

# How to manage your router – Part I

By Lance Whitney | Ask Woody | Issue 17.1.0 | 1/6/20

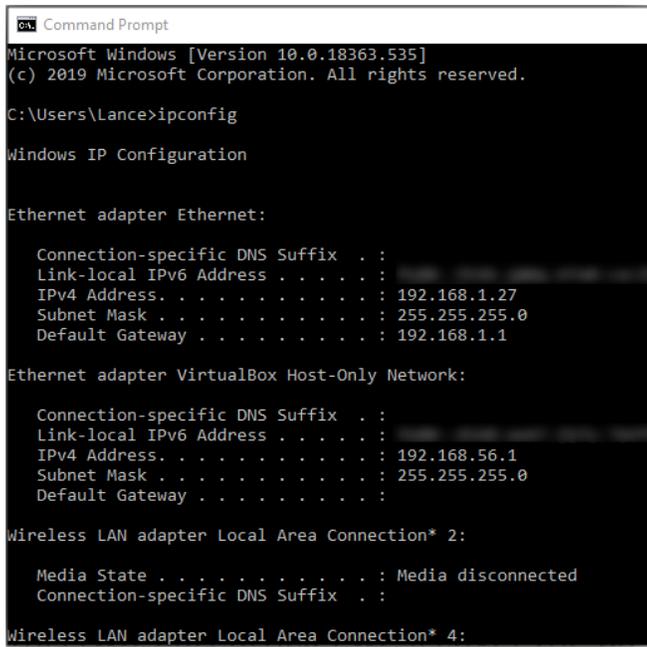
Your router holds the keys to your local network. Here's how to interpret and configure its various settings. Router management has always been a somewhat challenging task, especially if you venture beyond the basic settings. Over the years, router manufacturers have tried to make the initial configuration process simpler through one-touch buttons and easy-setup wizards.

But making sure your Wi-Fi network is configured securely and properly means delving into the local router's firmware, checking and tweaking various options.

In Part I of this two-part series, I'll cover the basics of router management. In Part II, I'll dive into some of the more esoteric settings.

## A plethora of interfaces

Describing router menus and settings can be a bit complicated: there are many brands of routers, each with its own spin



```
Command Prompt
Microsoft Windows [Version 10.0.18363.535]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Lance>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : 
    IPv4 Address. . . . . : 192.168.1.27
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : 
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 4:
```

on a user interface and settings nomenclature. Fortunately, most of the concepts and key settings are essentially the same across the board. So the information and steps I cover here should apply to virtually any brand of home/small-business router. Just be prepared to do a bit of interpretation. For this article, I'm using a NETGEAR Orbi mesh router.

I'll assume your router is already set up with a username, password, SSID (service set identifier), and other key information needed to establish a Wi-Fi network and Web connections. Using that as a starting point, let's check out the router's basic firmware settings.

Managing the router begins with signing in by simply entering its IP address into a browser. A typical default router address is **192.168.1.1**, but yours might be different. If you don't know the address for your device, it's easy to find: simply open a command window (type "cmd" into the Windows search box) and enter **ipconfig** at the prompt. Look for the address assigned to the *Default Gateway*. Figure 1 shows that my gateway/router has the common **192.168.1.1** address.

Figure 1

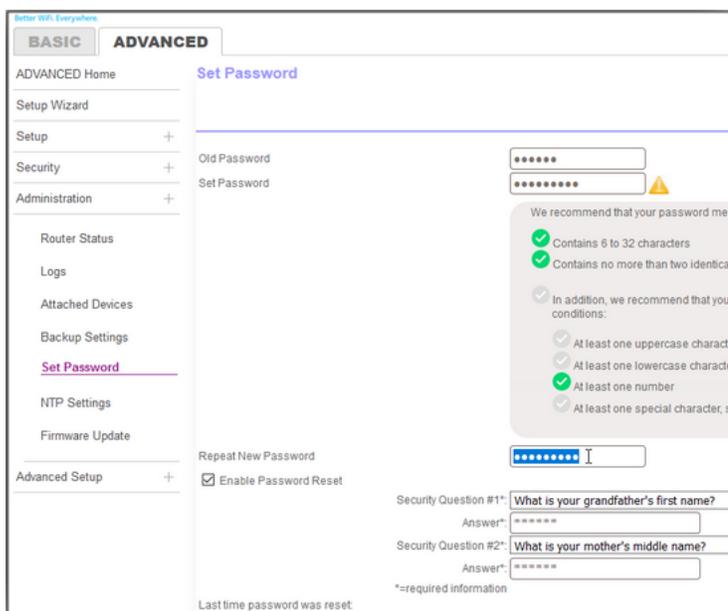


Figure 2

on my NETGEAR Orbi, I had to go to the *Advanced settings* screen to change the password.

## Check your router username and password

When your router's sign-in screen appears in the browser, enter the required username and password. (If you don't know it, try the credentials typically printed on the router's box. If that fails, it's probably time to call your router's installer or tech support. Come back to this article when you have that sorted out.)

If you're still using the router's default, factory-set username and password, your first task is to change them — they're often extremely simple (e.g., "admin" and "password") and are easily hacked. (They're probably published on the Internet for all to see.)

Some routers let you change the *username*; others don't. If you do see this option, reset the default name to something more secure and distinctive.

You might have to hunt a bit for the screen that lets you change the username and/or password. For example,

As with all passwords, create something that's strong and secure. Conventional wisdom is to use both alphanumeric and special characters, but that can be difficult to remember. An alternative is a *passphrase* made up of several easy-to-remember words strung together.

Be sure you don't lose your new password; regaining access might involve performing a factory reset. If your router, like mine, offers password-recovery options such as security/challenge questions (see Figure 2), be sure to set those up as well. In the event you forget the password, the recovery options will quickly get you back into the router settings.

### Check your Wi-Fi network name and password

Your router also came with a default SSID (your network name) and connection password. If you're still using them, all the devices connected to your network are vulnerable to hacks. Look for the screen that lets you change both settings (typically the *Wireless* screen). Figure 3 shows the Wireless Settings windows for my router. Don't include any personal information in your network name, such as your name or address.



Figure 3

Next, check the network-connection security level. On personal nets, **WPA2-PSK** is currently the strongest form of Wi-Fi authentication. Avoid options such as WEP or WPA-PSK, if offered. You might also see **WPA-PSK [TKIP] + WPA2-PSK [AES]** listed, which allows for backward compatibility. Use this option only if you have extremely old wireless devices that don't support WPA2.

The standard rules apply for the Wi-Fi password: use a passphrase or variety of characters to make it strong and secure.

**Remember:** If you change your Wi-Fi name and/or password, you'll need to update the sign-in on *every* device that connects to your network — including PCs, phones, tablets, streaming boxes, smart TVs, smart speakers, and all the other gadgets.

### Set up a guest network

Unless you have absolutely no social life, there will be times when friends, relatives, or others might want access to the Internet via your local Wi-Fi. Rather than giving them the credentials to your primary network, you can usually create a **guest** network. Look through your router's setup screens for those settings (see Figure 4). Enabling guest Wi-Fi is nearly identical to configuring the main network: you enter or select a name, password, SSID, and security level. Over time, you can easily turn the guest network on or off as needed.

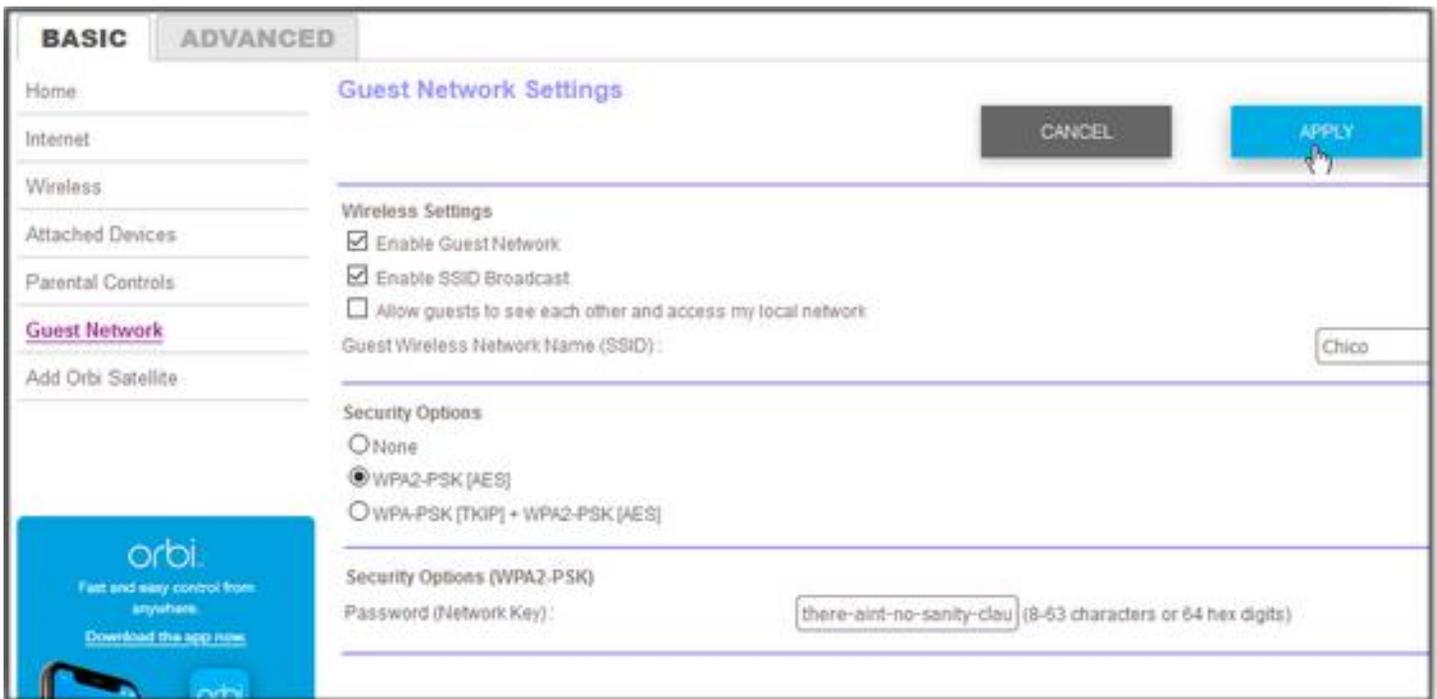


Figure 4

### Set up parental controls

If children will be accessing the Internet via your local Wi-Fi, check out the router's parental-control settings — assuming it even offers them. Options include filtering or blocking access to specific apps, services, and content — by listed device. If you have kids using multiple devices, limiting Web access via the router can be easier than managing each separate device.

### Check connected devices

While you're configuring basic router settings, peruse the screen that lists "attached" or "connected" devices; it's typically called **Access Control** (see Figure 5). You'll see everything connected to the network — by name, IP address, and other information. Look for any devices that *should not* be using your network. The access control screen also lets you block or otherwise manage any connected hardware. For example, my router allows me to automatically block any new devices.

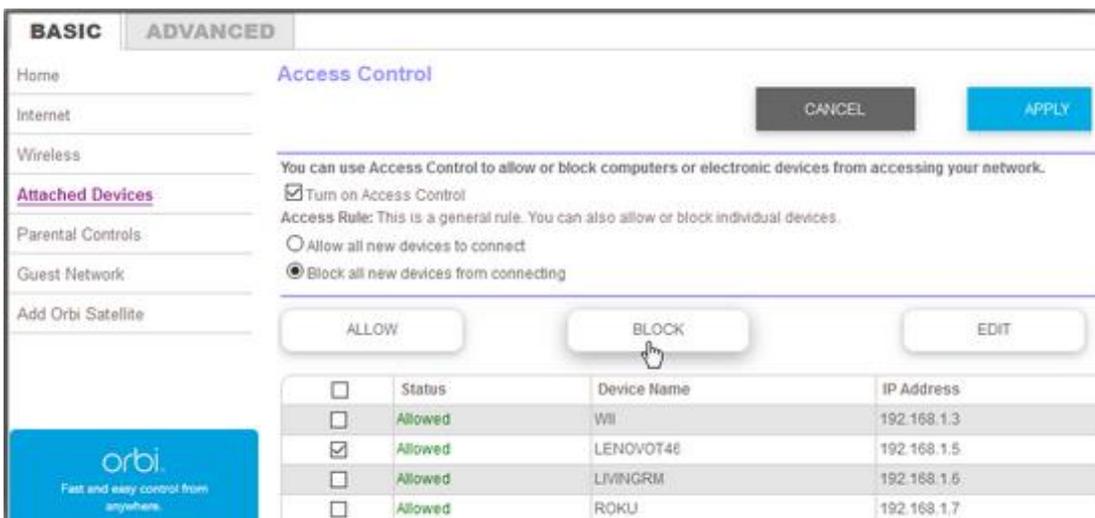


Figure 5

Your router is now fully secure. In Part II of this series, we'll look at some advanced router settings such as DNS server, speed tests, site blocking, MAC-address control, remote management, logs, and firmware updates.