4

SECURING WIRELESS NETWORKS

Wireless networking has become ubiquitous and is synonymous with being online. Most places with an internet connection have a wireless modem or router serving a multitude of devices, from desktops to phones and internet of things (IoT) devices such as TVs, light bulbs, and refrigerators. Without wireless technology, modern life would be much less convenient, but convenience often forces us to give up some of our online security.

Wireless networking has caused our networks to extend beyond the cables that originally served as physical boundaries. They even bypass other physical barriers we take for granted: walls. As wireless technologies evolve, the effective distance of our wireless networks improves, so much so that we're now seeing larger networks that overflow from what used to be local area networks (LANs) inside our premises, all the way out to our neighbors. This is fantastic in terms of connectivity, but potentially disastrous regarding security.

This chapter will address some of the pitfalls associated with wider wireless networks. You'll learn about reducing your attack surface by disabling IPv6 and limiting the number of devices allowed on a wireless network. The chapter will also delve into MAC address filtering, which allows only known devices onto the internal network; disabling features when they're not in use; using secure authentication methods; and grouping devices or users based on their necessary privilege level within the network.

UPGRADING YOUR HARDWARE

If you received wireless networking equipment from your internet service provider, it's likely an entry-level device. Usually, this means it has fewer features or is less configurable than a higher-end product. If, while making your way through this chapter, you find that your device doesn't allow the level of management required, consider purchasing a model with higher specifications. Netgear's Nighthawk series routers, for example, are reasonably priced and fully featured, even at the mid-range.

#15: Disabling IPv6

IPv6, the newer version of the Internet Protocol, was designed to combat the fact that we'll eventually run out of publicly addressable IPv4 space. IPv6 expands the available address space by many orders of magnitude, but it's not as common as another mitigation: network address translation (NAT), which we described in **Chapter 1**. If you don't use IPv6 in your network but leave it enabled, you're providing adversaries one more potential *intrusion vector* (that is, another way to enter or otherwise compromise your network). As a general rule, you should disable or uninstall all protocols and applications that are not in active use to prevent attackers from using those tools (or the tools' vulnerabilities) against you. Disabling unused protocols reduces the attack surface of your environment, which should be as small as possible.

If you aren’t actively using IPv6 in your network, disable it wherever you can, including in your Wi-Fi configuration. To disable IPv6, follow these steps:

Windows

1. Open **Network and Internet Settings**.
2. Click **Change adapter options**.
3. 3. For each adapter in the resulting window, double-click the adapter and then click **Properties**.
   a. Find the **Internet Protocol Version 6 (TCP/IPv6)** checkbox and uncheck it.
   b. Click **OK** and close the remaining windows.

macOS

1. Open **System Preferences**.
2. Click **Network**.
3. 3. For each adapter in the list, click **Advanced**.
   a. Open the **TCP/IP** tab.
   b. Ensure Configure IPv6 is set to **Off**.

Linux

1. Open **Settings**.
2. Select **Network** from the list on the left.
3. 3. For each adapter, click the configuration **Cog**.
   a. In the **IPv6** tab, click the **Disable** radio button and then click **Apply**.

Your Modem or Router

Configuring your modem or router may be trickier, since every device has its own configuration menus and options. Some devices will have an IPv6 section; if this is the case, access that menu and disable IPv6 entirely. Or, you might find the IPv6 option in the DHCP settings. Others may be hidden within the Wireless or LAN options. In the pfSense device discussed in Chapter 3, the IPv6 settings are found under **Services ▸ DHCPv6 Server & RA**. Unless you configured a network interface in pfSense with a static IPv6 address, this will be disabled by default.

If you're unable to find the setting for IPv6 in your device, search the make and model on the internet. Once you've disabled IPv6, you're one step closer to being more secure.

#16: Limiting Network Devices

Most small, nonenterprise networks rarely specify or otherwise limit the devices present in their networks and suffer from being too open, allowing all devices to connect. While this setup provides convenience, particularly when you buy a new device or friends come over, it's an insecure practice that leaves a wide hole for potential adversaries, whether targeted or opportunistic.

You can avoid this security risk by identifying all the devices allowed to connect to the network and restricting access to just those devices. Creating an *asset list*—a table containing data about each device, such as its type (PC, laptop, mobile phone, and so on), location, hostname, MAC address (its hardware address), and IP address—will complement your network map and vice versa, helping you keep track of the various devices on your network.

Once you've collected this information for all the endpoints in your network, you can assign static IP addresses to known devices and reduce the assignable IP address range in your DHCP server. Make the range small enough to include enough addresses for the devices in your asset list and on your network map. By reducing the number of available addresses, you lower the risk of an adversary adding new devices to your network without detection. Even having taken this security measure, an adversary may be able to force one of your devices to disconnect and connect their own in its place. This is where MAC address filtering comes in.

MAC address filtering lets you allow or deny access to your network based on a device's MAC address. If you know the MAC addresses of all allowed devices, you can make unauthorized devices harder to add to the network and easier to detect.

Creating an Asset List

Unlike in large enterprises, making an asset list in smaller networks is fairly straightforward. First, create a chart like the one in Table 4-1 using pen and paper, Excel, or some other tool.

Table 4-1: An Asset List Template

Device	IP address	MAC address	Hostname (optional)	Location (optional)
My laptop				
Their laptop				
My phone				
Their phone				
TV				

Table 4-1: An Asset List Template

Device	IP address	MAC address	Hostname (optional)	Location (optional)
Tablet				
Xbox				

You can choose to omit the hostnames and locations, but be sure to include the IP and MAC addresses of each device. If the devices are already connected to your network, you can retrieve this information from your router's DHCP section or your DHCP server if you have one. For devices without user interfaces, such as Wi-Fi-connected lights, this may be your best or only option. Alternatively, you can gather the details from each host.

Windows

1. Open **Network and Internet Settings**.
2. Click **Change adapter options**.
3. Identify the adapter that connects the device to your network. If connected to Wi-Fi, it will be the Wi-Fi adapter; otherwise, it's the Ethernet adapter. Double-click the adapter and then click **Details**.
4. Find the physical address and record this as the computer's MAC address in your asset list.
5. Locate the IP address and record this as well.
6. Click **Close** and close the remaining windows.

macOS

1. Open **System Preferences** and click **Network**.

2. Identify the adapter that connects the device to your network. If connected to Wi-Fi, it will be the Wi-Fi adapter; otherwise, it's the Ethernet adapter.
3. Click **Advanced** and then click the **TCP/IP** tab.
4. Record the IPv4 address.
5. Go to the **Hardware** tab and record the MAC address.
6. Click **OK** and close the Network window.

Linux

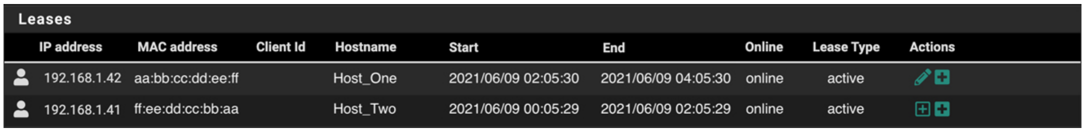
1. Open **Settings**.
2. Select **Network** from the list on the left.
3. Identify the adapter that connects the device to your network. If connected to Wi-Fi, it will be the Wi-Fi adapter; otherwise, it's the Ethernet adapter.
4. Click the configuration **Cog**.
5. In the **Details** tab, record the IP address and the hardware address (the MAC address).
6. Close the windows.

You should have successfully identified all known devices in the network. If any unknown devices are connected, you'll block them using the steps in the upcoming "MAC Address Filtering" section. Next, you'll assign each device a static IP address.

Static IP Addressing

IP addresses can be *static* or *dynamic*. By default, most routers use a Dynamic Host Configuration Protocol (DHCP) server to assign IP addresses to endpoints when they connect to the network. These assignments are called *DHCP leases* and are time-bound; a lease typically expires after 24 hours. Dynamic IP addresses may change each time the endpoint connects or the lease expires. However, you can alternatively assign each endpoint its own static IP address that it'll keep every time it connects to your network. This helps you know to which endpoint a given IP address corresponds and can prevent unknown devices from connecting by limiting available dynamic addresses.

You'll find the static IP address settings in the DHCP menu of most Wi-Fi routers. For this example, we'll be using the DHCP Leases menu of the Netgate SG-3100 covered in Chapter 3, but the process should be similar regardless of the device you're using. To reach the DHCP Leases menu in the SG-3100, click **Status ▸ DHCP Leases**. In similar devices, it might appear in the LAN or Advanced settings. You should see a table similar to Figure 4-1.



Leases

	IP address	MAC address	Client Id	Hostname	Start	End	Online	Lease Type	Actions
👤	192.168.1.42	aa:bb:cc:dd:ee:ff		Host_One	2021/06/09 02:05:30	2021/06/09 04:05:30	online	active	✎ ⊞
👤	192.168.1.41	ff:ee:dd:cc:bb:aa		Host_Two	2021/06/09 00:05:29	2021/06/09 02:05:29	online	active	⊞ ⊞

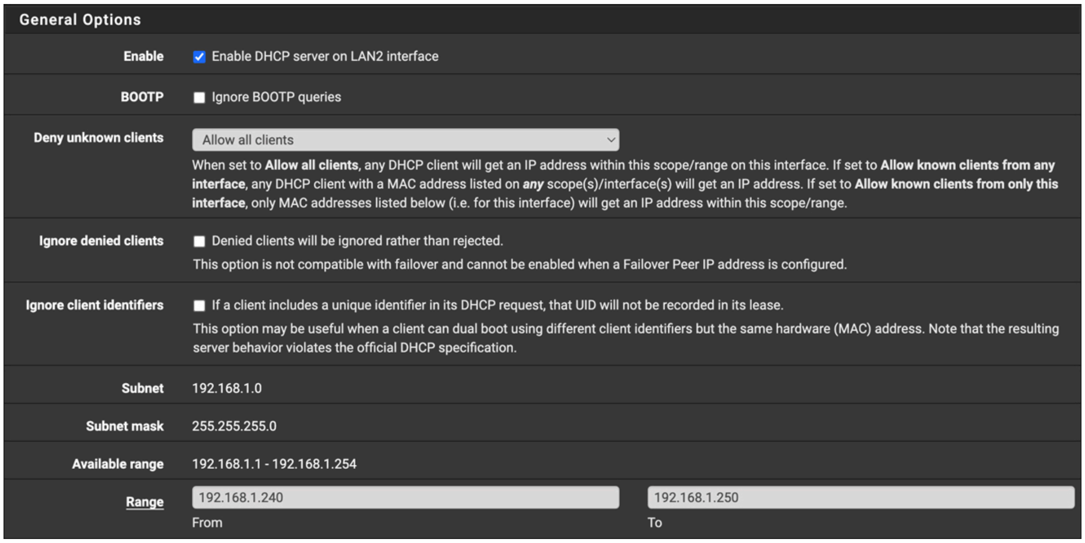
Figure 4-1*: DHCP leases menu on the Netgate SG-3100 pfSense firewall*

To create a static IP address (also called a *static lease*), click the **Add** button (in the SG-3100 it's the left, unfilled + button). The resulting page allows you to specify an IP address for the host you selected. Specify any address you'd like, as long as it's within your addressing scheme, and then click **Save**. For example, if your address scheme is *192.168.1.x*, you might choose *192.168.1.100*. The IP addresses you choose don't have to be consecutive; you can use *192.168.1.100* for this host and *192.168.1.54* for the next. After you've assigned the host's static address, it will probably need to reconnect to the network to acquire it; force it to do so by power-cycling the device (turn it off and on).

Once you've assigned static IP addresses to your authorized devices, update your asset list and network map. Then, to effectively ban additional devices from joining without authorization, reduce the range of addresses the DHCP server may assign.

By default, the DHCP server service makes the entire IP address range available for devices to connect to the network. If your IP addressing scheme is *192.168.0.0/16*, your network can have up to 65,534 hosts connected. No small network needs that many hosts, and leaving this wide open is a security risk.

To see the DHCP address range in the SG-3100, click **Services ▸ DHCP Server**. Your device should have an IP address range similar to Figure 4-2.



General Options

Enable	☑ Enable DHCP server on LAN2 interface
BOOTP	□ Ignore BOOTP queries
Deny unknown clients	Allow all clients When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on ***any*** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.
Ignore denied clients	□ Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore client identifiers	□ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Subnet	192.168.1.0
Subnet mask	255.255.255.0
Available range	192.168.1.1 - 192.168.1.254
Range	192.168.1.240 From 192.168.1.250 To

Figure 4-2: *DHCP address range*

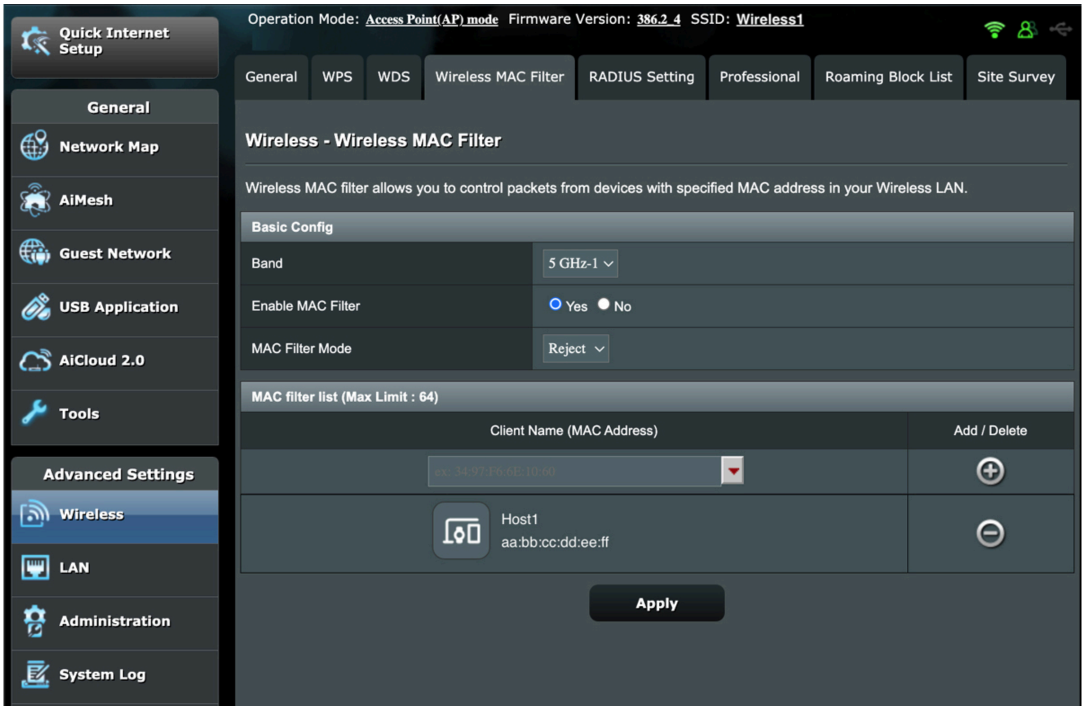
The numbers may be different, but the general configuration should be close. To manually authorize every device that connects to your network, disable the DHCP server and add new static addresses for every endpoint. An alternative is to shorten the available DHCP address range. Instead of allowing the range to be open from *192.168.1.100* to *192.168.1.245*, you could specify of range of *192.168.1.100* to *192.168.1.105*, limiting the number of devices that can be assigned a DHCP address to six. When these IP addresses have been statically assigned to the devices within your network, no additional devices can receive an IP address from the DHCP server without one of those devices going offline or being removed from the network. Reducing the available address space reduces the ability for unauthorized devices to connect to your network, thereby minimizing your attack surface.

You might be wondering if these steps are necessary, when anyone wanting to connect to your wireless network will need to be nearby, and you probably don't let strangers into your home or office. Consider, though, that "close proximity" might be as far away as a car on the street outside your building, or the suite of offices next door.

MAC Address Filtering

MAC address filtering can be implemented as either a stand-alone defense or an additional layer of security. Most wireless routers allow you to specify the MAC addresses allowed to connect to your network, thereby blocking unspecified MAC addresses. MAC addresses are less likely to change than IP addresses, as they're tied to a device's hardware.

These days it's not that difficult to fake, or *spoof*, a hardware address. However, any additional obstacle you can place between an adversary and your network will make it more secure. As an example, to access the MAC address filtering page on an ASUS RT-AC5300 wireless router, you'd click **Wireless** ▸ **Wireless Mac Filter**, as shown in Figure 4-3.



Operation Mode: Access Point(AP) mode Firmware Version: 386.2_4 SSID: Wireless1

Wireless - Wireless MAC Filter

Wireless MAC filter allows you to control packets from devices with specified MAC address in your Wireless LAN.

Basic Config	
Band	5 GHz-1
Enable MAC Filter	● Yes ○ No
MAC Filter Mode	Reject

MAC filter list (Max Limit : 64)

Client Name (MAC Address)	Add / Delete
ex: 34:97:F6:6E:10:60	⊕
Host1 aa:bb:cc:dd:ee:ff	⊖

Figure 4-3: *Wireless MAC address filtering on an ASUS AC-RT5300 router*

The Basic Config options shown in **Figure 4-3**—the wireless band, whether the filter is enabled or disabled, and whether the filter mode is Accept or Reject—can be applied to either the 2.4 GHz or 5 GHz radio.

2.4 GHZ AND 5 GHZ WIRELESS BANDS

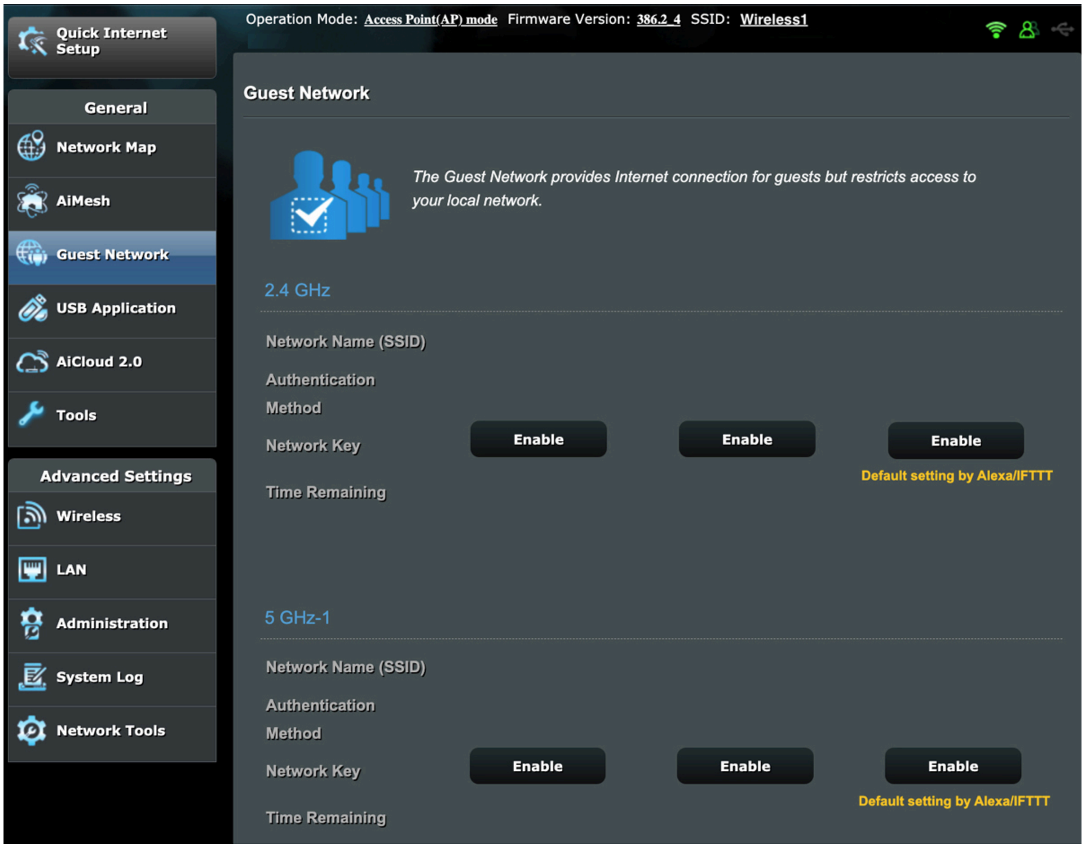
These two frequencies have several differences. One is the wavelength: the 2.4 GHz band will result in a wireless network that functions over greater distances, while the 5 GHz band will be less effective over longer distances, but it can provide faster speeds within its shorter range. There will likely be more interference on the 2.4 GHz band, as this is an older technology, so far more wireless networks and devices use this frequency (including microwaves, which can cause wireless interference). Finally, not all wireless devices are capable of handling both 2.4 GHz and 5 GHz wireless signals.

In **Figure 4-3**, the MAC filter for the 5 GHz band is Enabled, and the Mode option is set to Reject. This mode causes the filter to function as a *denylist*, meaning anything on the list will be blocked or denied access. An *allowlist*, on the other hand, is a list of endpoints that will be allowed access. Use a denylist when you know the MAC address of a device to which you want to deny access. In most cases, you'll use the Accept, or allowlist, mode instead. In Accept mode, the MAC filter list contains the MAC addresses that you've explicitly allowed access to the network.

Select **Enable Mac Filter** and **Accept** and then enter the MAC addresses from your asset list. Once you've added all the MAC addresses and saved your configuration, no devices except those specified can connect to the wireless network and acquire an IP address. You can test this by removing one of the less critical devices from the Accept list and trying to connect it to the network. If it refuses to connect, your MAC filtering is working correctly.

#17: Segmenting Your Network

Wireless networking grants you the ability to share an internet connection with guests by using a separate guest network without compromising your security. Most mid-range wireless routers offer this functionality. The ASUS RT-AC5300, for example, allows for multiple guest networks on both the 2.4 GHz and 5 GHz wireless frequencies, as shown in **Figure 4-4**.



Operation Mode: Access Point(AP) mode Firmware Version: 386.2_4 SSID: Wireless1

Guest Network

The Guest Network provides Internet connection for guests but restricts access to your local network.

Figure 4-4*: Multiple wireless network capability*

A guest network is not only convenient for your visitors; it also allows you to group users and devices by their level of risk or trust. For example, on your private internal network, you might connect your primary devices: laptops, mobile devices, and so on. Then, on the guest network, you might connect your IoT devices: your Google Home, Amazon Alexa, LIFX or other smart lightbulbs, and other similar devices.

Certain categories of devices are inherently less secure. For instance, IoT devices are susceptible to botnet infections. A *botnet* is a group of internet-connected devices, usually linked via malware installed on each device. The malware causes the group to be controlled as a collective, usually for malicious activity, such as distributed denial-of-service attacks, data theft, or spamming. Allowing devices with lower standards of security onto the same network segment as your primary devices is risky. The best way to mitigate this risk is to separate them, either logically or physically.

As shown in **Figure 4-4**, you can allow guest devices on the network for an unlimited amount of time or a specific period of your choosing, which is useful for guests who may need access for only a few hours. By configuring your router to allow guests unlimited access, you trade security for convenience. Conversely, limiting the amount of time a guest can connect before needing to be re-authorized requires more work. Still, it's a far more secure manner of access control.

One last feature provided by some wireless routers and access points is the option to allow or deny access to your *intranet*, which is the internal network where your private devices are connected. Allowing guests access to this segment of your network lessens your security, as it provides them with access to your computers and mobile devices. If you let guests access your entire network, you might as well give them access to your primary wireless network instead of configuring a guest network. The ASUS wireless router I've been discussing has this capability; if you configure a guest network, you can choose to allow endpoints connected to that wireless network to access your intranet or allow them to access only the gateway to the internet. The router handles this access by allowing or disallowing devices connected to your guest network to see devices connected to your primary network. Banning access from the guest network to your intranet is the more secure option and one that you should implement. If your router has this capability, a fairly obvious checkbox should be present in the wireless network settings. If you can't find it, chances are your router doesn't have it (although you can make sure by reading the manual or doing a quick internet search).

#18: Configuring Wireless Authentication

You should protect your Wi-Fi network with encryption by creating a passphrase to access the network. An open wireless network—with no protection or encryption—provides a prime target for an adversary. Today, most networks use one of three security algorithms to secure their communications: WEP, WPA/WPA2, or WPA3.

WEP

Wired Equivalent Privacy (WEP) is the oldest of the three security protocols and by far the least secure. WEP uses either a 40- or 104-bit encryption key, both of which are small when compared to those of later protocols. WEP combines this encryption key with 24-bit initialization vectors (IVs) meant to provide enhanced security, but the shortness of these IVs means the algorithm will likely reuse keys, which in turn makes the encryption easier to crack. Understanding the details isn’t necessary; just know that WEP is an insecure technology and shouldn’t be used. In fact, vendors phased out WEP by 2001; it’s no longer available on most hardware.

WPA/WPA2

Wi-Fi Protected Access (WPA), the successor to WEP, improved upon WEP’s protection. Although it relied on the same RC4 encryption cipher, it also introduced the *Temporal Key Integrity Protocol (TKIP)*. TKIP strengthened wireless security by using a 256-bit key and implementing message integrity checking, larger 48-bit IVs, and mechanisms to minimize IV reuse.

In turn, WPA2 improved the original WPA protocol. Both WPA and WPA2 allow users to choose between personal and enterprise modes. Personal mode, called WPA-PSK, uses a preshared key (PSK) or passphrase to grant access, while enterprise mode requires an authentication server. WPA2 replaced both the RC4 encryption cipher and TKIP in favor of more secure algorithms and encryption protocols. Moreover, it implemented *Counter Mode CBC-MAC Protocol (CCMP)*, a more secure encryption mechanism. All of this made WPA2 far more secure than the earlier encryption protocols and facilitated roaming between access points, providing a smoother user experience. If possible, choose WPA2 or greater in your wireless network.

Having said that, an adversary could still capture your wireless traffic and brute-force your network password. Though WPA2 is good, there's no such thing as perfect security. As a result, ensure that you use strong passphrases to secure your wireless networks. Passphrases are discussed in detail in **Chapter 11**.

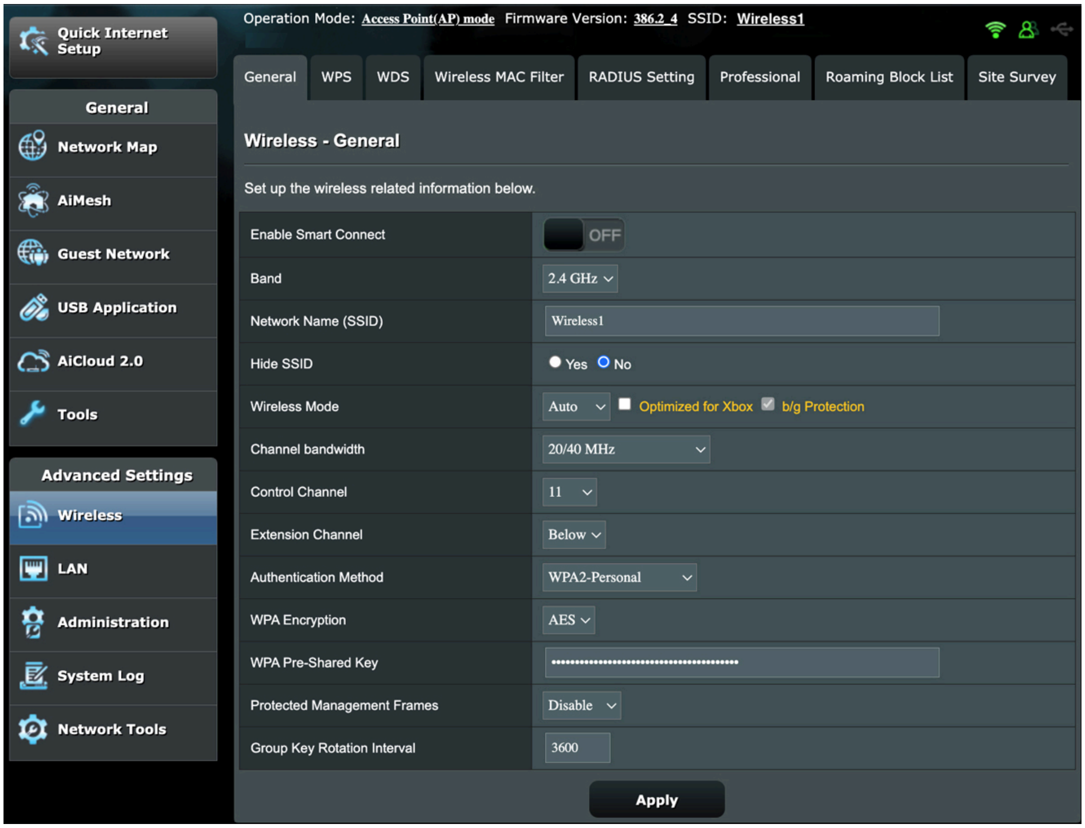
WPA3

Wi-Fi Protected Access version 3 (WPA3) is the latest wireless security technology. It's very recent and hasn't yet seen wide adoption. WPA3 improves security by keeping users who are connected to the same network from eavesdropping on each other's wireless communications—even if the wireless network is open and doesn't require a password to authenticate.

WPA3 achieves this by replacing the preshared key authentication used in WPA2 with a new protocol: *Simultaneous Authentication of Equals (SAE)*. This change also means adversaries can't capture the traffic needed to crack the network's password, making it even more difficult for them to gain unauthorized access to the network.

For now, WPA3 is in its infancy, so very few devices are compatible. Newer wireless routers and access points will come with WPA3 as standard. Even then, other devices will need to catch up before you can use it; there's little value in having a WPA3 router if your phones and computers can't connect to it. Once this changes, you should use WPA3 over any other wireless security standard.

To configure the ASUS router we've been discussing, in the wireless settings, under **Advanced Settings ▸ Wireless ▸ General**, you'd create your primary, internal network by specifying the network name (SSID) and a security key or passphrase, as shown in Figure 4-5. Then, in **General ▸ Guest Network ▸ Enable**, create one or more guest networks to which you'll connect all of your other devices by specifying a network name and security key or passphrase, just as you did for your primary wireless network.



Operation Mode: Access Point(AP) mode Firmware Version: 386.2_4 SSID: Wireless1

Wireless - General

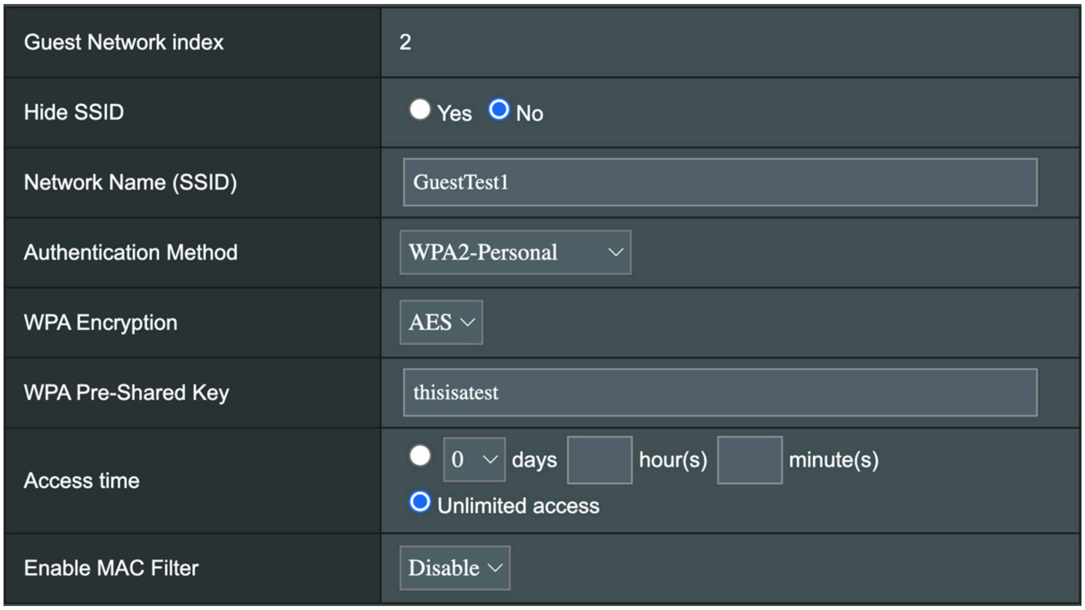
Set up the wireless related information below.

Enable Smart Connect	OFF
Band	2.4 GHz
Network Name (SSID)	Wireless1
Hide SSID	○ Yes ● No
Wireless Mode	Auto □ Optimized for Xbox ☑ b/g Protection
Channel bandwidth	20/40 MHz
Control Channel	11
Extension Channel	Below
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA Pre-Shared Key	••
Protected Management Frames	Disable
Group Key Rotation Interval	3600

Figure 4-5: Primary wireless network settings

The ASUS router used in this example keeps your main wireless network and the guest networks divided. The same process could be followed on most modern mid- to high-end wireless routers. Any endpoints connected to the main wireless network will be unable to communicate with endpoints connected to the guest networks, and vice versa. However, if you create multiple guest networks, devices on any of those networks will be able to see and communicate with one another. Some wireless routers may provide the ability to keep each of your guest networks completely separate as well. Do your research before investing in a wireless router if you want this capability.

Be sure to follow secure practices and take advantage of any security options available, such as those discussed earlier. For example, the ASUS router has several features available for securing your wireless networks, as shown in Figure 4-6.



Guest Network index	2
Hide SSID	○ Yes ● No
Network Name (SSID)	GuestTest1
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA Pre-Shared Key	thisisatest
Access time	○ 0 days hour(s) minute(s) ● Unlimited access
Enable MAC Filter	Disable

***Figure 4-6**: Wireless network security settings*

Where you have the ability to set a WPA passphrase or preshared key, do so. You should always take any opportunity to harden the network against opportunistic adversaries. In some cases, it's also beneficial to limit the access time allowed to endpoints connected to these networks. If you plan to use a secondary network for endpoints that are expected to be always on and connected, that option may not suit your needs. However, if you'll use these networks for guests, or endpoints that need only limited connectivity, limit the amount of time those endpoints are allowed to remain connected to a reasonable number of minutes or hours as you see fit. The last option shown in Figure 4-6, Enable MAC Filter, lets you allow or deny devices access to your networks based on their hardware addresses.

WIRELESS NETWORK TIPS

Most routers allow you to hide your wireless network by preventing the network name, or *SSID*, from being broadcast. Doing so will keep the network from appearing in the list of available networks on your device. Even if your network is hidden, you'll still be able to connect to it with the right access credentials. Hiding your network isn't recommended, however. Even though regular users won't be able to see it, an adversary with a network analyzer could still identify it. What's worse, a hidden wireless network actually creates more noise and is easier to discover than a nonhidden one. That's because devices connected to a hidden network have to constantly broadcast beacons to determine if the network is still available, generating traffic that an adversary can capture to attempt to breach the network. Hidden networks are great for protecting your network from your not-so-tech-savvy neighbors but will do the opposite for potential attackers.

Consider turning your Wi-Fi off when it isn't in use, such as when everyone in the house is asleep or when your office has closed down for the night. If the wireless is turned off, adversaries won't be able to detect it, much less breach it. The same goes for your guest network; if it isn't being used, turn it off to reduce your attack surface.

Summary

In this chapter, we've discussed common wireless network security risks and methods to mitigate them within your network by implementing measures such as IP and MAC address filtering and reducing the available address space in your DHCP server. Creating and maintaining an asset list and network map can help to ensure no unauthorized devices are connecting to your network. Eavesdropping is the easiest risk to mitigate. Add encryption to your network in the form of WPA security (ideally WPA3, as it becomes more common) and implement a passphrase rather than a password for network access.