EBOOK EXTRAS: v2.0
Downloads, Updates, Feedback

TAKE CONTROL OF

WI-FI NETWORKING and SECURITY

by GLENN FLEISHMAN

$12.99

2ND EDITION

Click here to buy "Take Control of Wi-Fi Networking and Security" for only $12.99!

Table of Contents

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Read Me First

Welcome to *Take Control of Wi-Fi Networking and Security, Second Edition,* version 2.0, published in January 2024 by alt concepts. This book was written by Glenn Fleishman and edited by Joe Kissell.

This book explains the ins and outs of setting up, modifying, and increasing the security of a home or small-office Wi-Fi network, from choosing hardware to configuring radio settings to working with adapters in macOS, iOS, iPadOS, Windows, Android, and ChromeOS.

If you want to share this ebook with a friend, we ask that you do so as you would with a physical book: "lend" it for a quick look, but ask your friend to buy a copy for careful reading or reference. Discounted classroom and Mac user group copies are available.

Copyright © 2024, Glenn Fleishman. All rights reserved.

Updates and More

You can access extras related to this ebook on the web (use the link in Ebook Extras, near the end; it's available only to purchasers). On the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy any subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading on mobile devices on our Device Advice page.)
- Read the ebook's blog. You may find new tips or information, as well as a link to an author interview.

If you bought this ebook from the Take Control website, it has been added to your account, where you can download it in other formats and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually; see Ebook Extras.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

What's New in the Second Edition

The development of Wi-Fi slowed down by the late 2010s after a turbulent first 15 years or so. But no technology stands still, especially as demands increase for higher throughput for video, better coverage and range, and more consistent transmission to keep streaming playback smooth and solid.

Since the first edition of this book, I rolled in changes large and small. This second edition provides a more thorough overview of what's new and brings the title up to date for 2024. In particular, this book is fully updated for the Wi-Fi 6E, Wi-Fi 7, and 802.11be specifications (see Wi-Fi Standards), the expanding availability of the 6 GHz band (see Pick a Wi-Fi Channel), and the broad availability of mesh networking gear (see Build a Mesh Network). See The 2020s for Wi-Fi for an in-depth explanation of major changes.

The update also refreshes the book for the latest operating system releases: Android 14, iOS 17, iPadOS 17, macOS 14 Sonoma, and Windows 11. (For macOS users, I assume you are using Ventura or later, which replaced System Preferences with System Settings; for Windows users, Windows 11.)

Basic Terminology

You should learn a few basic networking terms before proceeding, as you'll see them repeatedly in the rest of this book:

- **Bandwidth:** This is the measure of the overall amount of user and coordinating data that can flow over a networked medium—both actual information you're sending and other data that's required to package and send it successfully. For instance, gigabit Ethernet has 1 gigabit-per-second (Gbps) bandwidth, and one version of 802.11ac (Wi-Fi 5), has bandwidth of 1.45 Gbps.
- **Throughput:** This represents the actual data flow, or the true capacity of a system. Bandwidth is fixed, while throughput varies. A

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

1.45 Gbps Wi-Fi 5 network might only be able to transfer 500 Mbps of user data. (It's the "net"—not networked—data rate: maximum rate minus network overhead, including retransmitting lost or error-ridden portions equals throughput.)

- **Backhaul:** Backhaul describes the connection between a local network and a higher-level network that manages data needed for the local network. This term used to be used almost exclusively to refer to a connection between a home or business and an ISP, and an ISP and larger core internet network interchanges. Now, with mesh networking, it's used to refer to the connections mesh nodes make with one another. See Build a Mesh Network.
- **Radios:** Wi-Fi uses radio transmissions in specific electromagnetic bands (see next section), and carries data within its transmissions. This requires one or more radio transceivers (transmitter/receivers) to encode and decode the data. As Wi-Fi developed faster speeds, the protocols required adding multiple radio systems, such as for different spectrum bands (also described next), each of which produces a unique set of signals.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Introduction

You would think that in 2024, with Wi-Fi hitting a quarter-century in existence, an entire book would no longer be necessary to explain its intricacies. I wish that were the case! It's not so much that Wi-Fi wireless networking is inherently complicated. It's never been easier to plug in a network, configure it with a wizard, and connect.

The trouble is that whenever you need anything that's not built into the set of defaults, have a house or office full of signal obstructions, or try to troubleshoot problems, you may feel you are on your own. This book is an ongoing attempt to give you the knowledge and tools to set up or update a Wi-Fi network in your home or small office that fits your needs precisely—and work through fixing glitches.

Because we all now use many different kinds of equipment on a modern Wi-Fi network, I provide detailed, illustrated advice on connecting and configuring hardware running macOS, iOS, iPadOS, Android, and Windows with Wi-Fi. I also provide advice on Wi-Fi gateways compatible with nearly all hardware on the market.

If you're trying to understand the difference between standard Wi-Fi networks and mesh wireless networks, I go into great detail, and help you decide which will serve you better. I also provide information on how to plan a network and locate the Wi-Fi network devices that provide service to your various connected equipped, from computers to game systems to sous vide cookers.

This book will also help you set up and use personal hotspots, add printers and use networked drives, manage wireless security, and make sure your own data is secured when you use Wi-Fi on your own or other networks.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Wi-Fi Quick Start

With this book, you'll learn about Wi-Fi principles and standards so you can make choices about purchasing equipment and configuring it. You'll also learn about local area networking, connecting from different operating systems to Wi-Fi gateways, how to use a personal hotspot, and securing your network and your data. Once you Learn Wireless Basics, you're ready to take the next step.

Put a network together:

- In order to set up a network, consult Pick Wi-Fi Network Gear. Then, for standard networks, read Pick a Wi-Fi Channel for background on frequencies and spectrum. This all helps you get prepared for what's in Configure Your Network.
- With a network in place, you may want to have a networked printer or network-accessible hard drives, configuration of which is explained in Share Printers and Disks.

Use a network locally and remotely:

- While setting up a network may be old hat to you, you can learn the ins and outs across every major operating system in Connect to a Network. It's common to set up and use mobile hotspots, and you can learn the details in Connect with a Personal Hotspot. You may also need to reach devices on your network from elsewhere on the internet: see Reach Your Network Remotely.

Secure your local and internet data:

- When you use your network, you want to be safe from snoopers. Read Secure Your Network for how to set this up. Beyond your network, you should make sure nobody can intercept your communications, which is explained in Secure Yourself.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

The 2020s for Wi-Fi

Before we get into the body of the book, let me take you through the most significant big changes with Wi-Fi.

Wi-Fi 6, 6E, and 7

One of the most significant evolutions since the last edition of this book was the continued move towards more sophisticated flavors of Wi-Fi that used an increasingly large bag of tricks to better serve mobile devices, work in challenging and busy areas of overlapping networks, and provide tremendous amounts of bandwidth.

As you can read in Wi-Fi Standards, the Wi-Fi Alliance trade group that manages certifications for devices bearing the Wi-Fi name decided to part from using the technical IEEE 802.11 industry standard name to dub the last three generations at the point of this renaming to Wi-Fi 4, 5, and 6. Of course, that couldn't last.

The addition of more spectrum to the Wi-Fi "portfolio" for use by individuals and businesses led to the awkward introduction of the term Wi-Fi 6E to cover the 6 gigahertz (GHz) band discussed below.

In January 2024, the alliance formally introduced the specification for the next-generation standard, Wi-Fi 7 (based on the IEEE 802.11be standard), which I'll discuss in the section referenced above. Wi-Fi 7 once again increases throughput and reliability, calling out the need for much higher bandwidth for augmented reality (AR) and virtual reality (VR) headsets. More particularly, Wi-Fi 7 takes full advantage of the 6 GHz band with *very* wide channels, and adds a method of sending a single data stream over multiple radio bands at once for the maximum throughput to a single device.

The 6 GHz Band

It's a basic fact of wireless networking that it needs swaths of radio frequency spectrum over which to transmit data. (I explain all about

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

that in Learn Wireless Basics.) I believe every country in the world allocates spectrum for dedicated and shared use. Cellular operators have paid billions in some places, like the United States, to get exclusive ranges to build out their networks.

Wi-Fi relies in nearly all the world on *unlicensed spectrum*. These are ranges of frequencies that no single party has a monopoly on using, and are generally or always available for individual and business use, for personal and commercial purposes.

For the early part of Wi-Fi's history, it used the 2.4 GHz range, known as a "junk band" in the United States for how many non-networking purposes shared it. Microwave ovens, for instance, produce an intense, short-range magnetic field at 2.4 GHz, as do industrial sealers and other scientific and medical devices.

That led to the opening of the nearly unused 5 GHz band, impractical in earlier stages of technological development. A few years ago, the United States and a few other countries extended that into the even-less-used 6 GHz band. While most of the world allows 5 GHz use, access to 6 GHz varies. In the United States, the entire range can be used, while in most of Europe, only about half—which is still a lot. I dig into 6 GHz much more in Pick a Wi-Fi Channel.

The Widespread Adoption of Mesh

It was a long time coming, but in the last few years, mesh networking became the default option for many people in setting up home networks. I'm not sure why mesh networking hasn't taken over entirely as the cost of nodes has dropped. When I was first writing about high-quality mesh systems, it could run you $600 to $1,000 to get three nodes, though there were sales and bundles that sometimes dropped the price. As I write this in January 2024, three eero brand Wi-Fi 6 nodes cost a whopping $200. Prices go up from there, but are about 50% or less than a few years ago for comparable hardware.

The persistence of standalone Wi-Fi gateways, however, means that people are still price sensitive. For many people, a Wi-Fi 6 gateway under $100 or a Wi-Fi 6E one under $150 can produce effective

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Learn Wireless Basics

If you're already up to speed on how Wi-Fi works, skip to the next chapter, Pick Wi-Fi Network Gear, which digs in on network details. If not, let's quickly run through some basics to set the stage for what follows.

Adapters and Access Points

Wi-Fi networks need two connected parts: a *wireless adapter*, also referred to technically as a *station*, and an *access point* (*AP* for short). The wireless adapter is part of a computing device (such as a smartphone, tablet, desktop computer, or smart-home device), while the access point acts as a hub, allowing wireless adapters to communicate both with each other and with other networked devices (**Figure 1**).

Figure 1: Computing devices contain wireless adapters which communicate with an access point (shown at center).

What's Wi-Fi?

Wi-Fi doesn't stand for anything—it's a made-up name—but it loosely connotes *wireless fidelity,* in the sense of *faithfulness*: devices certified as Wi-Fi capable work with other similar devices. (The Wi-Fi name celebrates its 25th anniversary in 2024!) The Wi-Fi Alliance opted starting in 2018 to append numbers to Wi-Fi to indicate its generation and capabilities, now including 4, 5, 6, 6E, and 7.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

An access point that's coupled with a network *router* designed for home or small-office networks is called a wireless *gateway*. The router part of the gateway handles local networking details. For instance, it manages the addresses of connected devices, and moves traffic from higher-level networks (typically the internet via a connection to a broadband modem). A gateway frequently includes a built-in Ethernet switch for hooking up wired devices to its local network (**Figure 2**).

Figure 2: Gateways feature built-in Ethernet switches, as you see here at the center of this TP-Link Archer AX55.

The device with the wireless adapter also includes an operating system. The operating system directs the adapter to connect wirelessly to an access point after a user (that's you!) selects the network name from a list or otherwise picks it. For example, in macOS, you can choose a network from the Wi-Fi menu; on Android, launch Settings, tap Network & Internet > Internet >, and tap a network in the list.

If multiple access points have the same network name—a requirement to form a roaming Wi-Fi network—the operating system generally picks the strongest signal. When you move away from an access point, the operating system should switch to the next strongest one without intervention as soon as it starts receiving weak signals from its current selection or when there's an increase in the amount of noise and interference on your connection (**Figure 3**).

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Pick Wi-Fi Network Gear

I expect you bought this book for one of three reasons:

- You're setting up a network from scratch in a new location, and want to know the latest and smartest way to set it up.
- You have a network that doesn't meet your needs in terms of speed or coverage, and you want to upgrade one or more access points or gateways, while keeping most of the network intact.
- The current network you're using has fully displeased you, and you want to swap out everything. You know what kind of performance you get now, and you want to improve upon it.

Since this is the crux of why you may have purchased this book, this chapter will address all those needs. First, though, it's helpful to understand the two types of networks you're likely to encounter:

- **Standard networking:** A "standard" network is essentially all you have been able to buy since the earliest days of Wi-Fi networks (**Figure 4**). These typically have to be configured one by one. They can connect to each other to form a larger network using either or both wireless networking and Ethernet, depending on the model. When you replace only parts of a network, you will almost certainly wind up using these kinds of standard gateways.

Figure 4: The Netgear Nighthawk AXE11000 has a fancy design, but there's a standard Wi-Fi 6E gateway inside.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

- **Mesh networking:** The other option is *mesh* networking (**Figure 5**). The key difference between standard gateways and mesh ones, called *nodes*, is that mesh networks automatically configure themselves by using radios reserved solely for inter-node communication. Mesh networks nodes may cost a bit more than standard gateways and extenders, but they typically require almost no effort after initial setup to work at peak performance. When setting up a network from scratch or replacing an entire network, many people have opted for mesh networks for simplicity's sake.

Figure 5: Two Linksys Velop mesh nodes.

Make a Plan

Let's start by thinking about the kind of network layout you need. You need to figure out both its geography and *topology*. The geography is where you'll physically place hardware; the topology is how you connect devices via Ethernet, whether in series (one to the next) or through a hub-and-spoke model. You might even consider using wireless connections, though I'll try to talk you out of that.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Pick a Wi-Fi Channel

This chapter helps you tune your network for optimum performance. It starts by discussing the portion of the radio frequency spectrum that your access point uses and then shows how to determine the right channel to use in each frequency band.

Many modern gateways and range extenders automatically pick channels for you, but you may need to tap into this knowledge when your network isn't performing as expected.

Note: You don't really need to read this chapter if you've opted for mesh networking, which I discuss in Pick Wi-Fi Network Gear. Mesh networks automatically configure Wi-Fi channels and other parameters based on where you place nodes. However, this chapter can still be useful background for troubleshooting.

Spectrum Trade-Offs

To make the best choice when selecting channels for an access point, you may need some background on spectrum and channel choices. (If you don't know the basics of spectrum bands and channels, brush up with Wi-Fi Spectrum before proceeding here.)

What's a Wide Channel?

Starting with the 802.11n (Wi-Fi 4) standard, Wi-Fi can use *wide channels*. These are bound-together multiples of 20 MHz channels that carry greater amounts of data proportionate to their width. (See figures in the 2.4, 5, and 6 GHz sections that follow.)

Double-wide 40 MHz channels appeared in Wi-Fi 4; current Wi-Fi gear with Wi-Fi 5 or later can now span 80 and 160 MHz. In 2024, 320 MHz channels appeared with 802.11be (Wi-Fi 7).

Wi-Fi 6 and later can also automatically drop 20 MHz chunks of wider channels if they're in use—say, using 60 MHz instead of 80 MHz.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Choosing Among the Bands

Let's begin by comparing the three bands.

2.4 GHz Band

The 2.4 GHz band is crowded with Wi-Fi networks, Bluetooth devices, and other uses. In the 2.4 GHz band, Wi-Fi uses channels that overlap because of the lack of available spectrum when the group that created early Wi-Fi standards developed it. That means you have to plan carefully or let a base station figure the channel out automatically for you (**Figure 12**).

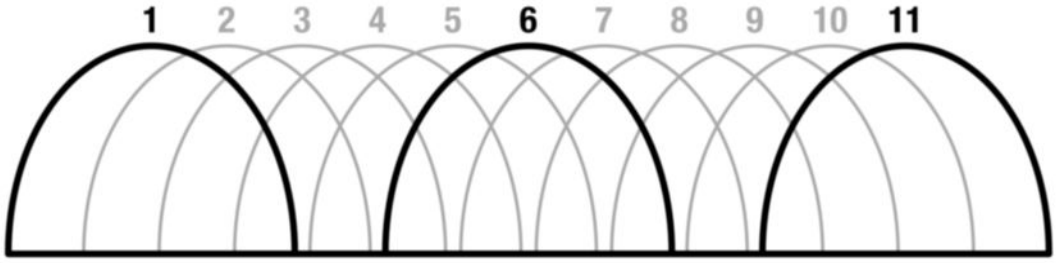

Figure 12: The 2.4 GHz band has overlapping channels, and in America, only three can be used effectively at the same time. (Channel separation exaggerated here for clarity.)

WiFi Explorer, a macOS app for detecting and graphically displaying network usage around your Mac, provides an excellent visualization of 2.4 GHz channels in practice in and near my home (**Figure 13**). You can see in the figure how several network with the same name have opted to use low-numbered channels (2 or 3), while others have picked a non-overlapping higher channel (9).

5 GHz Band

The 5 GHz band, on the other hand, is relatively empty: almost no common personal or business electronics makes use of most of it. In the United States, the 5 GHz band has almost seven times the amount of frequency available than the 2.4 GHz band. Each band is divided into a series of 20 MHz channels, which are spaced 5 MHz apart.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Configure Your Network

To use a Wi-Fi network, it has to be configured to connect on one side to the internet, and on the other side to the devices you want to have access to the internet. Outside of corporate networks, access points are embedded into home and small-office *gateways*. These almost always combine the functions of a Wi-Fi access point, an Ethernet switch, and a network router (which connects different kinds of networks and moves data among them).

Note: Gateways may also include USB and other ports so you can add printers and hard drives. This is discussed in Share Printers and Disks.

When it comes to setting up a connection to an internet service provider (ISP) and creating a local network that devices use to connect through Wi-Fi and Ethernet, every router's instructions are a bit different. In this chapter, I explain the typical choices you have to make to set up a gateway that combines a wireless access point and routing features. This includes advanced choices such as using static IP addresses and fixed private addresses as well as other less-frequent, but not unusual, options. I also discuss where to find specifics.

Let's start with a little background about how network addresses work before we get into the wide world of the internet and local networks.

Note: Mesh networks also need to be set up to connect to the internet and allow connections from wireless adapters in devices you use. However, nearly everything else about how they work is different. I explain mesh networking in Build a Mesh Network.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Learn About Dynamic Assignment and Private Addresses

Devices that use most network services need an Internet Protocol (IP) address. That's true even for a local network devices that only use local resources if those resource use IP addresses, too.

IP addresses can be *public* or *private*. Public addresses are typically *publicly routable*, meaning that they are unique across the internet and can be reached from any other point on the internet. (A firewall or other tools can block access, but the IP address is still *addressable* from the internet even if nothing can connect to a device there.)

> **Note:** The term *private address* here means something different than how Apple is using for deterring device tracking as explained in Private Addresses in iOS or iPadOS.

A private address, however, is unique only inside a Local Area Network (LAN). These addresses aren't routable from the internet, and they let you control more parameters than public addresses. They also generally make your networked equipment less reachable. (You can read more about private addresses in Dynamic Private Addresses, later in this chapter.)

Devices on a LAN typically obtain an IP address from a DHCP server. DHCP stands for Dynamic Host Configuration Protocol (DHCP), a relatively old internet technology. DHCP assigns out addresses to devices that request them on a LAN.

DHCP typically pairs with NAT (Network Address Translation). NAT allows a single address used by a gateway to be used as a conduit. NAT takes a connection between a given internet request (incoming or outgoing) from a given device on the LAN and the gateway, and then creates a new connection from the gateway with the destination address elsewhere on the internet. This allows many machines to "share" a single public IP address on a gateway. (I discuss more about how NAT works in Reach Your Network Remotely.)

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Connect to a Network

Whether you're working in your own home or helping customers with a public hotspot, once you've set up a Wi-Fi network and connected it to the internet, you'll want to configure your devices to connect to it.

Read this chapter to learn how to connect in macOS (just ahead), Connect in iOS and iPadOS, Connect in Windows 11 or Later, and Connect in Android.

Note: Just because a network is visible doesn't mean you can connect to it. MAC address access control and other restrictions could keep you from joining. See Secure Your Network.

Connect in macOS

Join a Wi-Fi network by clicking the Wi-Fi menu, which reveals networks you've previously connected to, personal hotspot networks available (from your devices, those of Family Sharing members, and others), and the network to which you're currently connected, if any. Click Other Networks to view a list of other networks that are in range. (If Wi-Fi is turned off in any version of macOS, click the Wi-Fi menu and then click the Wi-Fi switch.)

Tip: If you don't want your Mac to show you Wi-Fi networks previously unknown to your computer whenever you're not connected to one, go to Apple > System Settings > Network and deselect "Ask to join (new) networks."

To join a network when the network broadcasts its name—as most do—choose the network name from the Wi-Fi menu. Enter the network's password if it's protected.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Figure 24: On a Mac, choose a network from the list to join.

To connect to a closed (hidden) network, choose Other Networks > Join Other Network and then enter its name exactly (**Figure 25**). You also have to select the Security method.

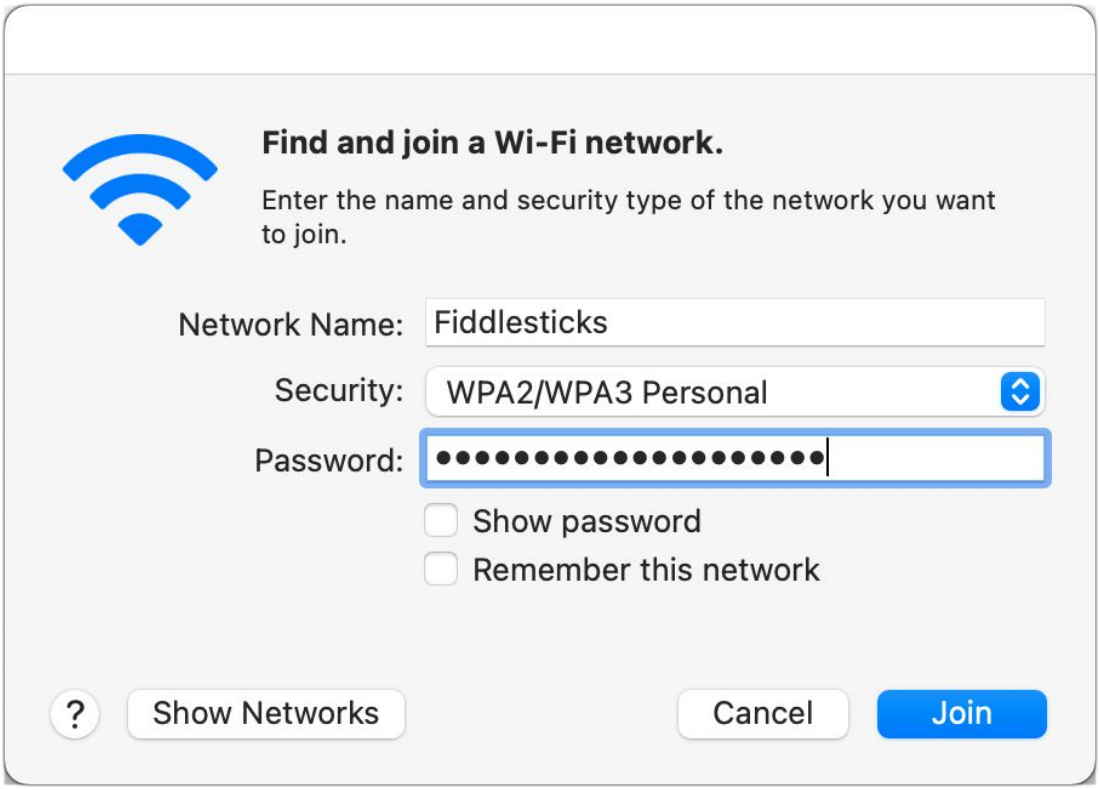

Figure 25: For hidden networks, enter a name and manually choose its security method.

Click here to buy the full 125-page “Take Control of Wi-Fi Networking and Security” for only $12.99!

Connect with a Personal Hotspot

In addition to a Wi-Fi radio, every smartphone and some tablets contain a built-in modem that lets them access high-speed mobile data networks. Early in the smartphone era, manufacturers took advantage of pairing the two together so you could use Wi-Fi to route traffic via the cellular data modem.

This took a lot of twists and turns in terms of cell carrier service plans, options, overages, and throttling, but most smartphones and some tablets (those with cellular modems) can act as personal hotspots for a few or many other devices, whether laptops or other phones and tablets.

While "personal hotspot" implies a Wi-Fi hotspot connection, many phones and tablets can also use Bluetooth or USB to extend access to other devices. On some hardware, all three methods may be used simultaneously.

Note: In this chapter, I talk about a "personal hotspot" or "mobile hotspot" to refer to all the features, but I use the term "tethering" when the discussion is specifically about Bluetooth or USB.

In this chapter, I first discuss how to turn your device into a personal hotspot and then I talk about how to connect with a personal hotspot.

How to Share a Personal Hotspot

Both iOS and Android offer personal hotspots, and can both share the connection in three ways:

- **Wi-Fi:** Any Wi-Fi–equipped device can connect as if the device were an access point. Depending on the mobile platform and age of

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

the device, you may have limits on how many devices can connect at once, which could be as low as three or five in iOS and iPadOS and as high as eight in Android.

- **USB:** Plugging your computer into your mobile device via USB gives you a high-speed data connection that you know works as long as the cable isn't bad. The downside? Being literally tethered.
- **Bluetooth:** This method requires more steps to make a connection initially, but it offers cable-free flexibility. Most Bluetooth-equipped devices can connect through this method. The OS may restrict the number of devices connecting via Bluetooth to as few as three.

Make a Computer into a Wi-Fi Hotspot

You can also turn a Mac or Windows system into a Wi-Fi hotspot if you have two connections, typically Ethernet and Wi-Fi.

Go to Apple > System Settings > General > Sharing. Click the Info ⓘ icon, enter an administrative password, and click Modify Settings. Choose the network to share from (like Ethernet) in the pop-up menu, and then select Wi-Fi in the "To devices using" list. Click Wi-Fi Options and set a password. Finally, check the box or enable the switch next to Internet Sharing.

Under Windows, navigate to Settings > Network & Internet and open "Mobile hotspot." Select the network to share from the "Share my Internet connection from" pop-up menu. Click Edit to enter a network name and Wi-Fi password, and then click Save. Enable "Share my Internet connection with other devices." (If you don't see this option, you may need to upgrade Windows to the latest release.)

Turn on Hotspot Sharing

Here's how to turn on the hotspot feature in iOS, iPadOS, and Android.

Note: If you expect to see the Personal Hotspot options in either operating system and don't, contact your carrier.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Reach Your Network Remotely

When you share an internet connection among one or more computers on a local network using private addresses, you gain the advantage of some privacy: all the machines are locked away from the rest of the internet by default. However, you also give up having an easy way to connect from the outside world to services—say, a gaming server or computer with remote desktop access—that's located on one of those local computers.

But just because it isn't easy doesn't mean it's not possible. In this chapter, I look at how you can configure gateways to route access from the outside world to specific computers, smart-home gear, and other devices for particular purposes.

Know Your Options

For systems outside your local network to reach devices on the LAN side of your gateway, you have to pursue one or more of the following four strategies:

- **Port mapping:** With a fixed address for a LAN-based device, you can create a connection between a sort of IP address cubbyhole, called a port, on the gateway and another port on the device. This *port mapping* exposes the local device's service that relies on that port to the outside world as if it's directly on the internet. Port mapping typically requires a DHCP reservation or a static address for a device on the LAN.

Tip: I explain the details of ports and port mapping later in this chapter, so don't worry if you can't visualize a port yet—most people can't!

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

- **Automatic punch-through:** Some software and devices rely on one of a few protocols that communicate directly with the gateway to negotiate automatically opening a connection—*punching through* a connection—almost always using UPnP (Universal Plug and Play). This automatic management is terrific, because in most cases you don't have to do any configuration other than turn the feature on, and thus don't have to lock a device to a fixed IP address or reconfigure gateway settings if devices or services change.
- **Use one computer as your default host:** A coarser way to make remote access work is to allowing a single computer behind a NAT act as though it's directly connected to the internet. This option fits limited cases where you want a machine to be reachable from the internet on any of its ports without getting publicly reachable IP addresses from your ISP for computers on your network. I describe this in Set a Default Host for Full Access.

> **Note:** This option is sometimes called the DMZ—a sort of inappropriate appropriation of the abbreviation for the demilitarized zone at the border between North and South Korea, as well as other troubled areas.

While I explain the three items above in their own sections in this chapter, there's one more method for reaching a computer remotely. It's self-explanatory, as it requires no configuration on your part after installation:

- **Remote connections between central servers:** Some kinds of software, notably remote screen-control software for computers, can punch through gateways, double-NAT configurations, and all sorts of nonsense. They accomplish this by having the device *from* which you're connecting and the device *to* which you're connecting create a session with a central server under the service's control. Instead of a device-to-device connection, this device-to-server-to-device gets around mapping or punching your way through. These kinds of services include the remote desktop service TeamViewer.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Share Printers and Disks

With a gateway set up to handle local computers and hooked into the internet, your next step may be to attach a printer to the access point so that it can be shared among all the local computers. In this chapter, I explain in overview how to use a gateway in this fashion, although the details vary so widely that you may plug everything in and see it work without a stitch, or need to consult the manuals for your hardware to fiddle with settings.

You can typically share printers via either USB or Wi-Fi, while disk drives need to be plugged in directly via USB.

Note: A Wi-Fi-only disk drive is typically *network-attached storage* (NAS) that relies on Wi-Fi just for networking and needs no special gateway configuration.

Add a Printer

Printers used to be connected to a network via a USB port on a gateway, or sometimes via a USB hub, for gateways that allowed multiple USB devices in that fashion.

More commonly now, printers connect via Wi-Fi, and already act as shared devices. The only gateway issue is how hard it is to add a printer with Wi-Fi security enabled.

Share a Printer via USB

This is typically as simple as plugging a USB cable from the printer into the gateway's USB port. If the gateway has both one or more USB 2 and USB 3 ports, pick USB 2, as the printer doesn't need the throughput of USB 3.

Some gateways require you to connect to their web admin system and enable a print server, name a printer, or otherwise configure the

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

settings. Others, including Apple's retired AirPort line, make the printer available under its standard driver name when it's plugged in, and have no options to customize whatsoever.

Depending on the gateway, you may be able to use a USB hub to connect multiple printers (and hard drives). Consult the manual.

Add a Wi-Fi Printer Using WPS

Wi-Fi–enabled printers that support Wi-Fi Protected Setup (WPS) can use this simplified method to connect to a Wi-Fi network. WPS lets a device join a network securely once you tell the access point that the device wants to connect.

In the best case, both the printer and the gateway have WPS buttons. You press the button—which may be physical or available via software—on the printer, and then press a physical button on the gateway. The printer is now on the Wi-Fi network.

With some printers and gateways, you may need to load the gateway's admin interface and click a button. Some printers may generate a short PIN that has to be verified or entered in the gateway admin software.

In all these cases, however, it's easier than typing a Wi-Fi password into a printer that has no keyboard!

Add a Gateway Printer to a Mac

To add a shared printer to a Mac, make sure the printer is on and not in standby-power mode, and then use these steps:

1. Go to Apple > System Settings > Printers & Scanners.
2. Click Add Printer, Scanner, or Fax. (Yes, fax!)
3. If needed, click the leftmost printer icon at the top of the window to see the printers available over Apple's network discovery standard, Bonjour (**Figure 42**).

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Secure Your Network

If you use a wired network in your home, someone would have to break into your house, plug into your Ethernet switch, and then crouch there in the dark to capture data passing over your network.

Wireless networks have no such protection: anyone with an antenna sensitive enough to pick up your radio signals can eavesdrop on traffic passing over your network. This could be a neighbor, someone in a parked car, or a nearby business. Many free, easy-to-use apps make this a simple task for only slightly sophisticated snoopers.

However, you're not powerless to prevent such behavior. Depending on what you want to protect and whom you're protecting against, you can close security holes with tools that range from a few settings up to industrial-grade protection that requires separate servers elsewhere on the internet.

I also suggest using a guest network account when you want to provide access to your network without giving out the password or providing access to devices and peripherals on it.

Simple Tricks That Don't Work

You may have read suggestions for setting up basic security that advise you to hide your network's name, or "close" the network, and make it hard to connect to. In practice, this doesn't work.

An open network appears by name in devices' Wi-Fi menus and in other places in a device's interface that show the names of networks to which you can connect. A closed network does not. However, this is less helpful from a security standpoint than it seems.

An access point set for a closed network stops broadcasting its name, but it still broadcasts other network details required by device's that know the network's name. Any device connecting has to be given the

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

network's name, and whenever those devices connect, they reveal that name openly.

An attacker can monitor the network for that connection, but they can also use free cracking tools to find an active connection between a device and the closed network and then force the name to be revealed. So you closing your network isn't a reliable way to get real security.

Timed Access Control

Some gateways offer controls that use the MAC address of a wireless adapter to restrict access during certain times or only allow usage for a certain amount of time in a given period.

This is intended to offer parents control over kids' devices, or to lock out usage at, say, a café where it's undesirable to have people using the network when no one is around to supervise. This isn't the same as using encryption, as it doesn't protect network traffic. A sophisticated attacker or child could *clone* the MAC address of a device that's allowed to connect without restrictions.

Use Built-In Encryption

For a real defense, you must use password-protected encryption. Wi-Fi has always offered some form of built-in encryption to secure the connection between a client computer or device and the access point; this connection is the most vulnerable part of a wireless network.

Note: The connection from the access point to the rest of the network or the internet must be secured separately from the Wi-Fi segment. Some people use virtual private network (VPN) connections to secure a larger chunk of their traffic, as it provides encryption between a device and a destination elsewhere on the internet, such as a data center or a corporate network. This protects against snooping on public networks and intermediate network points.

Encryption always requires a key. With Wi-Fi encryption, you don't enter the key directly, but instead enter a password that the system

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Secure Yourself

The data that travels to and from your devices isn't secure even when you're connected to a Wi-Fi network with a strong password. That's because any data you send that's not separately encrypted could be sniffed by anyone else on that network who has the right password or is connected via Ethernet.

The same is true for any point between you and your data's destination or wherever you're running an active session, whether you're using a protected Wi-Fi network, an open one, or a cellular data connection: any party in between, for unencrypted services, can see exactly what you're doing.

Encrypting our data in transit enables us to make decisions about how our data is being used and who sees it, preventing criminals, relatives, and government agencies from overstepping our rights.

In this chapter, I help you understand what's encrypted and what's not, and how to secure individual services as well as your whole network connection.

What Is TLS?

You'll read the term TLS (Transport Layer Security) repeatedly in this chapter. It's a way of securing a connection for both ends with strong encryption. It relies on digital certificates that are registered with one of many approved "certificate authorities" that help validate the identity of a site or service to which you're connecting.

Once the connection is validated and established, software on your device and the remote side exchange a strong encryption key that then protects all the data flowing between the two sides.

Note that TLS is a successor to SSL (Secure Sockets Layer), which was abandoned many years ago. Despite that, many sites, services, and people never got the message: they still say SSL (or SSL/TLS) even when SSL hasn't been used by their software or hardware for many years.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Protect Particular Services

Nearly every kind of service offers an encrypted option, and, fortunately, most modern services employ some kind of encryption by default. Here's a laundry list of what you should consider:

- **Email:** There's no good reason to avoid TLS for email. If your mail host doesn't provide secured email for your incoming email and for your outgoing email, find a new host. Without security, email apps may send passwords in the clear or with weak encryption, and likely send all data in the clear. All modern mail apps, including those that ship with an operating systems, will attempt to configure your mail settings securely.
- **Secure access to websites:** A huge movement starting a few years ago shifted most websites to secured connections for all requests, not just for commerce or banking. While not 100%, it's approaching that among the vast majority of most-visited websites. Browsers shifted from minor alerts to warnings and many may block you from connecting to a site that isn't using HTTPS and require you click through or override the block.
- **Transfer files to a server securely:** If you must use the very outdated FTP protocol for file transfer—some companies have ancient systems that require this—use only a secured alternative to plain FTP, such as the SSH-based SFTP or one of several TLS-protected methods. FTP apps otherwise send passwords and data in the clear. If you can't use secured FTP, emailing a file, or even sending a flash drive in the mail, is honestly better.

Tip: On a Mac, enable Remote Login and File Sharing in the Sharing preference pane to allow SFTP over a local network or through port-mapped remote connections.

These items are protected without any extra effort:

- **iMessage and FaceTime in Apple's ecosystem:** Apple builds in end-to-end encryption in such a way that even the company can't

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Appendix A: What and Where Is a MAC Address?

The MAC, or *Media Access Control,* address is a unique, factory-assigned address for every Ethernet and Wi-Fi adapter. With Wi-Fi adapters, it's often labeled as the "Wi-Fi address," but it's functionally equivalent and identical in format as a MAC address.

Note: It has nothing to do with Macintosh computers, despite the unfortunate homograph.

You may need to find a MAC address in a few different cases:

- If you or someone else configures an access point so that only specifically identified devices can connect. The MAC address is typically used for identification. (But it's not secure; see warning below.)
- If your network uses reserved DHCP addresses, allowing a gateway or another networked device to always assign a device the same private or public IP address. This often relies on the MAC address.
- If you're trying to determine to which access point a device has connected. Access points use a BSSID (Basic Service Set Identifier), which is effectively the same as a MAC address.

A MAC address consists of six two-digit hexadecimal numbers separated by colons, such as 0C:F2:33:01:02:FC. (*Hexadecimal,* or *hex,* is the base 16 number system, with values running from 0 to 9, and then from A to F for 10 to 15.) The first three numbers are assigned to a manufacturer by a coordinating association. MAC addresses may be used for filtering and authentication.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Warning! Some operating systems allow their network adapters to change their MAC address in a process called *MAC cloning* or *spoofing*. It can be used to attempt unauthorized access to a network, to swap in devices without reconfiguring a router, or to deter network-based unwanted tracking. Apple added random MAC address generation as an automatic privacy feature in iOS 14/iPadOS 14: see Private Addresses in iOS or iPadOS. Because MAC addresses are unreliable as a fixed method of identification, it also means you can't rely on them for authentication.

Here are the ways to locate MAC addresses in various operating systems and on some pieces of hardware.

Find the MAC Address in macOS

Find a Mac's MAC address like so:

1. Go to Apple > System Settings > Network.
2. Click Wi-Fi in the adapter list
3. Click the Advanced button.
4. In the Wi-Fi view, the MAC number is described as the Wi-Fi MAC Address.

Find the MAC Address in iOS or iPadOS

Take a three-step jaunt to locate an iPhone or iPad's MAC address:

1. Open Settings.
2. Tap General > About.
3. Swipe down to Wi-Fi Address, which is the MAC address.

Find the MAC Address in Windows

Windows 10 and later makes it a little harder, but here's how to obtain the MAC address:

1. Click Start.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

About This Book

Thank you for purchasing this Take Control book. We hope you find it both useful and enjoyable to read. We welcome your comments.

Ebook Extras

You can access extras related to this ebook on the web. Once you're on the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy a subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading on mobile devices on our Device Advice page.)
- Read the ebook's blog. You may find new tips or information, as well as a link to an author interview.
- Find out if we have any update plans for the ebook.

If you bought this ebook from the Take Control website, it has been automatically added to your account, where you can download it in other formats and access any future updates.

More Take Control Books

This is but one of many Take Control titles! We have books that cover a wide range of technology topics, with extra emphasis on Macs and other Apple products.

You can buy Take Control books from the Take Control online catalog as well as from venues such as Amazon and the Apple Books Store. But it's a better user experience and our authors earn more when you buy directly from us. Just saying…

Our ebooks are available in three popular formats: PDF, EPUB, and the Kindle's Mobipocket. All are DRM-free.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

About the Author

Glenn Fleishman never stops writing about technology and its implications. He's in his third decade of writing for publications as varied as *American History*, *Fast Company*, the *Economist*, Increment, the *New York Times*, *Macworld*, and TidBITS, and many others. In 2012, he was a two-game champion on Jeopardy!

You can find Glenn on Mastodon at https://twit.social/@glennf.

Acknowledgements

Thanks for Greg Knauss for providing assistance and screenshots in documenting Windows 11 behavior!

Shameless Plug

In 2024, I plan to produce *How Comic Were Made*, a book that traces the path from an artist's nib, brush, or digital stylus to the printed page or screen. In it, I cover the history of newspaper comics from the 1890s to 2020s. You can find out more about this book at its website and sign up to get a notification when its Kickstarter campaign launches in February 2024 (or afterwards to buy a copy).

About the Publisher

alt concepts, publisher of Take Control Books, is operated by Joe Kissell and Morgen Jahnke, who acquired the ebook series from

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

TidBITS Publishing Inc.'s owners, Adam and Tonya Engst, in 2017. Joe brings his decades of experience as author of more than 60 books on tech topics (including many popular Take Control titles) to his role as Publisher. Morgen's professional background is in development work for nonprofit organizations, and she employs those skills as Director of Marketing and Publicity. Joe and Morgen live in Saskatoon, Saskatchewan, Canada, with their two children and their cat.

Credits

- Editor and Publisher: Joe Kissell
- Cover design: Sam Schick of Neversink
- Logo design: Geoff Allen of FUN is OK
- Illustrations: Thanks to Andrew von Nagy for permission to use his 5 GHz channel illustration. Linear art used throughout for illustration via Flaticon under commercial license.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!

Copyright and Fine Print

Take Control of Wi-Fi Networking and Security
ISBN: 978-1-990783-46-3
Copyright © 2024, Glenn Fleishman. All rights reserved.

alt concepts, 419 8B-3110 8th St. East, Saskatoon, SK S7H 0W2 Canada

Why Take Control? We designed Take Control electronic books to help readers regain a measure of control in an oftentimes out-of-control universe. With Take Control, we also work to streamline the publication process so that information about quickly changing technical topics can be published while it's still relevant and accurate.

Our books are DRM-free: This ebook doesn't use digital rights management in any way because DRM makes life harder for everyone. So we ask a favor of our readers. If you want to share your copy of this ebook with a friend, please do so as you would a physical book, meaning that if your friend uses it regularly, they should buy a copy. Your support makes it possible for future Take Control ebooks to hit the internet long before you'd find the same information in a printed book. Plus, if you buy the ebook, you're entitled to any free updates that become available.

Remember the trees! You have our permission to make a single print copy of this ebook for personal use, if you must. Please reference this page if a print service refuses to print the ebook for copyright reasons.

Caveat lector: Although the author and alt concepts have made a reasonable effort to ensure the accuracy of the information herein, they assume no responsibility for errors or omissions. The information in this book is distributed "As Is," without warranty of any kind. Neither alt concepts nor the author shall be liable to any person or entity for any special, indirect, incidental, or consequential damages, including without limitation lost revenues or lost profits, that may result (or that are alleged to result) from the use of these materials. In other words, use this information at your own risk.

It's just a name: Many of the designations in this ebook used to distinguish products and services are claimed as trademarks or service marks. Any trademarks, service marks, product names, or named features that appear in this title are assumed to be the property of their respective owners. All product names and services are used in an editorial fashion only, with no intention of infringement. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.

We aren't Apple: This title is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc. Because of the nature of this title, it uses terms that are registered trademarks or service marks of Apple Inc. If you're into that sort of thing, you can view a complete list of Apple Inc.'s registered trademarks and service marks.

Click here to buy the full 125-page "Take Control of Wi-Fi Networking and Security" for only $12.99!