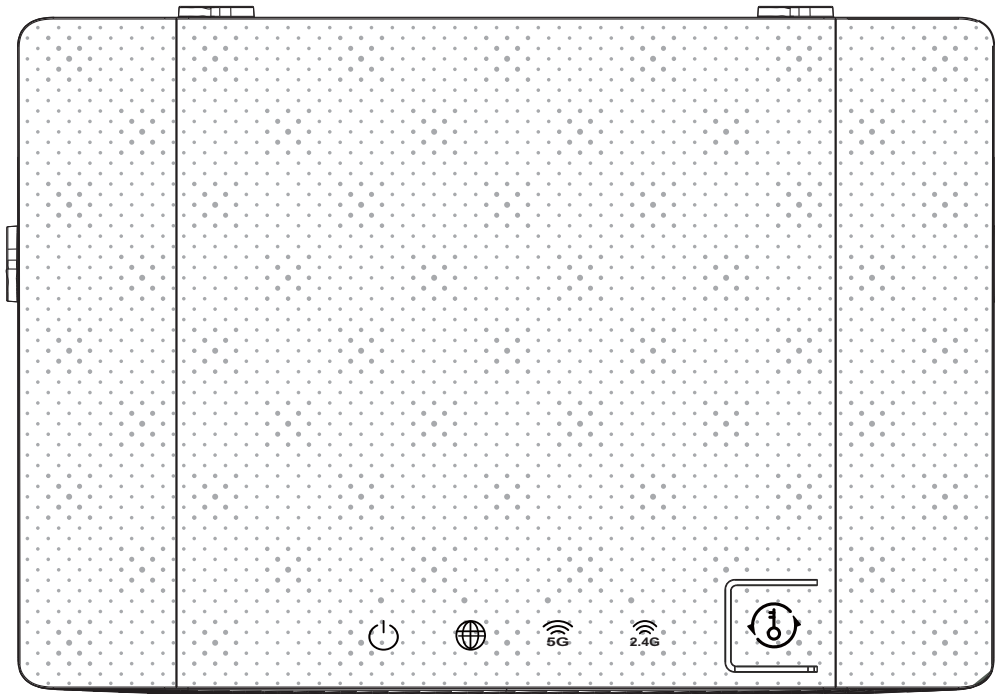
Table 1 Top Panel LEDs

FUNCTION	COLOR	STATUS	BEHAVIOR
Power/SYS	White	On	The NBG6604 is ready.
		Off	The NBG6604 is powered off.
		Blinking	The firmware is being updated and restored. System is booting.
Internet	White	On	The IP connection is available but no traffic.
		Off	The IP connection is not available.
		Blinking	The NBG6604 is transmitting/Receiving traffic.
WLAN 5G	White Amber	On	The WLAN interface is enabled.
		Off	The WLAN interface is disabled.
		White blinking	The NBG6604 is transmitting/receiving data.
		Amber blinking	The WPS process is in progress (at the same time, disable the white LED).
		Amber steady off	The WPS process is inactive.

Table 1   Top Panel LEDs (continued)

FUNCTION	COLOR	STATUS	BEHAVIOR
WLAN 2.4G	White Amber	On	The WLAN interface is enabled.
		Off	The WLAN interface is disabled.
		White blinking	The NBG6604 is transmitting/receiving data.
		Amber blinking	The WPS process is in progress (at the same time, disable the white LED).
		Amber steady off	The WPS process is inactive.
Note: When you connect the power, only the power/sys LED blinks. Others are off -> system ready -> all LEDs follow their behavior described in this table.			

Table 2   Buttons and Interface Behavior

FUNCTION	LABEL	DESCRIPTION/BEHAVIOR	LOCATION
Power Jack	DV IN 12v 1A	Connect the included power adapter.	Rear
Reset/Restore Button	Reset	- Press the button for 5 or less than 5 seconds, system will reboot. - Press the button for more than 5 seconds, system will reset configuration.	Rear
WPS Button		- WPS button can trigger both 2.4G and 5G. - WPS can work with 2.4G and 5G at the same time. - WPS LED will be off while the device is connected to clients (2.4G client or 5G client or both 2.4G/5G clients).	Top
Ethernet LAN	LAN WAN	WAN x1: - RJ45 Connector LAN x4: - RJ45 Connector	Rear

Figure 2   Rear Panel
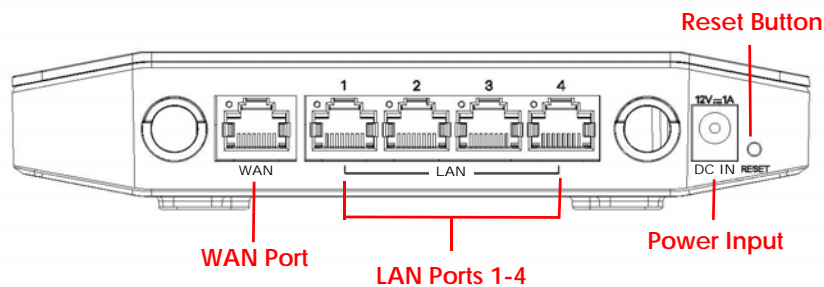
1.8 Wall Mounting

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

Table 3   Wall Mounting Information

Distance between holes	83 mm
M4 Screws	Two
Screw anchors (optional)	Two

Figure 3   Screw Specifications
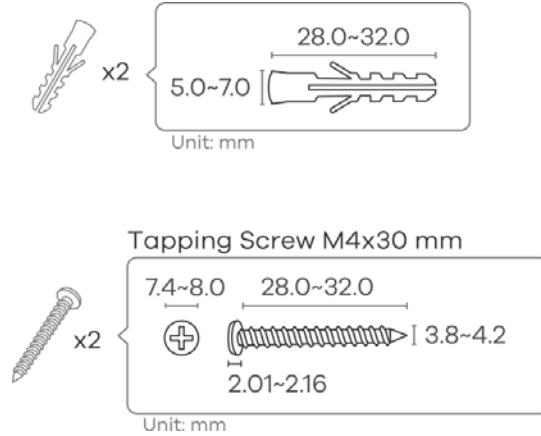
1   Select a position free of obstructions on a wall strong enough to hold the weight of the device.

2   Mark two holes on the wall at the appropriate distance apart for the screws.

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

3   If using screw anchors, drill two holes for the screw anchors into the wall. Push the anchors into the full depth of the holes, then insert the screws into the anchors. Do not insert the screws all the way in - leave a small gap of about 0.5 cm.

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

4   Make sure the screws are fastened well enough to hold the weight of the NBG6604 with the connection cables.

5   Align the holes on the back of the NBG6604 with the screws on the wall. Hang the NBG6604 on the screws.

Figure 4 Wall Mounting Example
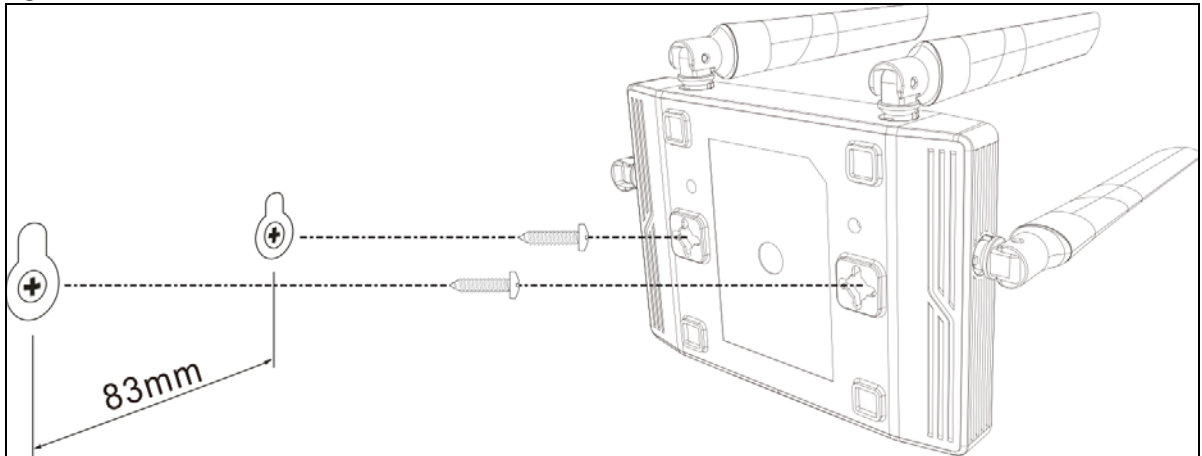
CHAPTER 2
Introducing the Web Configurator

2.1 Overview

This chapter describes how to access the NBG6604 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 NBG6604 via Internet browser. Use a browser that supports HTML5, such as Internet Explorer 11.0 and later versions, Mozilla Firefox 50 and later versions, Safari 10.0 and later versions, Edge 14 and later versions or Google Chrome 54 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

- JavaScript (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter (Chapter 15 on page 101) to see how to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

1   Make sure your NBG6604 hardware is properly connected and prepare your computer or computer network to connect to the NBG6604 (refer to the Quick Start Guide).

2   Launch your web browser.

3   The NBG6604 is in router mode by default. Type "http://myrouter" as the website address. If the NBG6604 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 52 for more information.

If the NBG6604 is in access point mode, the IP address will be 192.168.1.2. See Chapter 4 on page 25 for more information about the modes of the NBG6604.

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 17 for the eaZy123 setup screens.

The Web Configurator initially displays the following login screen.

Figure 5   Login Screen

The following table describes the labels in this screen.

Table 4   Login Screen

LABEL	DESCRIPTION
Please enter the device's administrator 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 6 Change Default Password Screen

The following table describes the labels in this screen.

Table 5   Change Default Password Screen

LABEL	DESCRIPTION
Enter your new password here	Type a new password.
Confirm password	Retype the password for confirmation.
Change	Click **Change** to save your changes back to the NBG6604.

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 14 on page 91 to change this). Simply log back into the NBG6604 if this happens.

C HAPTER 3
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://myrouter" as the website address. Type "1234" (default) as the password and click **Login**.

Note: The eaZy 123 wizard appears automatically when the NBG6604 is accessed for the first time or when you reset the NBG6604 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 7   Unable to continue: WAN
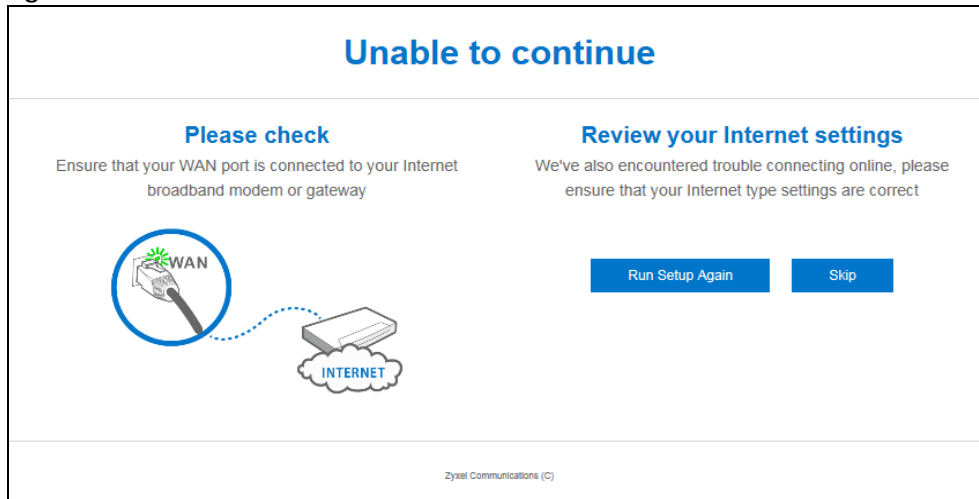
Figure 8   Detecting your Internet Connection Type

Figure 9   eaZy 123 Setup

3.3 Internet Type

The NBG6604 offers three WAN selection types. They are: **Automatic - DHCP**, **PPPoE**, and **Static**. Configure the Internet type settings on your NBG6604 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

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 NBG6604 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG6604 does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Figure 11 WAN Selection Type: PPPoE

The following table describes the labels in this screen.

Table 6 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

The following table describes the labels in this screen.

Table 7 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 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 NBG6604 in the second part. The default wireless security setting is WPA2-PSK.

Figure 13   Wireless Network

The following table describes the labels in this screen.

Table 8   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 NBG6604, 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 5GHz wireless network	Select this check box to configure different SSID and wireless security settings for the NBG6604's 5 GHz wireless network. If you do not select this option, the NBG6604 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 NBG6604, 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
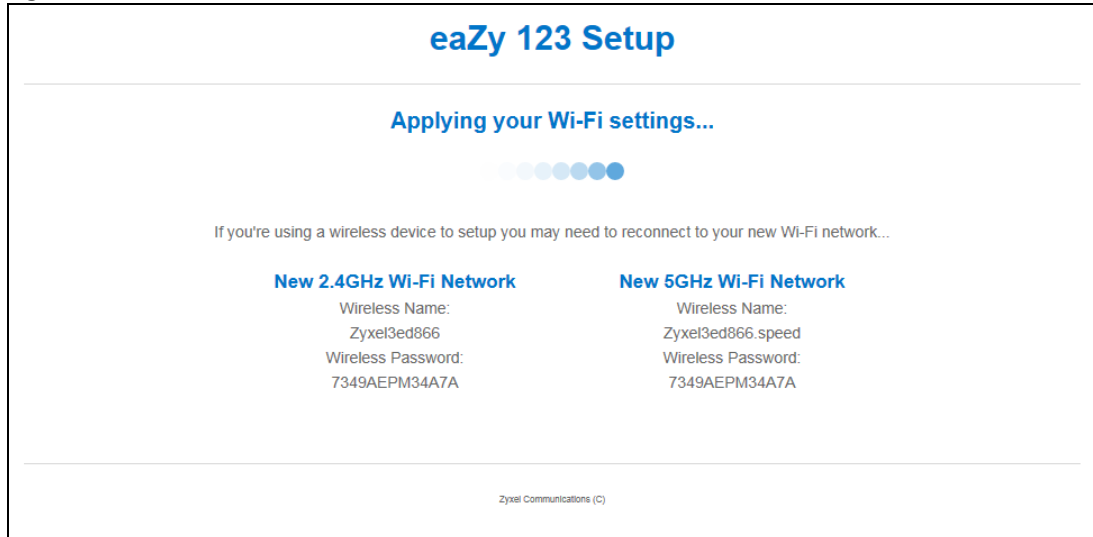
Congratulations! Open a web browser, such as Internet Explorer, to visit your favorite website.

Note: If you cannot access the Internet when your computer is connected to one of the NBG6604's LAN ports, check your connections. Then turn the NBG6604 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
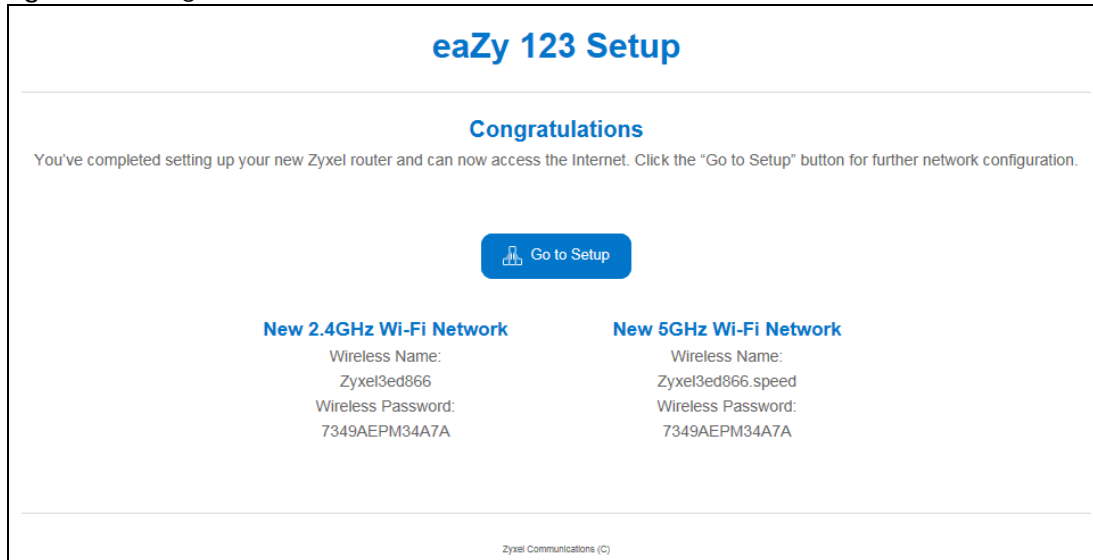
You have successfully set up your NBG6604 to operate on your network and access the Internet.

CHAPTER 4
Operating Modes

4.1 Overview

This chapter introduces the different operating modes of your NBG6604, or simply how the NBG6604 is being used in the network.

4.1.1 Operating Modes

This refers to the operating mode of the NBG6604, which can act as a:

- **Router**: This is the default operating mode of the NBG6604. Use this mode to connect the local network to another network, like the Internet. Go to Section 5.2 on page 26 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 NBG6604 wirelessly. Go to Section 6.4 on page 34 to view the **Status** screen in this mode.

For more information on these modes and to change the mode of your NBG6604, refer to Chapter 14 on page 99.

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

When changing to another mode, the IP address of the NBG6604 changes. The running applications and services of the network devices connected to the NBG6604 can be interrupted.

CHAPTER 5
Router Mode

5.1 Overview

The NBG6604 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 NBG6604 connects the local network (**LAN1 ~ LAN4**) to the Internet.

Figure 16 NBG6604 Network
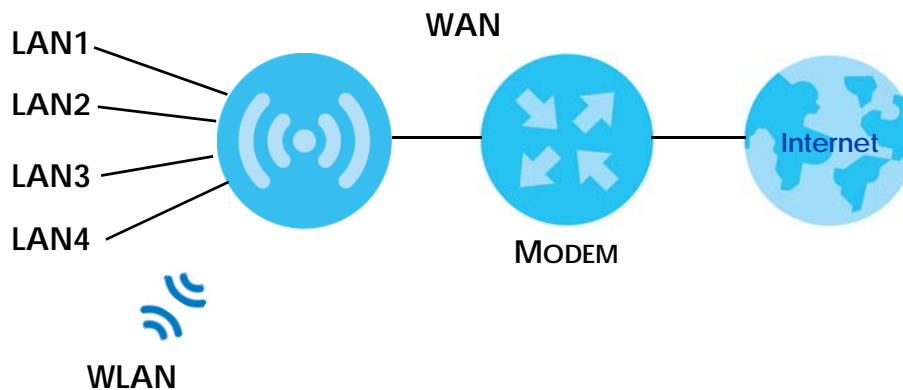
5.2 Router Mode Status Screen

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

Figure 17 Status > System Status: Router Mode
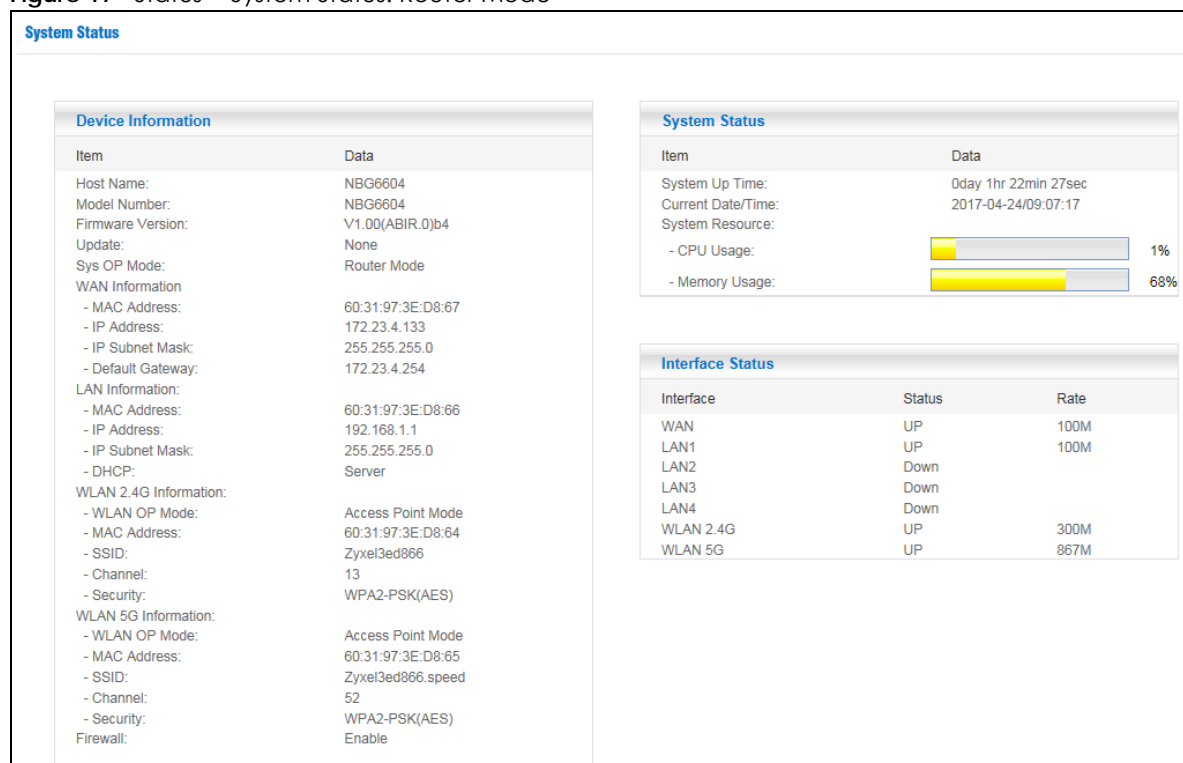
The following table describes the labels shown in the **Status** screen.

Table 9   Status > System Status: Router Mode

LABEL	DESCRIPTION
Device Information	
Item	This column shows the type of data the NBG6604 is recording.
Data	This column shows the actual data recorded by the NBG6604.
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 4.1.1 on page 25) to which the NBG6604 is set - **Router Mode**.
WAN Information	
MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
IP Address	This shows the WAN port's IP address.
IP Subnet Mask	This shows the WAN port's subnet mask.
Default Gateway	This shows the WAN port's gateway IP address.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP	This shows the LAN port's DHCP role - **Server** or **Disable**.
WLAN 2.4G Information	

Table 9   Status > System Status: Router Mode (continued)

LABEL	DESCRIPTION
WLAN OP Mode	This is the device mode (Section 4.1.1 on page 25) to which the NBG6604'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 NBG6604 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 NBG6604 is using.
WLAN 5G Information	
WLAN OP Mode	This is the device mode (Section 4.1.1 on page 25) to which the NBG6604'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 NBG6604 in the 5GHz wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the NBG6604 is using.
Firewall	This shows whether the firewall is enabled or not.
System Status	
System Up Time	This is the total time the NBG6604 has been on.
Current Date/Time	This field displays your NBG6604's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG6604's processing ability is currently used. When this percentage is close to 100%, the NBG6604 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 NBG6604 is using.
Interface Status	
Interface	This displays the NBG6604 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.

5.2.1 Navigation Panel

Use the sub-menus on the navigation panel to go to Web Configurator screens.

Figure 18   Navigation Panel: Router Mode
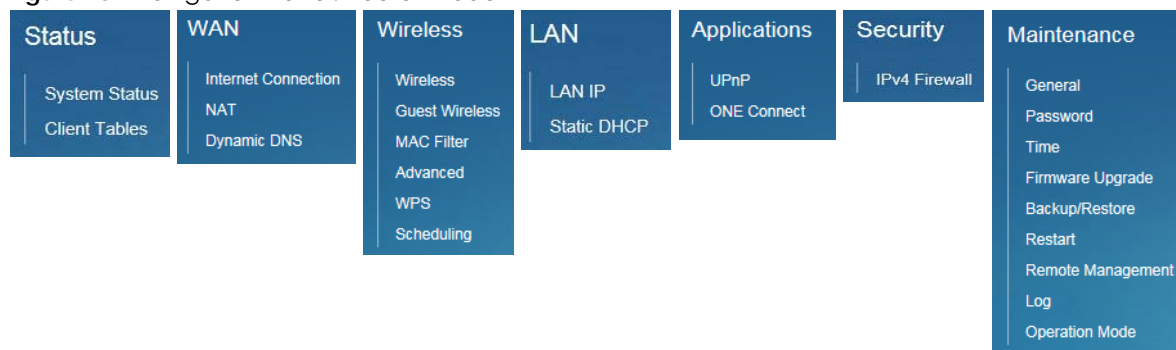
The following table describes the sub-menus.

Table 10   Navigation Panel: Router Mode

LINK	FUNCTION
Status	
System Status	This screen shows the NBG6604's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Client Tables	Use this screen to view current DHCP client information.
WAN	
Internet Connection	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address.
NAT	Use this screen to enable NAT.
	Use this screen to configure servers behind the NBG6604 and forward incoming service requests to the server(s) on your local network.
	Use this screen to change your NBG6604's port triggering settings.
	Use this screen to configure 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 NBG6604.
MAC Filter	Use the MAC filter screen to configure the NBG6604 to block access to devices or block the devices from accessing the NBG6604.
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 enable the NBG6604'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.
Applications	
UPnP	Use this screen to enable UPnP on the NBG6604.
One Connect	Use this screen to enable or disable Wi-Fi auto-configuration.
Security	

Table 10   Navigation Panel: Router Mode (continued)

LINK	FUNCTION
IPv4 Firewall	Use this screen to configure IPv4 firewall rules.
Maintenance	
General	Use this screen to view and change administrative settings such as system and domain names.
Password	Use this screen to change the password of your NBG6604.
Time	Use this screen to change your NBG6604's time and date.
Firmware Upgrade	Use this screen to upload firmware to your NBG6604.
Backup/Restore	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG6604.
Restart	This screen allows you to reboot the NBG6604 without turning the power off.
Remote Management	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 NBG6604.
Log	Use this screen to view the list of activities recorded by your NBG6604.
Operation Mode	This screen allows you to select whether your device acts as a router, or an access point.

Access Point Mode

6.1 Overview

Use your NBG6604 as an Access Point (AP) if you already have a router or gateway on your network. In this mode your NBG6604 bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

Figure 19 Wireless Internet Access in Access Point Mode
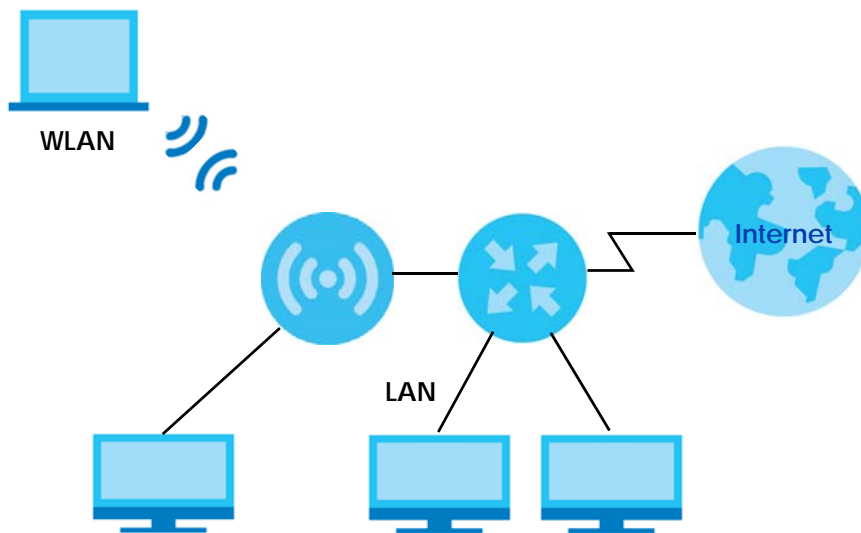
Many screens that are available in **Router Mode** are not available in **Access Point Mode**, such as firewall.

6.2 What You Can Do

- Use the **Status** screen to view read-only information about your NBG6604 (Section 6.4 on page 34).
- Use the **LAN** screen to set the IP address for your NBG6604 acting as an access point (Section 6.5 on page 36).

6.3 What You Need to Know

See Chapter 7 on page 38 for a tutorial on setting up a network with the NBG6604 as an access point.

6.3.1 Setting your NBG6604 to AP Mode

1 Log into the Web Configurator if you haven't already. See Section 2.2 on page 14 for how to do this.

2 To use your NBG6604 as an access point, go to **Maintenance** > **Operation Mode** and select **Access Point Mode**.

Figure 20 Changing to Access Point Mode
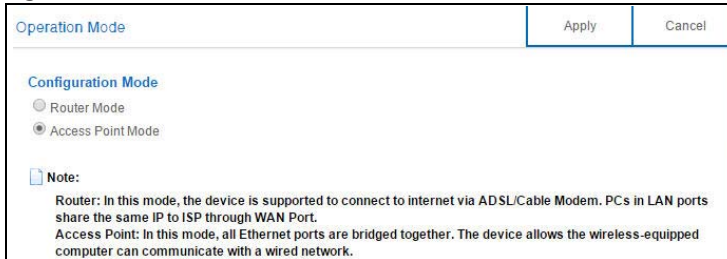
Note: You have to log in to the Web Configurator again when you change modes. As soon as you do, your NBG6604 is already in Access Point mode.

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

Figure 21 Pop up for Access Point Mode
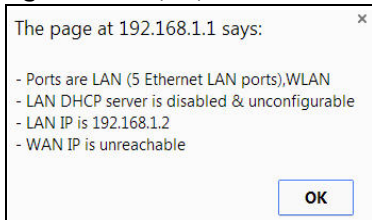
Click **OK**. Then click **Apply**. The Web Configurator refreshes once the change to Access Point mode is successful.

6.3.2 Accessing the Web Configurator in Access Point Mode

To log into the Web Configurator in Access Point mode, do the following:

1 Connect your computer to the LAN port of the NBG6604.

2 The default IP address of the NBG6604 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 your computer's help for information on changing your computer's IP address.

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

6.3.3 Configuring your WLAN and Maintenance Settings

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

- See Chapter 10 on page 63 for information on the configuring your wireless network.
- See Chapter 14 on page 91 for information on configuring your maintenance settings.

6.4 AP Mode Status Screen

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

Figure 22   Status > System Status: Access Point Mode
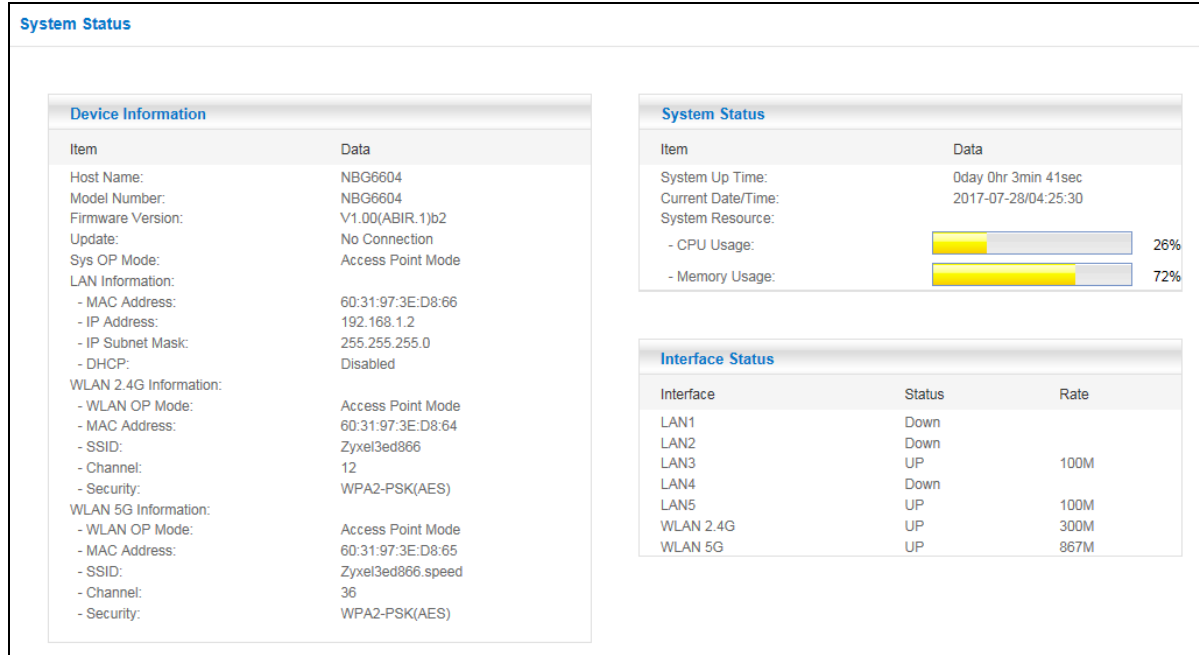
The following table describes the labels shown in the **Status** screen.

Table 11   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 and the date created.
Sys OP Mode	This is the device mode (Section 4.1.1 on page 25) to which the NBG6604 is set - **AP Mode**.
LAN Information	
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
DHCP	This shows the LAN port's DHCP role - **Client** or **None**.
WLAN 2.4G Information	
WLAN OP Mode	This is the device mode (Section 4.1.1 on page 25) to which the NBG6604'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 NBG6604 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 NBG6604 is using.

Table 11   Status > System Status: Access Point Mode (continued)

LABEL	DESCRIPTION
WLAN 5G Information	
WLAN OP Mode	This is the device mode (Section 4.1.1 on page 25) to which the NBG6604'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 NBG6604 in the 5GHz wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the NBG6604 is using.
System Status	
Item	This column shows the type of data the NBG6604 is recording.
Data	This column shows the actual data recorded by the NBG6604.
System Up Time	This is the total time the NBG6604 has been on.
Current Date/Time	This field displays your NBG6604's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG6604's processing ability is currently used. When this percentage is close to 100%, the NBG6604 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 NBG6604 is using.
Interface Status	
Interface	This displays the NBG6604 port types. The port types are: **LAN** and **WLAN**.
Status	For the LAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the 2.4GHz/5GHz WLAN, it displays **Up** when the 2.4GHz/5GHz WLAN is enabled or **Down** when the 2.4G/5G WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or is left blank when the line is disconnected. For the 2.4GHz/5GHz WLAN, it displays the maximum transmission rate when the 2.4GHz/5GHz WLAN is enabled and **N/A** when the WLAN is disabled.

6.4.1 Navigation Panel

Use the menu in the navigation panel to configure NBG6604 features in **Access Point Mode**.

Figure 23   Navigation Panel: Access Point Mode

Refer to Table 10 on page 29 for descriptions of the labels shown in the navigation panel.

6.5 LAN Screen

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

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

Note: If you change the IP address of the NBG6604 in the screen below, you will need to log into the NBG6604 again using the new IP address.

Figure 24   LAN > LAN IP

The table below describes the labels in the screen.

Table 12   LAN > LAN IP

LABEL	DESCRIPTION
IP Address	
Obtain an IP Address Automatically	When you enable this, the NBG6604 gets its IP address from the network's DHCP server (for example, your ISP). Users connected to the NBG6604 can now access the network (i.e., the Internet if the IP address is given by the ISP).
	The Web Configurator may no longer be accessible unless you know the IP address assigned by the DHCP server to the NBG6604. You need to reset the NBG6604 to be able to access the Web Configurator again (see Section 14.7 on page 95 for details on how to reset the NBG6604).
	Also when you select this, you cannot enter an IP address for your NBG6604 in the field below.
Static IP Address	Click this if you want to specify the IP address of your NBG6604. 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 NBG6604 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 NBG6604.
Default Gateway	Enter a **Default Gateway**'s IP address (if your ISP or network administrator gave you one) in this field.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the NBG6604's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.
	Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**.
	Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes to the NBG6604.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

CHAPTER 7
Tutorials

7.1 Overview

This chapter provides tutorials for setting up your NBG6604.

- Set Up a Wireless Network Using WPS
- Connect to NBG6604 Wireless Network without WPS
- Using Guest SSIDs on the NBG6604

7.2 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 NBG6604 as the AP and NWD210N as the wireless client which connects to a notebook.

The wireless client must be a WPS-aware device. 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 7.2.1 on page 38. 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 NBG6604's interface. See Section 7.2.2 on page 39. This is the more secure method, since one device can authenticate the other.

7.2.1 Push Button Configuration (PBC)

1 Make sure that your NBG6604 is turned on. and that the device is placed within range of your notebook.

2 Make sure that you have installed the wireless client (this example uses the NWD210N) driver and utility in your notebook.

3 In the wireless client utility, find the WPS settings. Enable WPS and press the WPS button (**Start** or **WPS** button)

4 Log into NBG6604's Web Configurator and press the **Push Button** in the **Wireless > WPS** screen.

Note: Your NBG6604 has a WPS button located on its top 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 NBG6604 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 NBG6604 securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both NBG6604 and wireless client (the NWD210N in this example).

Figure 25 Example WPS Process: PBC Method
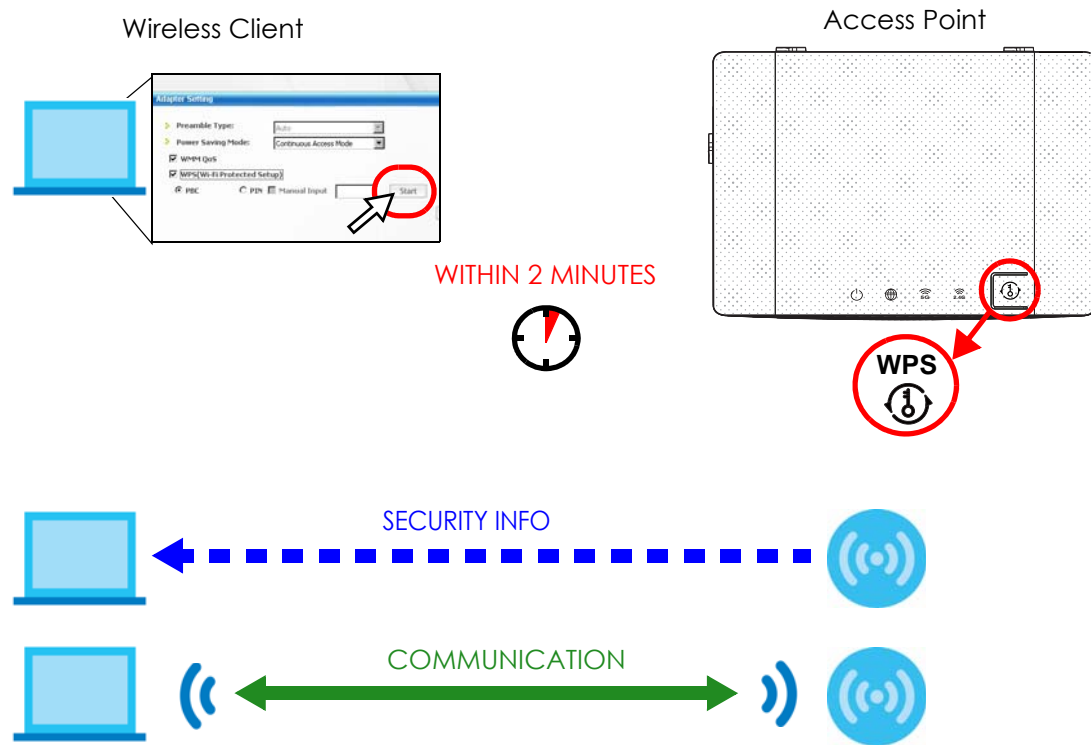
7.2.2 PIN Configuration

When you use the PIN configuration method, you need to use both NBG6604'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 **Wireless > WPS** screen on the NBG6604.

3 Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the NBG6604's **WPS** screen within two minutes.

The NBG6604 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 NBG6604 securely.

The following figure shows you the example to set up wireless network and security on NBG6604 and wireless client (ex. NWD210N in this example) by using PIN method.

Figure 26 Example WPS Process: PIN Method

Wireless Client

Access Point

WITHIN 2 MINUTES
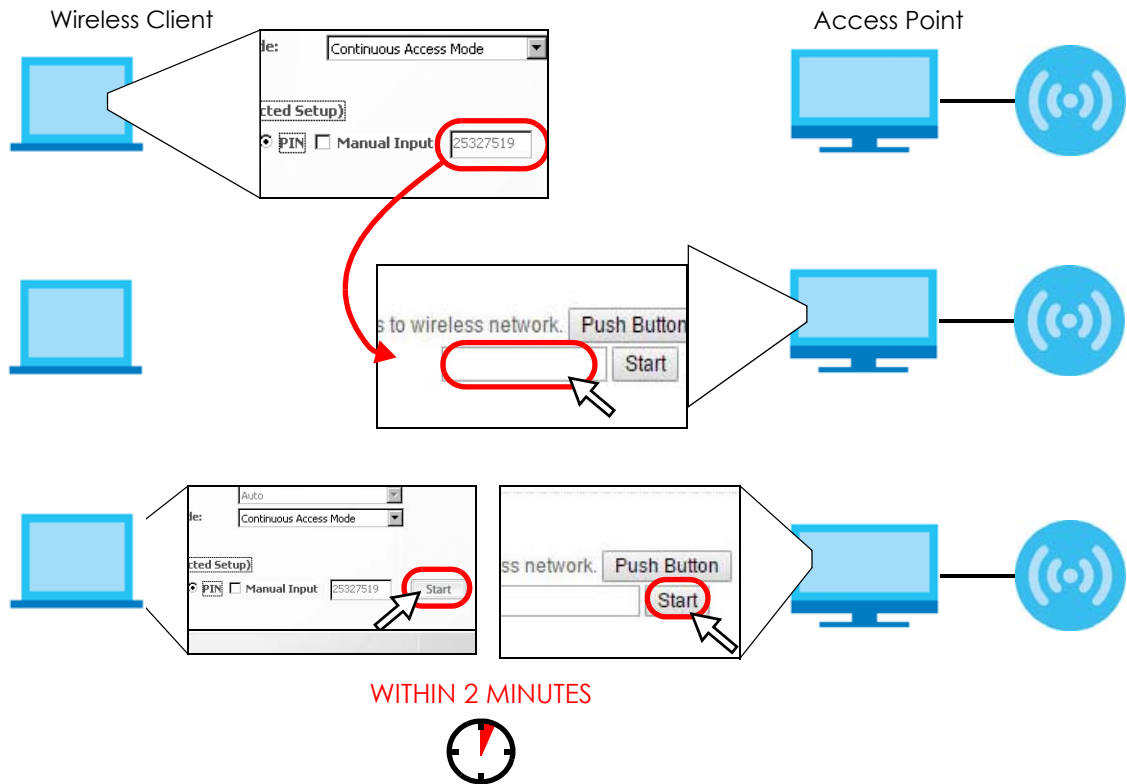
7.3 Connect to NBG6604 Wireless Network without WPS
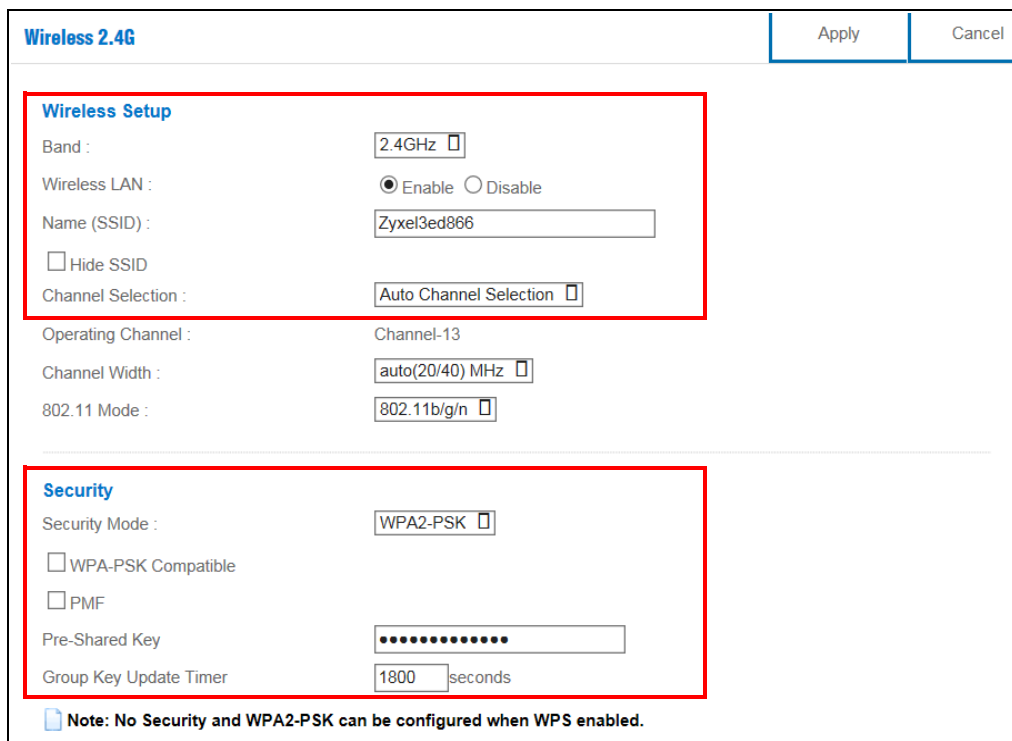
This example shows you how to configure wireless security settings with the following parameters on your NBG6604 and connect your computer to the NBG6604 wireless network.

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 NBG6604.

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 14).

1 Make sure the **WIFI** switch (at the rear panel of the NBG6604) is set to **ON**.

2 Open the **Wireless** > **Wireless** screen in the AP's Web Configurator.

3 Confirm that the wireless LAN is enabled on the NBG6604.

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) :	Zyxel3ed866		
☐ Hide SSID			
Channel Selection :	Auto Channel Selection		
Operating Channel :	Channel-13		
Channel Width :	auto(20/40) MHz		
802.11 Mode :	802.11b/g/n		
Security			
Security Mode :	WPA2-PSK		
☐ WPA-PSK Compatible			
☐ PMF			
Pre-Shared Key	••••••••••••		
Group Key Update Timer	1800 seconds		
🗋 Note: No Security and WPA2-PSK can be configured when WPS enabled.			

6 Click **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**.

7.3.1 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 NBG6604 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 The **Wireless Network Connection** screen displays. Click **Refresh network list** to view the available wireless APs within range.

4 Select **SSID_Example3** and click **Connect**.
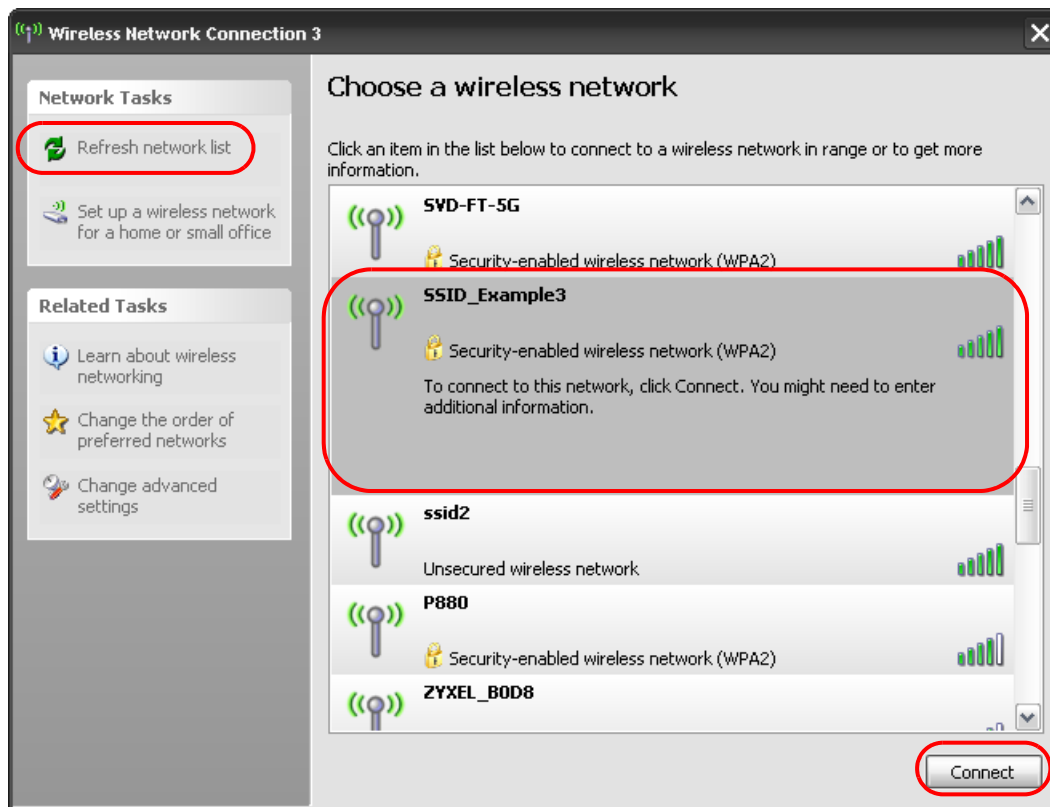
5 Type the security key in the following screen. Click **Connect**.

6 Check the status of your wireless connection in the screen below.
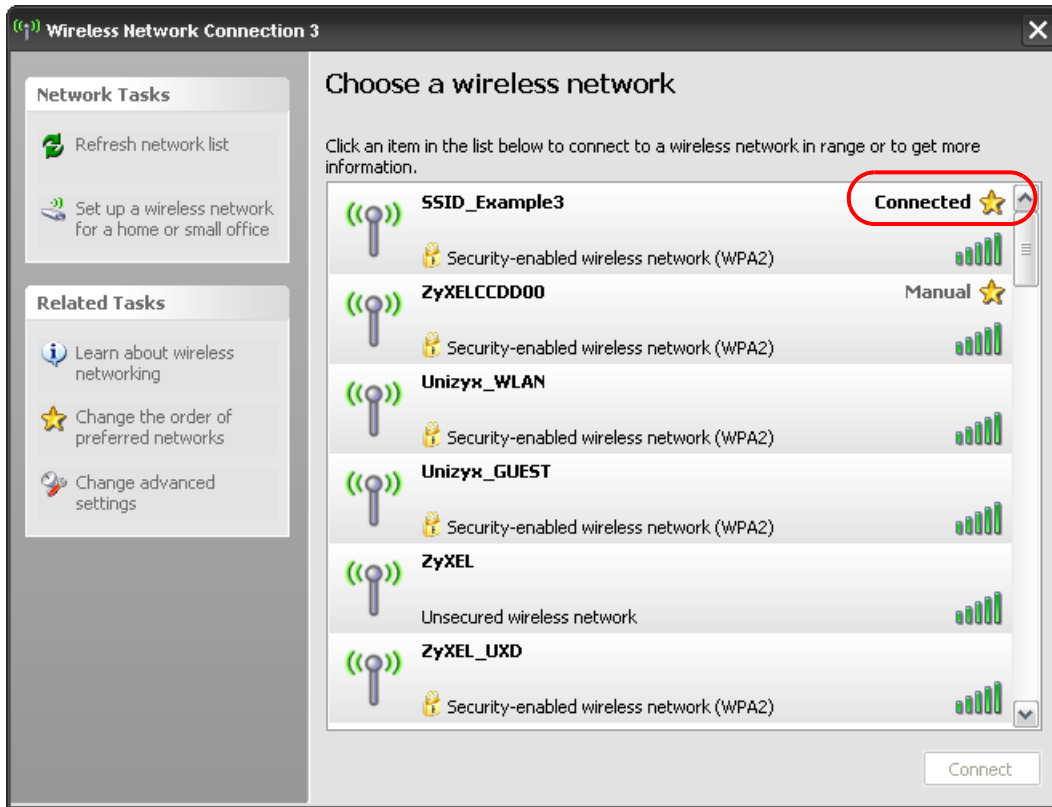
7 If the wireless client keeps trying to connect to or acquiring an IP address from the NBG6604, make sure you entered the correct security key.

If the connection has limited or no connectivity, make sure the DHCP server is enabled on the NBG6604.

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.

7.4 Using Guest SSIDs on the NBG6604

You can configure more than one guest SSID on a NBG6604. See Section 10.4 on page 72.

This allows you to configure multiple independent wireless networks on the NBG6604 as if there were multiple APs (virtual APs). Each guest SSID has its own wireless security type. That is, each SSID on the NBG6604 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 NBG6604 (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.
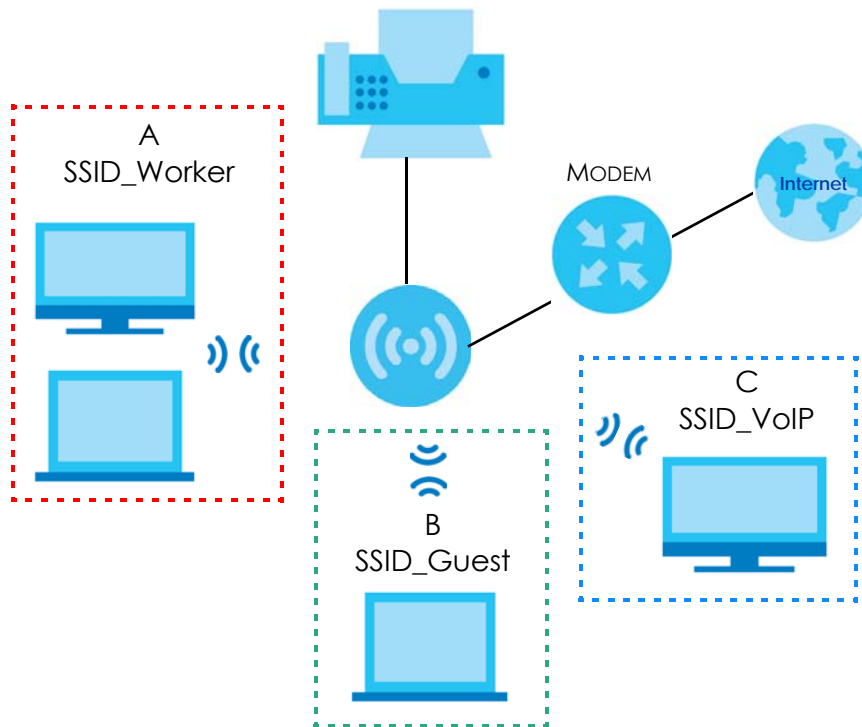
7.4.1 Configuring Security Settings of Guest SSIDs

The NBG6604 is in router mode by default.

This example shows you how to configure the SSIDs with the following parameters on your NBG6604 (in router mode).

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

Note: This tutorial assumes that you have disabled WPS in **Wireless > WPS**. Otherwise, the "WPA-PSK" security type is not available to configure.

1 Connect your computer to the LAN port of the NBG6604 using an Ethernet cable.

2 The default IP address of the NBG6604 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 your computer's help 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. Go to **Wireless > Guest Wireless**. Click the **Edit** icon of the first entry to configure wireless and security settings for **SSID_Worker**.

8 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**.

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

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

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

12 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**.

CHAPTER 8
Status

8.1 Overview

This chapter discusses read-only information related to the device state of the NBG6604.

8.1.1 What You Can Do

- Use the **Client Tables** screen to view the current DHCP client information ().

8.2 Client Tables Screen

You can configure the NBG6604's LAN as a DHCP server or disable it. When configured as a server, the NBG6604 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 current DHCP client information (including MAC Address, and IP Address) of all network clients using the NBG6604's DHCP server.

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

Figure 27   Status > Client Tables

Client Tables					Apply	Cancel
Interface : ALL						
DHCP Client Table						
#	Online	Host Name	IP Address	MAC Address	Interface/Rssi	Lease Time	Reserve
1	💡	TWPCMT03357-01	192.168.1.33	C0:3F:D5:F1:76:D9	LAN	2017-04-25 04:24	☐

The following table describes the labels in this screen.

Table 13   Status > Client Tables

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.

Table 13   Status > Client Tables

LABEL	DESCRIPTION
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 NBG6604.
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 NBG6604.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

9.1 Overview

This chapter discusses the NBG6604's **WAN** screens. Use these screens to configure your NBG6604 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 28 LAN and WAN
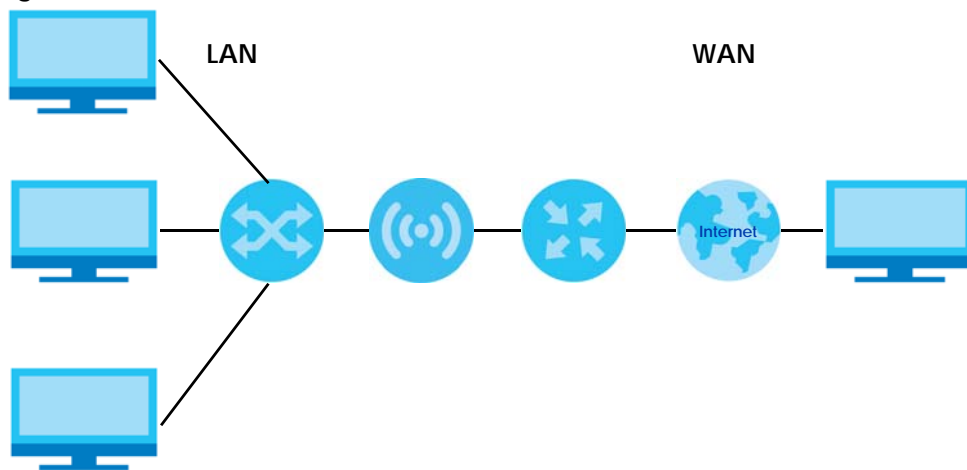
9.2 What You Can Do

- Use the **Internet Connection** screen to enter your ISP information and set how the computer acquires its IP, DNS and WAN MAC addresses (Section 9.4 on page 53).
- Use the **NAT > General** screen to enable NAT, set a default server and change your NBG6604's port forwarding settings (Section 9.5.1 on page 58).
- Use the **NAT > Port Trigger** screen to configure your NBG6604's trigger port settings (Section 9.5.2 on page 59).
- Use the **NAT > Passthrough** screen to configure your NBG6604's VPN pass-through settings (Section 9.5.3 on page 60).
- Use the **Dynamic DNS** screen to change your NBG6604's DDNS settings (Section 9.6 on page 61).

9.3 What You Need To Know

The information in this section can help you configure the screens for your WAN connection, as well as enable/disable some advanced features of your NBG6604.

9.3.1 Configuring Your Internet Connection

Encapsulation Method

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

WAN IP Address

The WAN IP address is an IP address for the NBG6604, which makes it accessible from an outside network. It is used by the NBG6604 to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the NBG6604 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 NBG6604 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 NBG6604'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 29   Multicast Example

A

B

C

D
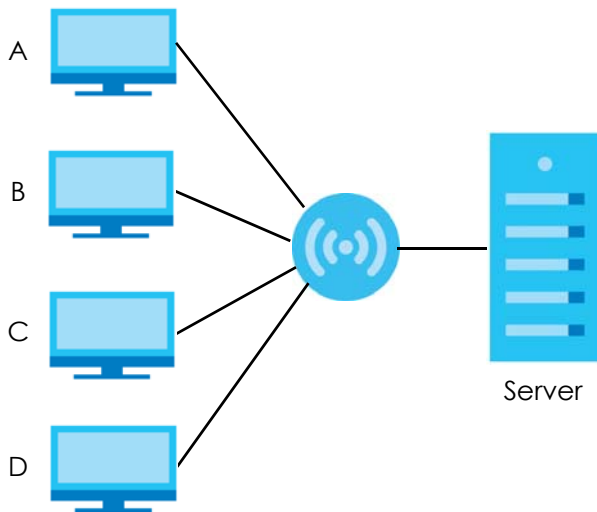
Server

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 NBG6604 supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**).

At start up, the NBG6604 queries all directly connected networks to gather group membership. After that, the NBG6604 periodically updates this information. IP multicasting can be enabled/disabled on the NBG6604 WAN interface in the Web Configurator (**WAN**). Select **None** to disable IP multicasting on these interfaces.

Auto-IP Change

When the NBG6604 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 NBG6604 to change its LAN IP address to 10.0.0.1 automatically. If the NBG6604'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 NBG6604 switches to use 192.168.1.1 as its LAN IP address.

Figure 30   Auto-IP-Change Example
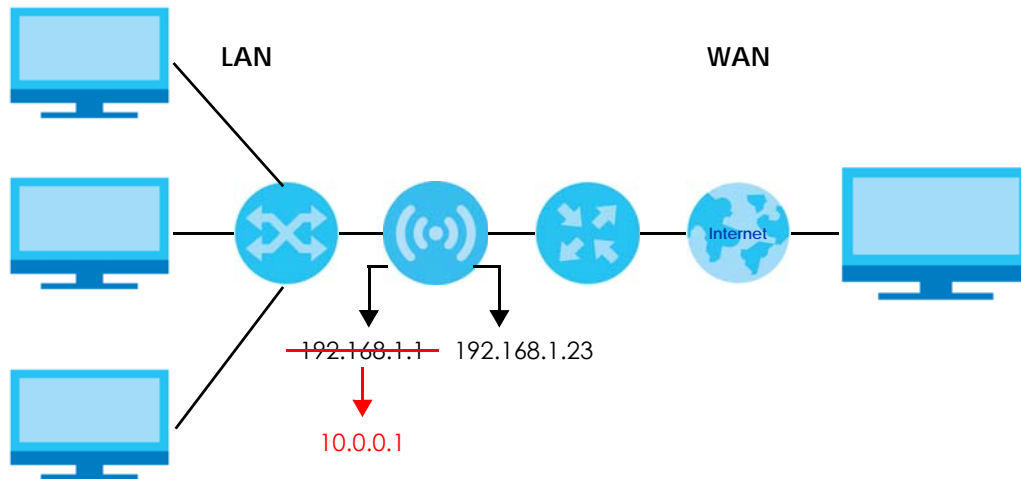
Auto-IP-Change only works under the following conditions:

- The NBG6604 must be in **Router Mode** (see Section 14.11 on page 98 for more information) for Auto-IP-Change to become active.
- The NBG6604 is set to receive a dynamic WAN IP address.

9.4 Internet Connection Screen

Use this screen to change your NBG6604's Internet access settings. Click **WAN** > **Internet Connection**.

9.4.1 IPoE Encapsulation

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

Figure 31   WAN > Internet Connection: IPoE Encapsulation (IPv4 Only)

The following table describes the labels in this screen.

Table 14   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	Select **IPv4 Only** if you want the NBG6604 to run IPv4 only. Select **Dual Stack** to allow the NBG6604 to run IPv4.
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 NBG6604 divides it into smaller fragments.
DNS Server	

Table 14   Network > WAN > Internet Connection: IPoE Encapsulation (continued)

LABEL	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the NBG6604'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 NBG6604 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.
Automatically configured by DHCPC	Select this to have the NBG6604 detect the relay server's IP address automatically through DHCP.
Manually Configured	Select this if you have the IPv4 address of the relay server.
IPv4 mask length	Enter the subnet mask number (1~32) for the IPv4 network.
Remote IPv4 Address	Enter the IPv4 address of the remote gateway to which this interface tunnels traffic.
Auto-Subnet Configuration	
Enable Auto-IP-Change Mode	Select this option to have the NBG6604 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG6604 gets a dynamic WAN IP address in the same subnet as the LAN IP address. Select this option to have the NBG6604 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG6604 gets a DNS server IP address in the same subnet as the LAN IP address. The NAT, DHCP server and firewall functions on the NBG6604 are still available in this mode.
Apply	Click **Apply** to save your changes back to the NBG6604.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.4.2 PPPoE Encapsulation

The NBG6604 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 NBG6604 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG6604 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 32   Network > WAN > Internet Connection: PPPoE Encapsulation (IPv4 Only)

The following table describes the labels in this screen.

Table 15   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	Select **IPv4 Only** if you want the NBG6604 to run IPv4 only.
	Select **Dual Stack** to allow the NBG6604 to run IPv4.
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 NBG6604 can receive and process.
PPP Auto Connect	Select this option if you do not want the connection to time out.

Table 15   Network > WAN > Internet Connection: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
IDLE Timeout (second)	This value specifies the time in minutes that elapses before the router automatically disconnects from the PPPoE server.
PPPoE Service Name	Enter the PPPoE service name specified in the ISP account.
WAN IP Address Assignment	
Get automatically from ISP	Select this option if your ISP did not assign you a fixed IP address. This is the default selection.
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 Second DNS Server Third DNS Server	Select **Obtained From ISP** if your ISP dynamically assigns DNS server information (and the NBG6604'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 The MAC address section allows users to configure the WAN port's MAC address by using the NBG6604'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.
Automatically configured by DHCPC	Select this to have the NBG6604 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.
IPv4 mask length	Enter the subnet mask number (1~32) for the IPv4 network.
Remote IPv4 Address	Enter the IPv4 address of the remote gateway to which this interface tunnels traffic.
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	

Table 15   Network > WAN > Internet Connection: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
Enable Auto-IP-Change Mode	Select this option to have the NBG6604 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG6604 gets a dynamic WAN IP address in the same subnet as the LAN IP address.
	Select this option to have the NBG6604 change its LAN IP address to 10.0.0.1 or 192.168.1.1 accordingly when the NBG6604 gets a DNS server IP address in the same subnet as the LAN IP address.
	The NAT, DHCP server and firewall functions on the NBG6604 are still available in this mode.
Apply	Click **Apply** to save your changes back to the NBG6604.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.5 NAT

Use this screen to change your NBG6604's NAT (Network Address Translation) settings. Click **WAN** > **NAT**.

9.5.1 General Screen

Use this screen to enable NAT, set a default server and configure your NBG6604's port forwarding settings to forward incoming service requests to the server(s) on your local network. Click **WAN** > **NAT** > **General**.

Figure 33   WAN > NAT > General

The following table describes the labels in this screen.

Table 16   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	

Table 16   WAN > NAT > General (continued)
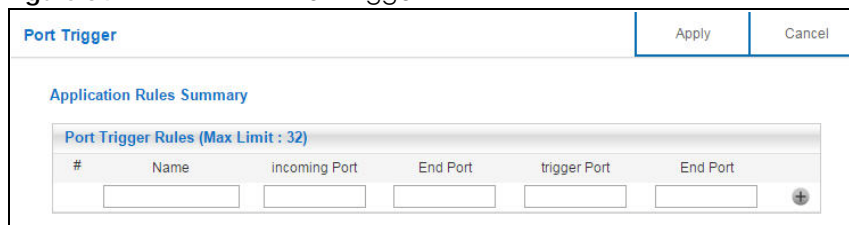
LABEL	DESCRIPTION
Default Server	You can decide whether you want to use the default server or specify a server manually. In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in the port forwarding summary table below. Select this to use the default server.
Change To Server	Select this and manually enter the server's IP address.
Port Forwarding (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(s) 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.
Local 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.
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.
Name	This field displays a name to identify this rule.
Protocol	This is the transport layer protocol used for the service.
Local Port	This field displays the port number(s).
Server IP Address	This field displays the inside IP address of the server.
Port	This field displays the port number(s).
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 NBG6604.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.5.2 Port Trigger Screen

To change your NBG6604's trigger port settings, click **WAN > NAT > Port Trigger**. The screen appears as shown.

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

Figure 34   WAN > NAT > Port Trigger

The following table describes the labels in this screen.

Table 17   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 NBG6604 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 NBG6604 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 NBG6604.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.5.3 Passthrough Screen

ALG Overview

Application Layer Gateway (ALG) allows VPN traffic to operate properly through the NBG6604's NAT.

The ALG feature is only needed for traffic that goes through the NBG6604's NAT.

To change your NBG6604's VPN pass-through settings, click **WAN > NAT > Passthrough**. The screen appears as shown.

Figure 35   WAN > NAT > Passthrough

The following table describes the labels in this screen.

Table 18   WAN > NAT > Passthrough

LABEL	DESCRIPTION
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 NBG6604 and the NBG6604 will drop the request. When **PPTP** is enabled, the NBG6604 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 NBG6604 and the NBG6604 will drop the request. When **L2TP** is enabled, the NBG6604 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 NBG6604 and the NBG6604 will drop the request. When **IPSEC** is enabled, the NBG6604 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 NBG6604.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.6 Dynamic DNS Screen

To change your NBG6604's DDNS, click **WAN** > **Dynamic DNS**. The screen appears as shown.

Figure 36   WAN > Dynamic DNS

The following table describes the labels in this screen.

Table 19   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.

Table 19   WAN > Dynamic DNS (continued)

LABEL	DESCRIPTION
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 NBG6604.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 10
Wireless LAN

10.1 Overview

This chapter discusses how to configure the wireless network settings in your NBG6604. The NBG6604 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 **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 37   Example of a Wireless Network
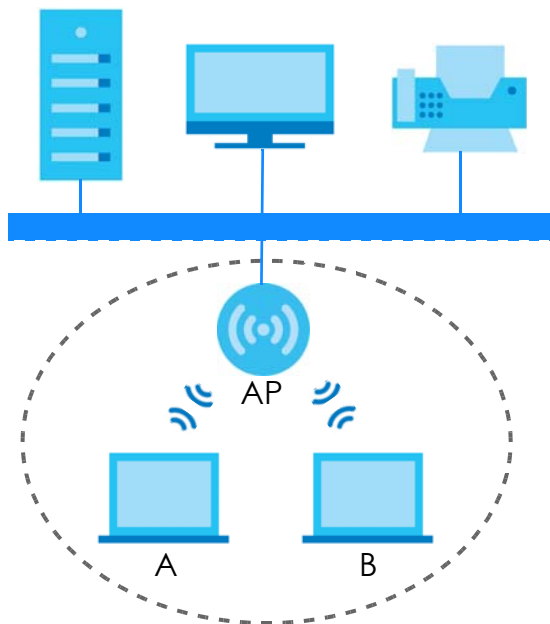
The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the Access Point (AP) to interact with other devices (such as the printer) or with the Internet. Your NBG6604 is the AP.

10.1.1 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 NBG6604 and the wireless clients, and make other basic configuration changes (Section 10.2 on page 68).
- Use the **Guest Wireless** screen to set up multiple wireless networks on your NBG6604 (Section 10.4 on page 72).
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the NBG6604 (Section 10.5 on page 74).
- Use the **Advanced** screen to allow intra-BSS networking and set the RTS/CTS Threshold (Section 10.6 on page 75).
- Use the **WPS** screen to quickly set up a wireless network with strong security, without having to configure security settings manually (Section 10.7 on page 77).
- Use the **Scheduling** screen to set the times your wireless LAN is turned on and off (Section 10.8 on page 78).

10.1.2 What You Should Know

Every wireless network must follow these basic guidelines.

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

  The SSID is the name of the wireless network. It stands for Service Set IDentity.

- If two wireless networks overlap, they should use different channels.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every wireless client in the same wireless network must use security compatible with the AP.

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

Wireless Security Overview

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

SSID

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

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

MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

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

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

User Authentication

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

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

• In the AP: this feature is called a local user database or a local database.

• In a RADIUS server: this is a server used in businesses more than in homes.

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

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

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

Encryption

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

---

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

The types of encryption you can choose depend on the type of user authentication. (See page 65 for information about this.)

Table 20   Types of Encryption for Each Type of Authentication

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

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

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

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

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

When you select **WPA2** or **WPA2-PSK** in your NBG6604, 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 NBG6604.

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 NBG6604 (**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 38   Guest Wireless LAN Network
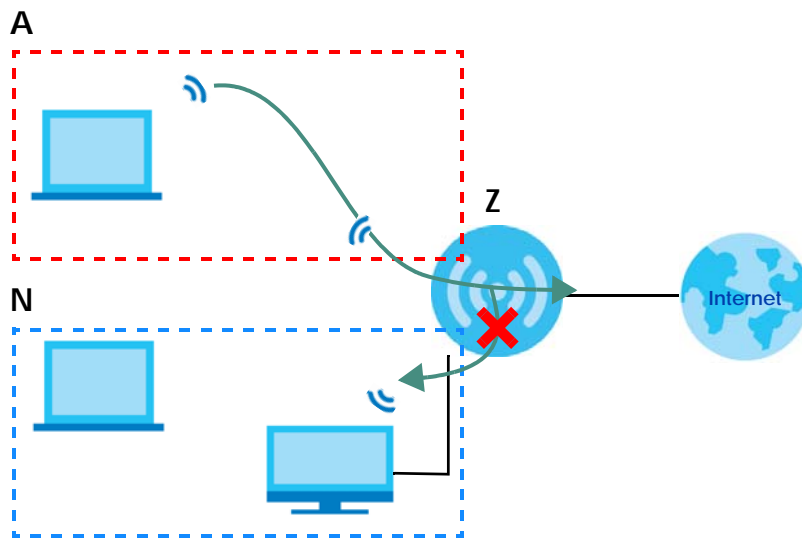
Guest WLAN Bandwidth

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 39   Example: Bandwidth for Different Networks

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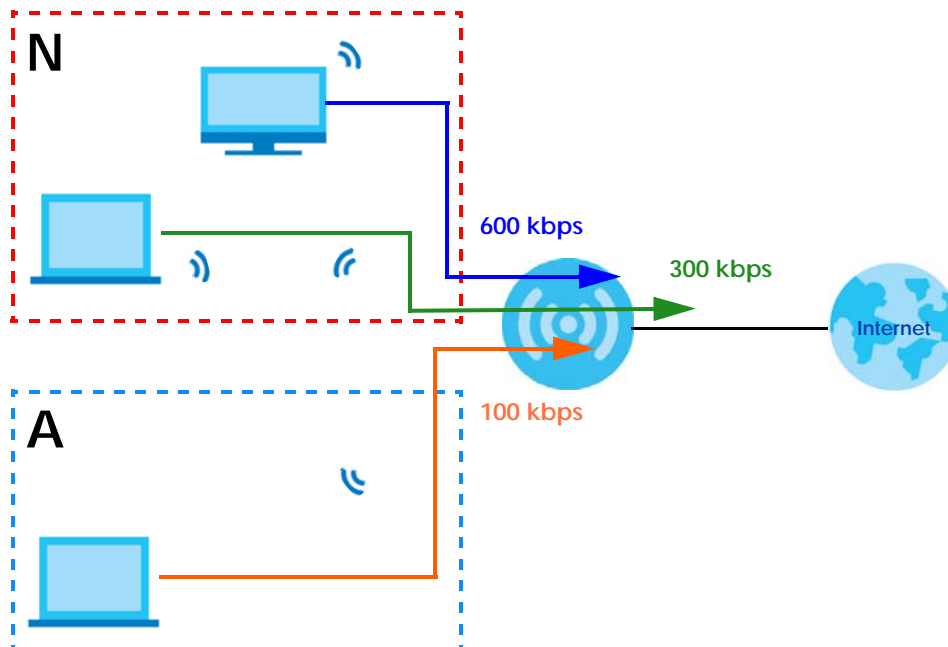
WiFi Protected Setup (WPS) is an industry standard specification, defined by the WiFi Alliance. WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Depending on the devices in your network, you can either press a button (on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

10.2 Wireless Screen

Use this screen to configure the SSID and wireless security of the NBG6604's default wireless LAN.

Note: If you are configuring the NBG6604 from a computer connected to the wireless LAN and you change the NBG6604'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 NBG6604's new settings.

Click **Wireless**.

Figure 40   Wireless

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

Table 21   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.

Table 21   Wireless (continued)

LABEL	DESCRIPTION
Wireless LAN	Select **Enable** to activate the 2.4GHz and/or 5GHz wireless LAN. Select **Disable** to turn it off.
Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. This option is only available if **Auto Channel Selection** is disabled.
Operating Channel	This displays the channel the NBG6604 is currently using.
Channel Width	Select the wireless channel width used by NBG6604. 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). Because not all devices support 40 MHz channels, select **Auto 20/40MHz** to allow the NBG6604 to adjust the channel bandwidth automatically. **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. 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.
802.11 Mode	If you set **Band** to **2.4GHz**, you can select from the following: • **802.11b**: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the NBG6604. 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 NBG6604 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 NBG6604. The NBG6604 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 NBG6604. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the NBG6604. • **802.11gn**: allows either IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the NBG6604. The transmission rate of your NBG6604 might be reduced. • **802.11 bgn**: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the NBG6604. The transmission rate of your NBG6604 might be reduced. If you set **Band** to **5GHz**, you can select from the following: • **802.11a**: allows only IEEE 802.11a compliant WLAN devices to associate with the NBG6604. • **802.11a/an**: allows both IEEE802.11n and IEEE802.11a compliant WLAN devices to associate with the NBG6604. The transmission rate of your NBG6604 might be reduced. • **802.11a/an/ac**: allows IEEE802.11n, IEEE802.11a and IEEE 802.11ac compliant WLAN devices to associate with the NBG6604.
Security	

Table 21   Wireless (continued)

LABEL	DESCRIPTION
Security Mode	Select **WPA2-PSK** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See Section 10.3 on page 70 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.
WPA-PSK Compatible	This field appears when you choose **WPA2-PSK** as the **Security Mode**. Select this to allow wireless devices using **WPA-PSK** security mode to connect to your NBG6604.
PMF	Protected Management Frames (PMF) is a protection mechanism of action management frames. Select this to allow wireless devices using the PMF protection mechanism to connect to your NBG6604.
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 NBG6604.
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.

10.3 Wireless Security

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

10.3.1 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 NBG6604, your network is accessible to any wireless networking device that is within range.

Figure 41   Wireless > Security Mode: No Security

The following table describes the labels in this screen.

Table 22   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 NBG6604.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.3.2 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 **Wireless > Wireless** screen.

Figure 42   Wireless > Security Mode: WPA-PSK/WPA2-PSK

The following table describes the labels in this screen.

Table 23   Wireless > Security Mode: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Security Mode	Select **WPA-PSK** or **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 NBG6604.
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 NBG6604.
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 NBG6604.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.4 Guest Wireless Screen

This screen allows you to enable and configure multiple guest wireless network settings on the NBG6604.

You can configure up to four SSIDs to enable multiple BSSs (Basic Service Sets) on the NBG6604. 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 **Wireless > Guest Wireless**. The following screen displays.

Figure 43 Wireless > Guest Wireless

The following table describes the labels in this screen.

Table 24   Wireless > Guest Wireless

LABEL	DESCRIPTION
Band	Use **2.4GHz** or **5GHz** to set up the NBG6604'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 NBG6604'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 the **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 NBG6604 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.

10.4.1 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 44 Wireless > Guest Wireless > Guest Wireless Setup: Edit

The following table describes the labels in this screen.

Table 25 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 NBG6604 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.
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 10.3 on page 70 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 NBG6604.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.5 MAC Filter Screen

The MAC filter screen allows you to configure the NBG6604 to give exclusive access to devices (**Allow**) or exclude devices from accessing the NBG6604 (**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 NBG6604's MAC filter settings, click **Wireless > MAC Filter**. The screen appears as shown.

Figure 45   Wireless > MAC Filter

The following table describes the labels in this menu.

Table 26   Wireless > MAC Filter

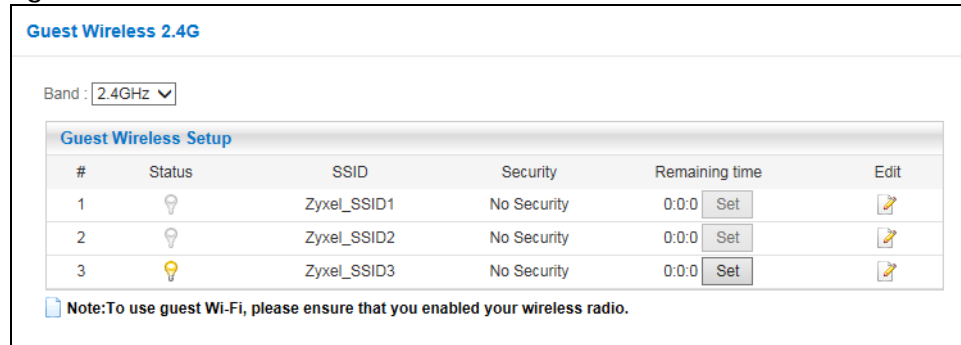| LABEL	DESCRIPTION
Band	Select the frequency band to set whether you want to apply the wireless and security settings to the default **2.4GHz** or **5GHz** wireless LAN.
SSID Select	This shows the SSID for which you are configuring MAC filtering.
MAC Address Filter	Select to turn on (**Enable**) or 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 NBG6604, MAC addresses not listed will be denied access to the NBG6604.
	Select **Deny** to block access to the NBG6604, MAC addresses not listed will be allowed to access the NBG6604.
MAC Filter Summary (Maximum: 16)	
#	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 NBG6604. 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 NBG6604.
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.
Apply	Click **Apply** to save your changes back to the NBG6604.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.6 Advanced Screen

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

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

Figure 46   Wireless > Advanced

The following table describes the labels in this screen.

Table 27   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 NBG6604 automatically changes to use the maximum value if you select **802.11n**, **802.11an**, **802.11gn**, or **802.11bgn** in the **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 NBG6604 automatically changes to use the maximum value if you select **802.11n**, **802.11an**, **802.11gn**, or **802.11bgn** in the **Wireless** screen.
Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).
	Intra-BSS traffic is traffic between wireless clients in the BSS. When 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.
Tx Power	Set the output power of the NBG6604 in this field. If there is a high density of APs in an area, decrease the output power of the NBG6604 to reduce interference with other APs. Select one of the following **100%**, **90%**, **75%**, **50%**, **25%**, or **10%**.
QoS Setup	
WMM QoS	Select **Enable** to have the NBG6604 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.
	This field is not configurable and the NBG6604 automatically enables WMM QoS if you select **802.11n**, **802.11an**, **802.11gn**, or **802.11bgn** in the **Wireless** screen.

Table 27   Wireless > Advanced (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NBG6604.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.7 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 **Wireless > WPS**.

Note: With WPS, wireless clients can only connect to the wireless network using the first SSID on the NBG6604.

Figure 47   Wireless > WPS

The following table describes the labels in this screen.

Table 28   Wireless > WPS

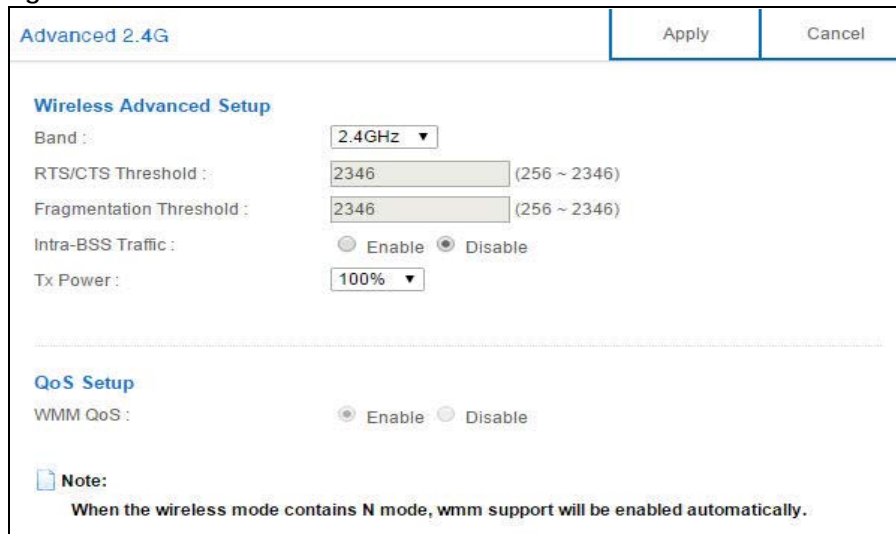| LABEL	DESCRIPTION
WPS Setup	
Band	Select the frequency band to set whether you want to apply the wireless and security settings to the default **2.4GHz** or **5GHz** wireless LAN.
WPS	Select **Enable** to turn on the WPS feature. Otherwise, select **Disable**.
PIN Code	Select **Enable** and click **Apply** to allow the PIN Configuration method. If you select **Disable**, you cannot create a new PIN number.

Table 28   Wireless > WPS (continued)

LABEL	DESCRIPTION
PIN Number	This is the WPS PIN (Personal Identification Number) of the NBG6604. Enter this PIN in the configuration utility of the device you want to connect to the NBG6604 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.
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 NBG6604 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 NBG6604 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 NBG6604.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the NBG6604.
SSID	This is the name of the wireless network (the NBG6604'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 NBG6604.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

10.8 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 **Wireless > Scheduling**.

Figure 48   Wireless > Scheduling

The following table describes the labels in this screen.

Table 29   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 NBG6604.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

11.1 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 49   LAN Example
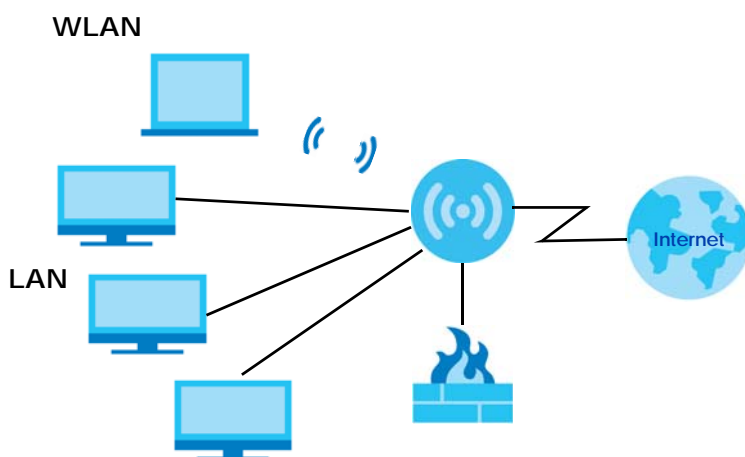
The LAN screens can help you configure a manage IP address, and partition your physical network into logical networks.

11.2 What You Can Do

- Use the **LAN IP** screen to configure the IPv4 address for your NBG6604 on the LAN (Section 11.4 on page 81).
- Use the **Static DHCP** screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses (Section 11.5 on page 82).

11.3 What You Need To Know

The actual physical connection determines whether the NBG6604 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 50   LAN and WAN IP Addresses
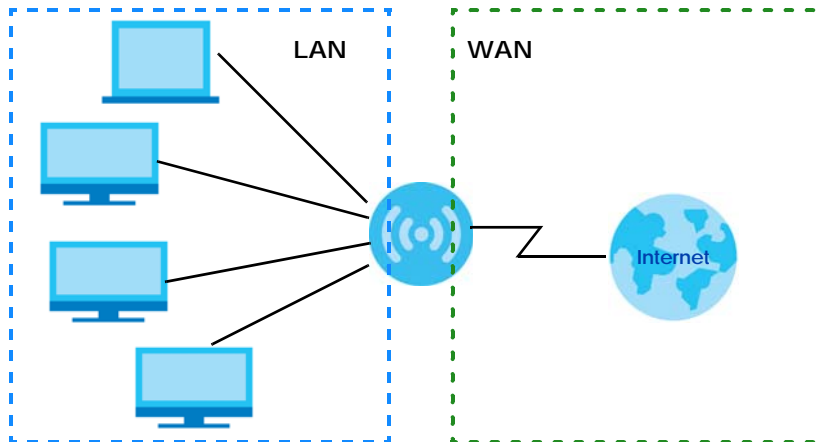
The LAN parameters of the NBG6604 are preset in the factory with the following values:

- IPv4 address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IPv4 addresses starting from 192.168.1.33.

These parameters should work for the majority of installations.

11.4 LAN IP Screen

Use this screen to change the IP address for your NBG6604. Click **LAN** > **LAN IP**.

Figure 51   LAN > LAN IP

The following table describes the labels in this screen.

Table 30   LAN > LAN IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your NBG6604 in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG6604 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 NBG6604.
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 NBG6604 acting as a DHCP server. When configured as a server, the NBG6604 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.
Lease Time	Specify for how many hours each DHCP client device can use the DHCP information (especially the IP address) before it has to request the information again.
Apply	Click **Apply** to save your changes back to the NBG6604.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.5 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 NBG6604's static DHCP settings, click **LAN > Static DHCP**.

Figure 52   LAN > Static DHCP

The following table describes the labels on this screen.

Table 31   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.

Table 31   LAN > Static DHCP (continued)

LABEL	DESCRIPTION
Add/Delete	Click ⊕ to add the rule in the MAC filter summary table. Click ⊖ to remove a rule.
Apply	Click **Apply** to save your changes with the NBG6604.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER **12**
Applications

12.1 Overview

This chapter shows you how to configure UPnP and One Connect.

12.1.1 What You Can Do

- Use the **UPnP** screen to enable UPnP on your NBG6604 (Section 12.2 on page 84).
- Use the **One Connect** screen to enable or disable Wi-Fi auto-configuration (Section 12.3 on page 85).
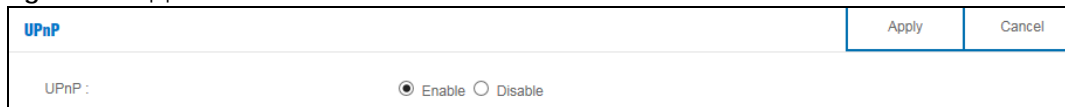
12.2 UPnP Screen

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 NBG6604.

Click **Applications** > **UPnP** to open the following screen.

Figure 53   Applications > UPnP

UPnP		Apply	Cancel
UPnP :	⦿ Enable ○ Disable		

The following table describes the fields in this screen.

Table 32   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 NBG6604's IP address (although you must still enter the password to access the web configurator).
Apply	Click **Apply** to save the setting to the NBG6604.
Cancel	Click **Cancel** to return to the previously saved settings.

12.3 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, NBG6604 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 NBG6604's web configurator. The mobile device with the App installed must be connected to the NBG6604 wirelessly.

Figure 54   Zyxel ONE Connect App

Use this screen to enable or disable Wi-Fi auto-configuration on the NBG6604.

Click **Applications** > **ONE Connect** to open the following screen.

Figure 55   Applications > ONE Connect

The following table describes the labels in this screen.

Table 33   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.
One Connect Compatible Devices	

Table 33   Applications > ONE Connect (continued)

LABEL	DESCRIPTION
Automatically Update AP/ Repeater Wi-Fi Settings	Select **Enable** to allow the NBG6604 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 NBG6604.
Cancel	Click **Cancel** to begin configuring this screen afresh.

12.4 Technical Reference

The following section contains additional technical information about the NBG6604 features described in this chapter.

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 NBG6604 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.

CHAPTER 13
Security

13.1 Overview

Use these screens to enable and configure the firewall that protects your NBG6604 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 56   Default Firewall Action
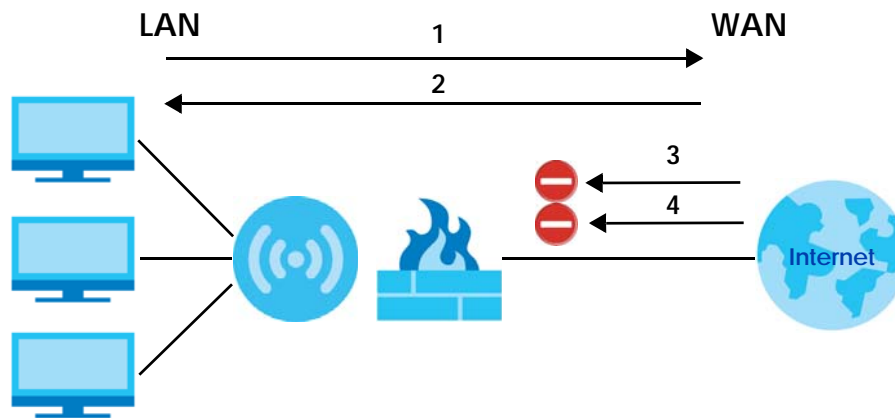
13.1.1 What You Can Do

- Use the **IPv4 Firewall** screen to enable or disable the NBG6604's IPv4 firewall ().

13.1.2 What You Need To Know

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

About the NBG6604 Firewall

The NBG6604'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** tab under **Security** and then click the **Enable Firewall** check box). The NBG6604's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG6604 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 NBG6604 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 NBG6604 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 Local Area Network (LAN) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

Guidelines For Enhancing Security With Your Firewall

1 Change the default password via Web Configurator.

2 Think about access control before you connect to the network in any way, including attaching a modem to the port.

3 Limit who can access your router.

4 Don't enable any local service (such as NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.

5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.

6 Protect against IP spoofing by making sure the firewall is active.

7 Keep the firewall in a secured (locked) room.

13.2 IPv4 Firewall Screen

Use this screen to enable or disable the NBG6604's IPv4 firewall, and set up firewall logs. Click **Security** > **IPv4 Firewall** to open the firewall setup screen.

Figure 57   Security > IPv4 Firewall

The following table describes the labels in this screen.

Table 34   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 NBG6604 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 NBG6604 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.
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 NBG6604 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 NBG6604 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	

Table 34   Security > IPv4 Firewall (continued)

LABEL	DESCRIPTION
#	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.
	Click to remove the firewall rule.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to start configuring this screen again.

CHAPTER 14
Maintenance

14.1 Overview

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

14.2 What You Can Do

- Use the **General** screen to set the timeout period of the management session (Section 14.3 on page 91).
- Use the **Password** screen to change your NBG6604's system password (Section 14.4 on page 92).
- Use the **Time** screen to change your NBG6604's time and date (Section 14.5 on page 93).
- Use the **Firmware Upgrade** screen to upload firmware to your NBG6604 (Section 14.6 on page 94).
- Use the **Backup/Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration (Section 14.7 on page 95).
- Use the **Restart** screen to reboot the NBG6604 without turning the power off (Section 14.8 on page 96).
- Use the **Remote Management** screen to configure the interface/s from which the NBG6604 can be managed remotely and specify a secure client that can manage the NBG6604. (Section 14.9.1 on page 97).
- Use the **Log** screen to see the logs for the activity on the NBG6604 (Section 14.10 on page 98).
- Use the **Operation Mode** screen to select how you want to use your NBG6604 (Section 14.12 on page 99).

14.3 General Screen

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

Figure 58   Maintenance > General

The following table describes the labels in this screen.

Table 35   Maintenance > General

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the NBG6604 in an Ethernet network.
Domain Name	Enter the domain name you want to give to the NBG6604.
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 NBG6604.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.4 Password Screen

It is strongly recommended that you change your NBG6604's password.

If you forget your NBG6604's password (or IP address), you will need to reset the device. See Section 14.8 on page 96 for details.

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

Figure 59   Maintenance > Password

The following table describes the labels in this screen.

Table 36   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.
Apply	Click **Apply** to save your changes back to the NBG6604.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.5 Time Screen

Use this screen to configure the NBG6604's time based on your local time zone. To change your NBG6604's time and date, click **Maintenance** > **Time**. The screen appears as shown.

Figure 60   Maintenance > Time

The following table describes the labels in this screen.

Table 37   Maintenance > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your NBG6604.
	Each time you reload this page, the NBG6604 synchronizes the time with the time server.
Current Date	This field displays the date of your NBG6604.
	Each time you reload this page, the NBG6604 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.
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 NBG6604 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).

Table 37   Maintenance > Time (continued)
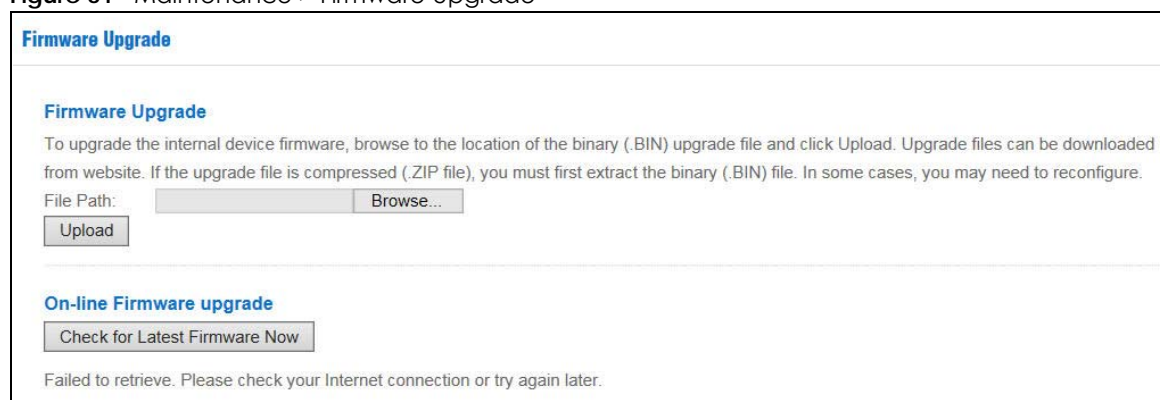
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NBG6604.
Cancel	Click **Cancel** to begin configuring this screen afresh.

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

Click **Maintenance** > **Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your NBG6604.

Figure 61   Maintenance > Firmware Upgrade

The following table describes the labels in this screen.

Table 38   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 NBG6604 while firmware upload is in progress!

After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the NBG6604 again.

The NBG6604 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 62   Network Temporarily Disconnected
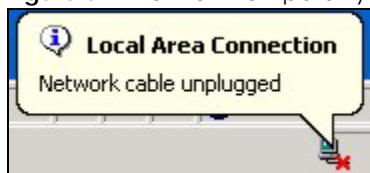
After two minutes, log in again and check your new firmware version in the **Status** screen.

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

14.7 Backup/Restore Screen

Backup configuration allows you to back up (save) the NBG6604's current configuration to a file on your computer. Once your NBG6604 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 NBG6604.

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

Figure 63   Maintenance > Backup/Restore

The following table describes the labels in this screen.

Table 39   Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup Configuration	
Backup	Click **Backup** to save the NBG6604's current configuration to your computer.
Restore Configuration	
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.
Upload	Click **Upload** to begin the upload process. Note: Do not turn off the NBG6604 while configuration file upload is in progress. After you see a "configuration upload successful" screen, you must then wait one minute before logging into the NBG6604 again. The NBG6604 automatically restarts in this time causing a temporary network disconnect. If you see an error screen, click **Back** to return to the Backup/Restore screen.
Back to Factory Defaults	
Reset	Pressing the **Reset** button in this section clears all user-entered configuration information and returns the NBG6604 to its factory defaults. You can also press the **RESET** button on the rear panel to reset the factory defaults of your NBG6604. Refer to the chapter about introducing the Web Configurator for more information on the **RESET** button.

Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default NBG6604 IP address (192.168.1.1). See your computer's help for details on how to set up your computer's IP address.

14.8 Restart Screen

System restart allows you to reboot the NBG6604 without turning the power off.

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

Figure 64   Maintenance > Restart

Click **Restart** to have the NBG6604 reboot. This does not affect the NBG6604's configuration.

14.9 Remote Management

Remote Management allows you to manage your NBG6604 from a remote location through the LAN/
WLAN or WAN interface.

14.9.1 Remote Access

Use this screen to change your NBG6604's remote management settings. You can use Telnet, HTTP or
HTTPS to access and manage the NBG6604.

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

Figure 65   Maintenance > Remote Management > Remote Access

The following table describes the labels in this screen.

Table 40   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 interfaces through which a computer may access the NBG6604 using this service.
Secured Client IP Address	Select **All** to allow all computes to access the NBG6604. Otherwise, check **Selected** and specify the IP address of the computer that can access the NBG6604.
Telnet	
Telnet	Select this to allow Telnet access.
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 NBG6604 using this service.

Table 40   Maintenance > Remote Management > WAN Access

LABEL	DESCRIPTION
Secured Client IP Address	Select **All** to allow all computes to access the NBG6604. Otherwise, check **Selected** and specify the IP address of the computer that can access the NBG6604.
Apply	Click **Apply** to save your changes back to the NBG6604.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.10 Log Screen

The Web Configurator allows you to look at all of the NBG6604'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 NBG6604. The log wraps around and deletes the old entries after it fills. Select the 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 66   Maintenance > Log

14.11 System Operation Mode Overview

The **Sys OP Mode** (System Operation Mode) function lets you configure your NBG6604 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 NBG6604.

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 67   LAN and WAN IP Addresses in Router Mode
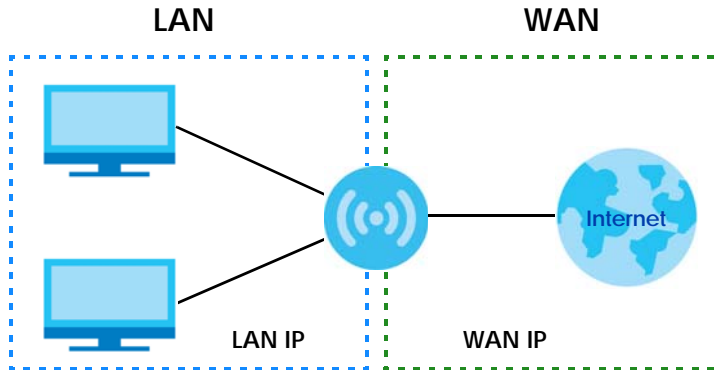
Access Point

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

Figure 68   Access Point Mode
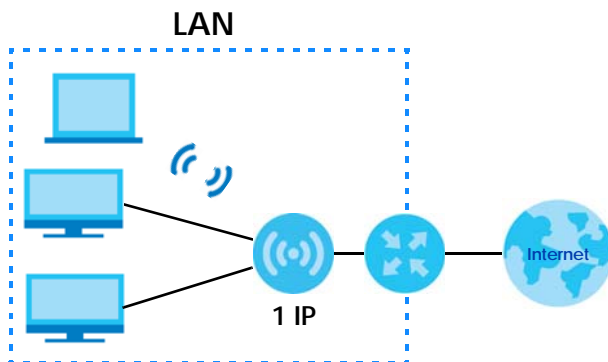
14.12 Operation Mode Screen

Use this screen to select how you want to use your NBG6604.

Figure 69 Maintenance > Operation Mode

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

Table 41   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. 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. • 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, remote management, firewall and so on) are not available when the NBG6604 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.

CHAPTER 15
Troubleshooting

15.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- NBG6604 Access and Login
- Internet Access
- Resetting the NBG6604 to Its Factory Defaults
- Wireless Connections

15.2 Power, Hardware Connections, and LEDs

The NBG6604 does not turn on. None of the LEDs turn on.

1   Make sure you are using the power adaptor or cord included with the NBG6604.

2   Make sure the power adaptor or cord is connected to the NBG6604 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 NBG6604.

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 10.

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 NBG6604.

5   If the problem continues, contact the vendor.

15.3 NBG6604 Access and Login

I don't know the IP address of my NBG6604.

6 The default IP address of the NBG6604 in **Router Mode** is **192.168.1.1**. If the NBG6604 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 52 for more information.
The default IP address of the NBG6604 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 NBG6604 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 NBG6604 (it depends on the network), so enter this IP address in your Internet browser.

8 If your NBG6604 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 NBG6604 to change all settings back to their default. This means your current settings are lost. See Section 15.5 on page 105 in the **Troubleshooting** for information on resetting your NBG6604.

I forgot the password.

1 The default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 15.5 on page 105.

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 NBG6604 in **Router Mode** is **192.168.1.1**. If the NBG6604 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 52 for more information.
The default IP address of the NBG6604 in **Access Point Mode** is **192.168.1.2**.

- If you changed the IP address (Section 11.4 on page 81), 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 NBG6604.

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.

5   Make sure your computer is in the same subnet as the NBG6604. (If you know that there are routers between your computer and the NBG6604, skip this step.)

   • If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 11.4 on page 81.

   • If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG6604. See Section 11.4 on page 81.

6   Reset the device to its factory defaults, and try to access the NBG6604 with the default IP address. See Section 1.5 on page 9.

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

Advanced Suggestions

   • Try to access the NBG6604 using another service, such as Telnet. If you can access the NBG6604, check the remote management settings and firewall rules to find out why the NBG6604 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 NBG6604.

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 NBG6604.

4   If this does not work, you have to reset the device to its factory defaults. See Section 15.5 on page 105.

15.4 Internet Access

I cannot access the Internet.

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

2   Go to **Maintenance > Operation Mode**. Check your System Operation Mode setting.

- If the NBG6604 is in **Router Mode**, make sure the WAN port is connected to a broadband modem or router with Internet access. Your computer and the NBG6604 should be in the same subnet.

    - If the NBG6604 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 NBG6604 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 NBG6604), 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 10.

2 Reboot the NBG6604.

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 10. If the NBG6604 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 NBG6604 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 NBG6604.

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

Advanced Suggestion

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

15.5 Resetting the NBG6604 to Its Factory Defaults

If you reset the NBG6604, you lose all of the changes you have made. The NBG6604 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 NBG6604:

1 Make sure the power LED is on.

2 Press the **RESET** button for one to four seconds to restart/reboot the NBG6604.

3 Press the **RESET** button for longer than five seconds to set the NBG6604 back to its factory-default configurations.

If the NBG6604 restarts automatically, wait for the NBG6604 to finish restarting, and log in to the Web Configurator. The password is "1234".

If the NBG6604 does not restart automatically, disconnect and reconnect the NBG6604's power. Then, follow the directions above again.

15.6 Wireless Connections

I cannot access the NBG6604 or ping any computer from the WLAN.

1 Make sure the wireless LAN is enabled on the NBG6604.

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 NBG6604.

4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG6604.

5 Check that both the NBG6604 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 NBG6604.

7 Make sure you allow the NBG6604 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 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".

See your computer's help 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.

APPENDIX A
Customer Support

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

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

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

Required Information

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

Corporate Headquarters (Worldwide)

Taiwan

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

Asia

China

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

India

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

Kazakhstan

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

Korea

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

Malaysia

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

Pakistan

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

Philippines

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

Singapore

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

Taiwan

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

Thailand

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

Vietnam

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

Europe

Belarus

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

Belgium

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

- https://www.zyxel.com/be/fr/

Bulgaria

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

Czech Republic

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

Denmark

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

Estonia

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

Finland

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

France

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

Germany

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

Hungary

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

Italy

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

Latvia

- Zyxel Latvia
- https://www.zyxel.com/lv/lv/

Lithuania

- Zyxel Lithuania
- https://www.zyxel.com/lt/lt/

Netherlands

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

Norway

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

Poland

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

Romania

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

Russia

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

Slovakia

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

Spain

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

Sweden

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

Switzerland

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

Turkey

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

UK

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

Ukraine

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

South America

Argentina

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

Brazil

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

Colombia

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

Ecuador

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

South America

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

Middle East

Israel

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

Middle East

- Zyxel Communications Corporation
- https://www.zyxel.com/me/en/

North America

USA

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

Oceania

Australia

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

Africa

South Africa

- Nology (Pty) Ltd.
- https://www.zyxel.com/za/en/

APPENDIX B
Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 42   Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.Zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.

Table 42   Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.

Table 42   Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

APPENDIX C
Legal Information

Copyright

Copyright © 2019 by Zyxel Communications Corporation.

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

Published by Zyxel Communications Corporation. All rights reserved.

Disclaimer

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

Regulatory Notice and Statement

UNITED STATES of AMERICA

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

FCC EMC Statement

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

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

    (2) This device must accept any interference received, including interference that may cause undesired operation.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.
- This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.
- If this device does cause harmful interference to radio or television reception, which is found by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
    - Reorient or relocate the receiving antenna
    - Increase the separation between the devices
    - Connect the equipment to an outlet other than the receiver's
    - Consult a dealer or an experienced radio/TV technician for assistance

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

FCC Radiation Exposure Statement

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

CANADA

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

Innovation, Science and Economic Development Canada ICES Statement

CAN ICES-3 (B)/NMB-3(B)

Industry Canada CS-03 Statement

- This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

- The Ringer Equivalence Number (REN) indicates the maximum number of devices allowed to be connected to a telephone interface. The termination of an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices not exceed five.

Déclaration de conformité
- Le présent produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada.
- L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de dispositifs qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme des IES de tous les dispositifs n'excède pas cinq.

Innovation, Science and Economic Development Canada RSS-GEN & RSS-247 statement

- This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
- This radio transmitter has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed, are strictly prohibited for use with this device.

If the product with 5G wireless function operating in 5150-5250 MHz and 5725-5850 MHz, the following attention must be paid,
- The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate; and
- Where applicable, antenna type(s), antenna model(s), and the worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in Section 6.2.2.3 of RSS 247 shall be clearly indicated.

If the product with 5G wireless function operating in 5250-5350 MHz and 5470-5725 MHz , the following attention must be paid.
- For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit.
- L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage; (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
- Le présent émetteur radio a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Lorsque la fonction sans fil 5G fonctionnant en 5150-5250 MHz and 5725-5850 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes
- Les dispositifs fonctionnant dans la bande de 5 150 à 5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée, selon le cas;
- Lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3 du CNR-247, doivent être clairement indiqués.

Lorsque la fonction sans fil 5G fonctionnant en 5250-5350 MHz et 5470-5725 MHz est activée pour ce produit , il est nécessaire de porter une attention particulière aux choses suivantes.
- Pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e.

Industry Canada radiation exposure statement

This device complies with ISED radiation exposure limits set forth for an uncontrolled environment. This device should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

EUROPEAN UNION

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

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

- Compliance information for wireless products relevant to the EU and other Countries following the EU Directive 2014/53/EU (RED). And this product may be used in all EU countries (and other countries following the EU Directive 2014/53/EU) without any limitation except for the countries mentioned below table:
- In the majority of the EU and other European countries, the 5GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries in which additional restrictions or requirements or both are applicable. The requirements for any country may evolve. Zyxel recommends that you check with the local authorities for the latest status of their national regulations for the 5GHz wireless LANs.

- If this device for operation in the band 5150-5350 MHz, it is for indoor use only.
- This equipment should be installed and operated with a minimum distance of 20cm between the radio equipment and your body.
- The maximum RF power operating for each band as follows:
  - the band 2,400 to 2,483.5 MHz is 99.77 mW
  - the band 5,150 to 5,350 MHz is 197.7 mW
  - the band 5,470 to 5,725 MHz is 751.62 mW

Български (Bulgarian)	С настоящото Zyxel декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 2014/53/ЕС. **National Restrictions** - The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details. - Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens. - Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.
Español (Spanish)	Por medio de la presente Zyxel declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/UE..
Čeština (Czech)	Zyxel tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU.
Dansk (Danish)	Undertegnede Zyxel erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. **National Restrictions** - In Denmark, the band 5150 - 5350 MHz is also allowed for outdoor usage. - I Danmark må frekvensbåndet 5150 - 5350 også anvendes udendørs.
Deutsch (German)	Hiermit erklärt Zyxel, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet.
Eesti keel (Estonian)	Käesolevaga kinnitab Zyxel seadme seadmed vastavust direktiivi 2014/53/EL põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Ελληνικά (Greek)	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Zyxel ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/ΕΕ.
English	Hereby, Zyxel declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.
Français (French)	Par la présente Zyxel déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/UE.
Hrvatski (Croatian)	Zyxel ovime izjavljuje da je radijska oprema tipa u skladu s Direktivom 2014/53/UE.
Íslenska (Icelandic)	Hér með lýsir, Zyxel því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53/UE.
Italiano (Italian)	Con la presente Zyxel dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/UE. **National Restrictions** - This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details. - Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.
Latviešu valoda (Latvian)	Ar šo Zyxel deklarē, ka iekārtas atbilst Direktīvas 2014/53/ES būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. **National Restrictions** - The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details. - 2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.
Lietuvių kalba (Lithuanian)	Šiuo Zyxel deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 2014/53/ES Direktyvos nuostatas.
Magyar (Hungarian)	Alulírott, Zyxel nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvető követelményeknek és az 2014/53/EU irányelv egyéb előírásainak.
Malti (Maltese)	Hawnhekk, Zyxel, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/UE.
Nederlands (Dutch)	Hierbij verklaart Zyxel dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU.

Polski (Polish)	Niniejszym Zyxel oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/UE.
Português (Portuguese)	Zyxel declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/UE.
Română (Romanian)	Prin prezenta, Zyxel declară că acest echipament este în conformitate cu cerințele esențiale şi alte prevederi relevante ale Directivei 2014/53/UE.
Slovenčina (Slovak)	Zyxel týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EÚ.
Slovenščina (Slovene)	Zyxel izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU.
Suomi (Finnish)	Zyxel vakuuttaa täten että laitteet tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska (Swedish)	Härmed intygar Zyxel att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.
Norsk (Norwegian)	Erklærer herved Zyxel at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 2014/53/EU.

Notes:

- Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 2014/53/EU has also been implemented in those countries.
- The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Switzerland	CH
Ireland	IE	Sweden	SE
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks.
- Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.

- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,

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

  - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.

Environment Statement

ErP (Energy-related Products)

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

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

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

European Union - Disposal and Recycling Information

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

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

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

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

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

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

台灣

以下訊息僅適用於產品具有無線功能且銷售至台灣地區

- 第十二條 經型式認證合格之低功率射頻電機，非經許可，公司，商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
  前項合法通信，指依電信法規定作業之無線電通信。 低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

- 無線資訊傳輸設備忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。
- 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中
- 使用無線產品時，應避免影響附近雷達系統之操作。
-
- 高增益指向性天線只得應用於固定式點對點系統。

以下訊息僅適用於產品屬於專業安裝並銷售至台灣地區
- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

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

About the Symbols

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

Explanation of the Symbols

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

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product

have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Index

T

TCP/IP configuration **48**

Time setting **93**

U

Universal Plug and Play **84**
Application **86**
Security issues **86**
UPnP **84**
user authentication **65**
local (user) database **65**
RADIUS server **65**

V

VoIP pass through
see also ALG

W

WAN (Wide Area Network) **50**

WAN MAC address **51**

warranty **121**
note **122**

Web Configurator
how to access **14**
Overview **14**

web configurator **8**

WEP Encryption **72**

wireless channel **105**

wireless LAN **105**

wireless LAN scheduling **78**

Wireless network
basic guidelines **64**
channel **64**
encryption **65**
example **63**
MAC address filter **65**
overview **63**
security **64**

SSID **64**

Wireless security **64**
overview **64**
type **64**

wireless security **105**

Wireless tutorial **38**

Wizard setup **17**

WLAN button **9**

WPA compatible **66**

WPS **8**