EBOOK EXTRAS: v2.0
Downloads, Updates, Feedback



TAKE CONTROL OF

WI-FI NETWORKING and SECURITY

by GLENN FLEISHMAN

$12.99

2ND EDITION

Table of Contents

Read Me First 4
- Updates and More 4
- What's New in the Second Edition 5
- Basic Terminology 5

Introduction 7

Wi-Fi Quick Start 8

The 2020s for Wi-Fi 9

Learn Wireless Basics 12
- Adapters and Access Points 12
- Wi-Fi Spectrum 14
- Wi-Fi Standards 17

Pick Wi-Fi Network Gear 21
- Make a Plan 22
- Build a Standard Network 26
- Build a Mesh Network 34

Pick a Wi-Fi Channel 39
- Spectrum Trade-Offs 39
- Troubleshoot Your Connections 50
- Testing from Device to Access Point 51

Configure Your Network 55
- Learn About Dynamic Assignment and Private Addresses 56
- Get a WAN Address 57
- Hand Out LAN Addresses 61

Connect to a Network 67
- Connect in macOS 67
- Connect in iOS and iPadOS 70
- Connect in Windows 11 or Later 73
- Connect in Android 76

Connect with a Personal Hotspot 79
- How to Share a Personal Hotspot 79

Turn on Hotspot Sharing 80
Connect to a Personal Hotspot 83
Reach Your Network Remotely 88
Know Your Options 88
Map Ports for Remote Access 90
Set a Default Host for Full Access 95
Share Printers and Disks 97
Add a Printer 97
Set Up a Shared Disk 102
Punch Through Automatically 106
Secure Your Network 107
Simple Tricks That Don't Work 107
Use Built-In Encryption 108
Allow Guest Networking 112
Secure Yourself 114
Protect Particular Services 115
Encrypt Files and Email 116
Umbrella Protection with a VPN 117
Appendix A: What and Where Is a MAC Address? 119
About This Book 122
Ebook Extras 122
About the Author 123
About the Publisher 123
Copyright and Fine Print 125

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, and Android.

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.

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

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.

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.

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.

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

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

coverage across a home or small business, offering the highest throughput in areas near it that correspond with the most need for streaming video. As a result, you might find that a gateway is all you need.

I discuss gateways and mesh networking in Pick Wi-Fi Network Gear.

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.

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**).



Figure 3: When there are multiple access points in a network, a wireless device will switch to the one with the stronger signal.

A device's wireless adapter attempts to connect—or *associate*—with an access point. If the access point has encryption enabled, then the device must provide a passphrase (on home and small-office networks) or a username and password (for corporate or enterprise networks) before the access point allows the device access to its network.

Once authenticated, the device's operating system proceeds to the next steps—typically requesting an Internet Protocol (IP) address. When the gateway receives and replies to that request, the device can send data to and receive it from the wireless network.

Note: With newer adapters, a connection can be made directly between devices via *Wi-Fi Direct*, which uses peer-to-peer networking regardless of whether the adapter is connected to a regular Wi-Fi network. (Apple calls its version of Wi-Fi Direct *AirDrop*.)

Note: You might have heard of *ad hoc networking* or *computer-to-computer* connections. This was a very early method of letting computers create a Wi-Fi network among themselves. It's been entirely replaced with the personal hotspot approach on computers and mobile devices.

Wi-Fi Spectrum

When wireless transmissions—originally the code popularized by Morse for telegraphy—were new in the 19th century, many variations of this explanation tried to help people conceptualize it: Imagine a very

long cat with its head in Los Angeles and its tail in New York. If you pull its tail in New York, it meows in Los Angeles. Wireless telegraphy is exactly like this, except *there is no cat*.

Note: The cat metaphor is often attributed to Einstein, but he probably didn't coin it. The Quote Investigator has the full history.

Wi-Fi is just like a wired network except, *there are no wires*. Wi-Fi was designed to work just like any other networking method, but relies on data encoded into radio signals instead of electrical impulses passing through wires. In fact, the original name of the trade group that came up with the Wi-Fi name was the Wireless Ethernet Compatibility Alliance or WECA. (And, yes, there are cats—in the form of photos—sent over many Wi-Fi networks.)

Wi-Fi networks use *unlicensed spectrum,* so called because regulatory agencies allow license-free use of those airwaves by everyone in a given country. In contrast, cellular telephone companies pay huge amounts for the exclusive geographic rights to certain frequencies.

Note: In the United States, Australia, Japan, South Korea, and most of Europe, Wi-Fi uses truly unlicensed spectrum. However, some other nations that allow Wi-Fi may require a license. For example, you might need permission if you're a business or if you want to use Wi-Fi outdoors. Check with the manufacturer of your gear and the regulator in your country to see if licensing is required.

Spectrum *bands* are defined ranges of frequencies with a beginning and ending point. Bands are further divided into smaller portions called *channels,* which allow many devices to use the same band within "hearing" distance of each other, ideally with little or no overlap across bands. Because unlicensed bands are intended for broad use by individuals and businesses, there's no guarantee that interference won't reduce your speeds.

The rule is that in these unlicensed bands, devices use relatively low signal power, but that means signals can be hard to differentiate from background noise and other networks. This requires the devices to be

robust on the receiving side: they use a lot of tricks and techniques to pull out usable data from these very low power signals. Much of the improvement in Wi-Fi over the last decade has been improving technology to allow data to pass at high throughput rates even in highly congested areas.

In the United States and in most countries, three distinct bands are available for use, the 2.4 GHz (gigahertz), 5 GHz, and 6 GHz bands.

Note: Starting in 2021, countries began allowing the use of the 6 GHz band, starting mostly in the United States and the European Union. Now, it's widely available except in Africa and most of Asia.

The precise frequencies and channels vary enormously by country. Each band requires a different radio system. Hardware that can communicate in two bands has two radios, three bands needs three radios, and so on. A three-band radio might support 2.4 GHz and have two different 5 GHz radios; or it might have a 2.4 GHz radio, a 5 GHz radio, and a 6 GHz one.

Note: The 900 MHz (megahertz) band is also unlicensed in the United States, but it is not employed for wireless local area networks (WLANs). The 1.9 GHz band is used by newer cordless telephones.

Even after the introduction of 802.11n (now labeled Wi-Fi 4) and for years afterward, many gateways and routers either worked on a single band or required rebooting to switch among bands.

Almost all modern Wi-Fi gateways have the capability to handle more than a single band. A few very cheap gateways and extenders still have one-band-at-a-time dual-band support. But gateways that simultaneously handle data over both 2.4 and 5 GHz bands have been the standard for several years. (Many devices with 6 GHz support are still dual-band: 2.4 GHz in one radio and 5 GHz and 6 GHz in the second radio.)

Many Radios in Mesh Nodes

Mesh networks, described in Build a Mesh Network, offer simultaneous 2.4/5 GHz dual-band networking, but some models also have an additional radio that uses a separate 5 GHz or 6 GHz channel devoted entirely to communicating with other mesh nodes. And some regular, non-mesh Wi-Fi gateways now include three Wi-Fi radios to improve throughput. I discuss this further in Pick Wi-Fi Network Gear.

Early adapters had a similar limitation: they started out as single band, almost always 2.4 GHz, but shifted over time to support either the 2.4 GHz or 5 GHz band, automatically switching without a restart or other configuration. Early mobile devices, like the original iPhone and Android phone models, only worked over 2.4 GHz.

Now, you'd be hard pressed to find Wi-Fi that supported just one band built into a modern mobile device, gaming system, Internet of Things (IoT) gadget, or desktop computer.

For more on 2.4, 5, and 6 GHz bands, see Spectrum Trade-Offs.

Note: In 2022, 6 GHz radios—part of Wi-Fi 6E—began to appear in consumer hardware, like iPhones and home gateways. It's now in wide use.

Warning! Many manufacturers sell specific hardware for each country or regulatory domain in which they do business, or have settings in the router's configuration that require you pick the country in which you're using the network. Because laws vary, it's crucial that you don't take an access point from, say, the United States to France and turn it on. You could wind up facing fines and even jail time.

Wi-Fi Standards

Wi-Fi standards rely on a series of specifications created by the IEEE, the Institute of Electrical and Electronics Engineers's 802.11 wireless LAN group. These use letters, like 802.11n or 802.11ax, to differentiate

among them. It's useful to understand the standards because you will encounter their names repeatedly, often without any explanation, in gateway admin interfaces and elsewhere.

The Alphabet Soup Was Eaten

Each lettered 802.11 standard refers to a task group within the larger working group. Only some define data rates. In the past, some task groups were convened for security or automatic coordinated channel switching. This meant you could buy an 802.11g router that came with 802.11e, 802.11h, and 802.11i. Fortunately, later data rate standards swept in separate initiatives as a single lettered name.

The Wi-Fi Alliance, a trade group, builds tests based on the 802.11 standards, and then allows the Wi-Fi trademark to appear on equipment that passes. These tests allow the many makers of Wi-Fi hardware to ensure that all Wi-Fi adapters and routers, regardless of manufacturer, can communicate and carry out a common set of tasks in the same way.

In 2018, the alliance cut through the confusion of numbered names and generations by numbering Wi-Fi more simply as Wi-Fi 4, Wi-Fi 5, and Wi-Fi 6. These labels now appear on products and are intended to describe backward compatibility broadly. A device with Wi-Fi 6 can connect to a gateway that supports Wi-Fi 4, 5, or 6; a device with Wi-Fi 4 can connect to a device that supports Wi-Fi 4 or later.

The addition of the 6 GHz band, however, complicated this simplicity. The Wi-Fi 6 label sweeps in the new inclusion of the 6 GHz band in some devices; the 6 in both is merely coincidental—and confusing. As a result, the Wi-Fi Alliance had to break their pattern and deploy the term Wi-Fi 6E to refer to "Wi-Fi 6 devices that include 6 GHz support." Harmony returned with Wi-Fi 7, which incorporates everything in Wi-Fi 6E plus new improvements in throughput and other features.

Note: The Wi-Fi Alliance has separate names for technology that crosses many generations, like Wi-Fi Protected Setup (WPS), Wi-Fi Protected Access (WPA), and Wi-Fi Direct.

Here's an explanation of how the Wi-Fi numbering system maps to the 802.11 standards, from the oldest version you're likely to see available for purchase to the latest:

- **Wi-Fi 5 (802.11ac):** Wi-Fi 5 can achieve multi-Gbps throughput with high-end consumer and business devices alongside the right network adapters. However, this standard works only in the 5 GHz band, leaning on the older 802.11n/Wi-Fi 4 (see sidebar below) for handling 2.4 GHz channels. Wi-Fi 5 was split into two releases because some features weren't ready for deployment at its intended introduction: "wave 1" and "wave 2," appearing first in 2012 and 2015, respectively. Wi-Fi 5 is good enough that companies still sell equipment that use it.
- **Wi-Fi 6 (802.11ax):** Unlike 802.11ac, Wi-Fi 6 isn't limited to one band—the 802.11ax standard covers both 2.4 and 5 GHz bands. This revision, which debuted broadly in 2019, allowed hardware makers to increase throughput dramatically yet again through several techniques, some of which hadn't appeared previously in Wi-Fi. Some access points became capable of more than 10 Gbps of throughput—faster than any home wired network. For home users, it's intended to speed streaming video from multiple video players to multiple recipients or TV sets at once. It also allows mobile devices to send and receive data simultaneously from a gateway, improving throughput.
- **Wi-Fi 6E (802.11ax):** Also part of 802.11ax, Wi-Fi 6E makes use of spectrum made available in 2021 in the 6 GHz band in the United States, the European Union, and several other countries. The throughput is higher (as in all of Wi-Fi 6) compared to Wi-Fi 5. But the real advantage is that the 6 GHz band in Wi-Fi 6E allows for many, many more wide channels than in the next best option, 5 GHz. Have more channels makes it far more likely you can avoid interfering with neighbors and run multiple routers in a home or business that don't step on each other while using the maximum available bandwidth. (For more on why wide channels are a big deal, see What's a Wide Channel?, ahead.).

- **Wi-Fi 7 (802.11be):** There's always another generation of Wi-Fi in the wings, and 802.11be promises rates of up to tens of gigabits per second with extremely low latency by doubling the maximum channel width of 802.11ax in countries that have spectrum bands with enough capacity in 5 GH or 6 GHz. The Wi-Fi Alliance formally announced the release of Wi-Fi 7 in January 2024, although some routers appeared in 2023 with "precertified" versions.

With these names and numbers in mind, let's look into what equipment fits your needs for a new network or an upgrade.

Older Standards You Likely Won't See

Wi-Fi has gone through so many transformations, the original standards are fully left by the wayside. For historical reasons—or in case you encounter any of the below—here's how they worked:

- **802.11b and 802.11a:** The original flavors from 1999 functioned only in the 2.4 GHz band and 5 GHz band respectively. 802.11b carried up to 11 Mbps and 802.11a, 54 Mbps. It's rare to find either version in use, particularly 802.11b.
- **802.11g:** Released in 2003, this somewhat faster version of 2.4 GHz networking was coupled with a security improvement, and a top rate of 54 Mbps. You may find quite old hardware that relies on 802.11g, but it lacks compatibility with later security requirements for password-protected networks, so it has fallen away.
- **802.11n (Wi-Fi 4):** Much faster than 802.11b and g, this version appeared widely in 2007, and could use either band. Configured to the max, 802.11n can peak at 450 Mbps in 5 GHz and 225 Mbps in 2.4 GHz. You're most likely to find 802.11n built into outdated and inexpensive devices, like network extenders.

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.

- **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.

Note: In the next chapter, I discuss radio issues, like how to determine the best channel to use in each frequency band.

When you walk around with a cell phone, the number of bars varies, depending on the strength of signals your phone is receiving from nearby cellular network transmitters. It's the same situation over a much smaller space when you connect a computer to a Wi-Fi gateway. Depending on where you place access points, their signals may or may or not penetrate walls or floors with enough strength to be useful (**Figure 6**).

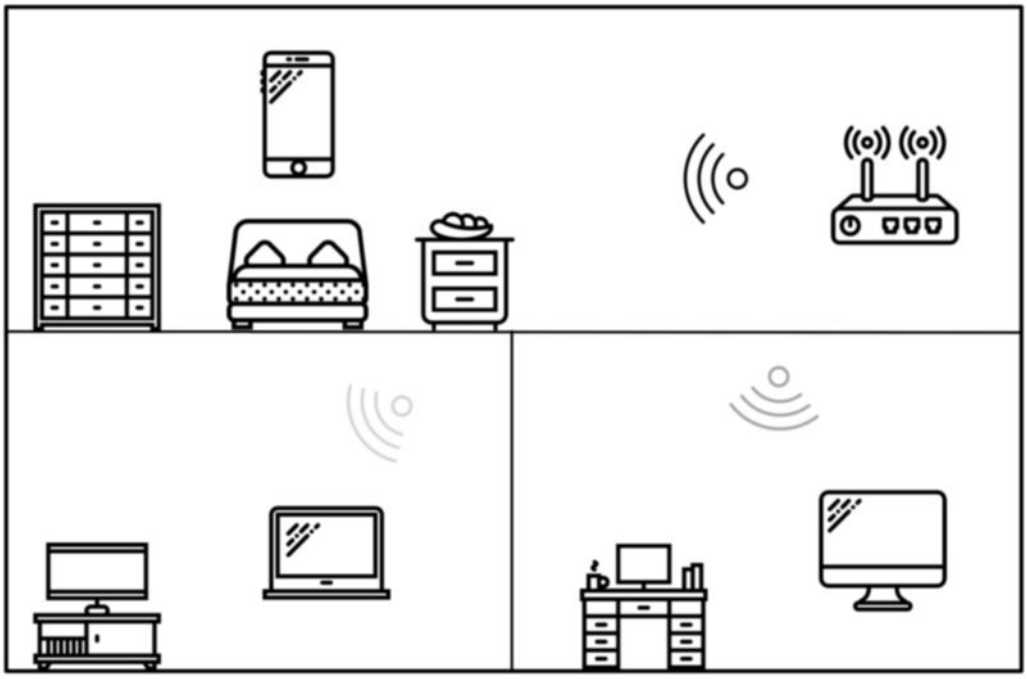


Figure 6: Wi-Fi signals pass through walls and floors more weakly than they do through open space.

Note: Some manufacturers include a smartphone app that helps you figure out where best to place access points. This is more common with mesh networks, but you may also find it with standard Wi-Fi gateways.

When you position your standard gateway or mesh router, consider these factors:

- **Does your broadband hookup constrain where you locate the main gateway that must plug into the broadband modem?** Many of us have phone or cable connections in non-ideal locations—like a basement or near a far corner of a front room—for locating a Wi-Fi gateway. You might turn to a nifty method of running data over your home electrical system—powerline networking—or even run an Ethernet cable through the walls. Both options are discussed in Connect via Ethernet and Alternatives later in this chapter, and both would let you place your gateway farther from your broadband modem. But the harder it is to add Ethernet, the more likely mesh suits your needs.
- **Where do you want to use Wi-Fi?** Do you want to work in your backyard? Upstairs and downstairs? If you're sticking to just one floor or maybe two, you might be able to manage with a single gateway instead of multiple gateways or a mesh system.
- **What obstacles might block your signal?** Walls, ceiling, floors, and even your metal exercise bike can all absorb and reflect Wi-Fi signals, reducing their range and quality. The thicker the walls or the more dense the building material (like plaster, brick, and stone versus drywall and studs), the more trouble you'll have with signals getting through.
- **Will your location be less than ideal for the band you need to rely on for coverage or distance?** 2.4 and 5 GHz/6 GHz networks perform differently over distance at the same signal power, which typically corresponds to better range and coverage in 2.4 GHz and better throughput in 5 GHz/6 GHz. Can you get the faster higher-frequency signals where you need them, but have the coverage of the 2.4 GHz network for the rest of the area in which you want service (**Figure 7**)?

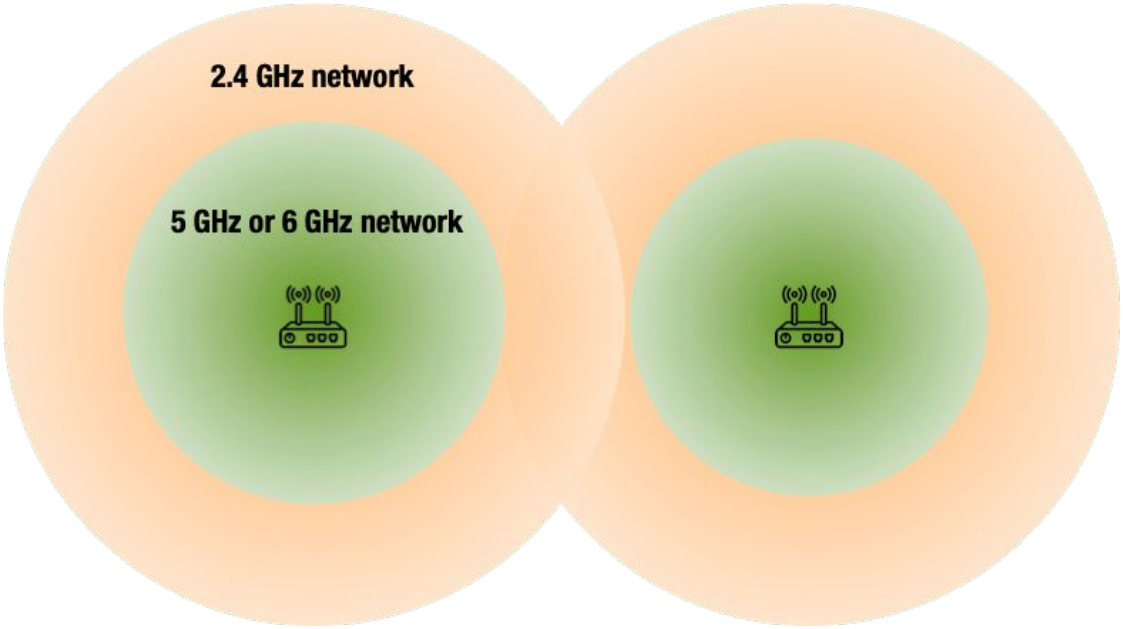


Figure 7: 2.4 GHz networks have greater coverage areas, but 5 GHz and 6 GHz networks provide higher throughput.

- Do you need a super-fast network? Instead of an inexpensive (sub-$100) Wi-Fi 6 gateway with one 2.4 GHz and one 5 GHz radio, you might opt for a more expensive (around $200) Wi-Fi 6 gateway with one 2.4 GHz radio and *two* in the 5 GHz band, or even a Wi-Fi 6E tri-band model with 2.4, 5, *and* 6 GHz radios, claiming a maximum throughput of 8 Gbps across all its radios running full blast.

Don't Spend Extra for Wi-Fi 6E or 7 Without a Purpose

While you can buy routers with Wi-Fi 6E or 7, you won't get better performance from your existing devices unless they include adapters that handle the 6 GHz band or the improved throughput algorithms built into hardware for Wi-Fi 7. Even if you have hardware with the right support, consider whether you're either moving terabytes of data inside your network each day or streaming continuously at 1080p or higher. Wi-Fi 6 might more than suffice for now.

After purchasing hardware based on recommendations in the next section, pick a spot near the middle of where you want your signal to reach and test if it's a good location for your gateway. Make sure the top part of a Wi-Fi 5 or later gateway isn't obstructed: it should have a clear line of sight around it, and not be inside a cabinet or behind a computer.

Then proceed around your home or small office and see if you can achieve the performance and coverage you need:

- If you're relying on wireless connections—called *backhaul*—between mesh nodes, it's an easy matter to move the units to where you want and try again, especially using planning tools that come with the hardware.
- For standard networks, you may have to purchase longer Ethernet cables or go get more gear to meet your needs.

With this in mind, let's look first at standard networks and then at mesh networks.

Build a Standard Network

The kind of Wi-Fi network most of us are familiar with relies on individual gateways and extenders. With these models, you typically have to configure everything from scratch for each unit, determine optimal placement, and figure out how to connect them—typically via Ethernet wiring.

These networks also work best if you have a small enough footprint to get by with a single Wi-Fi gateway. If you can use just one, modern gateway—with Wi-Fi 6 or later and superb throughput—it can be very inexpensive.

If you need more than a single gateway, however, standard networks can get complicated, making mesh more appealing and potentially not much more expensive for comprehensive coverage—plus taking less of your time to set up and run.

Note: Pulling all this together doesn't have to be hard, but it may be more work than you want, which is why I often refer people at this stage to mesh networking; see Build a Mesh Network. However, if cost is your principal concern or you're not concerned about how difficult set up may be, read on.

Understand Wi-Fi Network Devices

You might wind up using a mix of two kinds of Wi-Fi devices while setting up a standard network.

Gateway

A gateway combines an access point, network router, and an Ethernet switch. (Almost no gateways omit an Ethernet switch.) It's an all-in-one solution, has the best coverage and throughput, and many homes and small offices may need just one per network, placed near the broadband modem.

A gateway can cost well under $100; midrange models run around $150 to $250; and high-end gateways can cost as much as $700.

The difference between the cheapest and most expensive? Typically, it's the alleged top speed measured by the number of radios and simultaneous streams (see Multitask Across Space and Time) and maximum Ethernet throughput (see Use Gigabit Ethernet). Units with less throughput cost less.

Range Extender

Range extenders (**Figure 8**) typically lack the routing features of gateways—they're focused, instead, on access point features. They sometimes include an Ethernet port or a two- or three-port switch.



Figure 8: A range extender, like this roughly $50 TP-Link RE500X, has fewer features than a gateway, but offers Wi-Fi 6 coverage.

Most of them are designed to connect as a sort of fake *client* to a full-featured gateway and relay access to other Wi-Fi devices. However, many offer an access point mode, in which you plug them via Ethernet into an existing network where a gateway provides all the network and internet features—the extender just handles Wi-Fi. In both cases, extenders can pass DHCP requests, use the same network name, and employ the same security method and key. Some let you configure unique details (like a unique network name or security key), but that defeats the usual purpose of making a roaming network grow larger.

In either, mode you can use a range extender with any network hardware as no special configuration is required to work as a client or to extend over Ethernet.

Extenders cost in the range of $20 for Wi-Fi 4 to $75 for Wi-Fi 6. However, extenders wind up re-broadcasting the same data over the air, because they relay it, and thus reduce your throughput. I highly recommend instead either an Ethernet or powerline connection (see Connect via Ethernet and Alternatives for details).

Picking the Right Hardware

There's no one right answer here, although unfortunately there are a lot of wrong answers. Companies introduce new models at an absurdly frequent rate while sometimes abruptly canceling popular ones. As a result, here are the guidelines that I follow instead of providing exact model recommendations:

- **Find reviews on sites you trust:** I've worked for and with Wirecutter (part of the New York Times); IDG publications TechHive, PCWorld, and Macworld; TidBITS; and Six Colors. You may have other sites you read regularly and find their reviews match up with your experience.
- **Wait for maturity:** Don't buy the newest, just-released device until there's been time for people to find out if it has flaws in general use, and for early bugs to be fixed through firmware updates. Wirecutter does a great job of follow-up, re-testing devices as new

ones come in and listening to its users' experiences to guide revisiting recommendations.

- **Check customer reviews on Amazon and other sites:** Beware of manufacturer-paid positive reviews of their own products and "hit" reviews of competitors. You can often smell these out on your own, as they are brief, use the same text across multiple reviews, and stand out. But you can also check Fakespot and ReviewMeta. I also look for at least dozens, if not hundreds, of reviews.
- **Avoid unreviewed products:** If a product has good Amazon and other site reviews, but *none* at major review sites, I avoid the product. While it's great to give unknown brand names a chance, we live at a time when weak products are repackaged and sold under hundreds of company names with poor customer support, a high failure rate, and no firmware upgrades for security flaws or other problems. If you're determined, use social media to find people who have purchased an item and see what their experience was.
- **Check for security updates:** It's not a stretch to think your Wi-Fi device could be turned into a zombie attack bot running attacks against other people or companies, or your network could be compromised. As a result, it's very important for any product you buy to have a history of security updates: check the device's support page to see whether any updates were released, why, and how recently. Gateways use stripped-down, custom-purpose, embedded operating systems that typically can only be updated if the manufacturer continues to provide support. In the past, many gateways have suffered from significant security flaws, and only some received firmware updates.

Wirecutter regularly updates its round-up of Wi-Fi gateways. (It describes them as routers, shorthand many people use, but networking router is one *feature* of a Wi-Fi gateway.) In its latest update in August 2023, Wirecutter recommended the TP-Link Archer AX55 ($120), which has a top raw speed of 3 Gbps across its two frequency bands. Wirecutter found in testing it could push 400 Mbps over 15 feet through one wall and over 140 Mbps across 50 feet through four walls.

Now, on to ways to connect multiple pieces of network hardware.

Connect via Ethernet and Alternatives

Newer houses and apartments often feature Ethernet wiring in the walls or you may have added the wiring yourself. Small offices that are reasonably recent may also include Ethernet jacks.

Ethernet is always the best course for connecting base stations in a standard network, as you'll achieve the greatest possible speed without compromise among Wi-Fi gateways and other network components.

If you don't have Ethernet wiring and can't install it, you've got a strong alternative in powerline networking, discussed after Ethernet; see Try Ethernet Alternatives.

Use Gigabit Ethernet

Gigabit Ethernet is cheap, and modern gateways offer it, though not all extenders. Check what kind of Ethernet wiring it is:

- If it's labeled Category or Cat5E or Cat6, you're fine. (It might even have a higher number.)
- If your cabling is marked Cat5, you will likely be unable to use 1 Gbps Ethernet reliably. You should look into whether you could pull new wiring to replace the older, which can be relatively easy if the wiring is in conduits.

Pair your Cat5E or better Ethernet backbone with Cat5E or better patch cables—the cords that go from the wall into a port on a device. Otherwise, you'll find yourself having erratic network performance. Many people I've talked with in recent years saw a huge performance increase over Ethernet by getting a higher category of cable! (Don't get talked into gold-plated cabling—there's no advantage!)

Tip: Need to learn more about Ethernet and cabling types? Check out my book *Take Control of Untangling Connections*. It's all about peripheral and network jacks and plugs, including Ethernet.

For homes or small offices without Ethernet, if you have blank outlet covers that don't have electrical wiring pulled to them, you can typically reuse those for Ethernet jacks. And while it's best to feed Ethernet wiring into crawlspaces and out of sight, the advantage of gigabit throughput might overwhelm your aesthetic needs, and have you running wires across the floor or behind furniture.

Remember that Ethernet relies on a hub-and-spoke topology for best performance: you need to bring each end of the Ethernet back to a switch, in which each Ethernet connection plugged into it can established up to a 1 Gbps connection with every other device.

Faster Than Gigabit

Some routers include 2.5 Gbps Ethernet ports, useful for Wi-Fi network links that can far exceed 1 Gbps. To make use of 2.5 Gbps, you need an Ethernet switch that includes 2.5 Gbps ports or backwards-compatible 10 Gbps ones. (The 10 Gbps version was initially extremely expensive to add to devices and switches.)

If you really need that kind of throughput, a few 5-port Ethernet switches for about $120 to $140 support up to 2.5 Gbps on all ports. These include the QNAP Qsw-1105-5T and the TP-Link TL-SG105-M2.

However, if you have a LAN switch on gateways around your home or small office, you can also effectively daisy chain, too, as traffic passes among Ethernet ports on the switch in a gateway as effectively as a standalone one.

Let's say you had a long house and needed three gateways, one at each end and one in the middle. You could connect the ones at each end to the one in the middle, and still connect switches and other devices at the far ends, too.

Case Study: My Home's Slender Backbone

When we had a project in our basement to add a guest room, we had our contractor pull Ethernet, as our older house lacked any. With the backbone created, we connected several routers around our house, required because the lath-and-plaster walls reduce signal passthrough. Because our contractor wasn't a network technician, I bought prefab cables and wall plates to snap a connector onto.

This eliminated any wire crimping. To make the wall jack work, we plugged standard Ethernet cables into inline couplers (jack-to-jack) that connected to back of the wall jacks. The front side of the plate presented a standard Ethernet jack for a cable. This is a very inexpensive set of parts—about $10 for the coupler and the wall plate.

Try Ethernet Alternatives

The strongest available alternative to Ethernet is powerline networking, which sends networking signals as encoded data through the electrical wiring in your house. The simplest option is to get a pair of units that have Ethernet jacks on them. You plug one into one AC outlet near one of your network hubs; and then plug another into an outlet near another gateway. Connect Ethernet cables between each gateway or extender and their respective powerline devices. Done! Your home's electrical wiring acts just like Ethernet.

Early generations of this equipment was expensive, insecure, and slow, and sometimes required some electrical fooling around to get it to work across different segments of a home's electrical system. (Older homes may still have wiring that reduces performance, however.)

Note: Without an encryption option, in an apartment building or other shared electrical system someone might be able to sniff your traffic or use your internet connection by plugging in a compatible powerline device!

Fortunately, this improved enormously. Now, powerline devices are cheap, fast, and secure. A pair of TP-Link two-port "2,000 Mbps" adapters—the TL-PA9020P Kit—has a street price of $80 (**Figure 9**).



Figure 9: Powerline devices, like this pair from TP-Link, let you send networking signals securely through your homes electrical wiring.

That's probably far cheaper than the cost and time required to install a similar Ethernet setup in many houses. It's also a great option for renters who can't drill through walls, as well as for people who live in homes with brick or masonry in interior walls.

Your actual performance won't be 2 Gbps across all connections, but it will still be plenty fast. Powerline networking typically shares bandwidth, like Wi-Fi, among all attached devices, as opposed to Ethernet switches, which create unique, full-speed connections among different devices.

Depending on the system, you can add several powerline nodes to attach more computers, entertainment systems, or routers. The total you can use across your home or office varies by system. While there are standards for interoperability, you should read up on compatibility if you want to mix and match among vendors.

Case Study: My House and the Wrath of Lath

During the pandemic, my wife trained to become an ADHD coach and went into practice. Training and client sessions are all by video, largely Zoom, and she herself up in part of our bedroom as her day office. However, we didn't realize how poor the throughput there was.

After trying lots of alternatives, powerline networking turned out to be far easier and cheaper than running wire—and less stressful in an old house full of crumbly and fragile lath-and-plaster walls. A pair of 1 Gbps adapters connecting an Ethernet-backbone wired router in the basement below our bedroom to an outlet where in the corner she set up produced admirable results.

Build a Mesh Network

Mesh networking isn't just another buzzword, but an idea implemented in modern hardware whose time has come. At one point, mesh wasn't ready for use, and was oversold as a solution to municipalities, public-safety agencies, and corporations. The equipment we see today has come a long way, and finally represents a maturation of ideas that date back decades.

Mesh's biggest benefit is that it's easy to use. Instead of worrying about how to design and build your network, you can make loose plans. Buy two or more nodes from the same manufacturer and then use visual, audible, or smartphone-assisted help to place the units in optimal locations (**Figure 10**). Turn them on and walk away.

Let's take a quick look at how mesh works and its pros and cons.

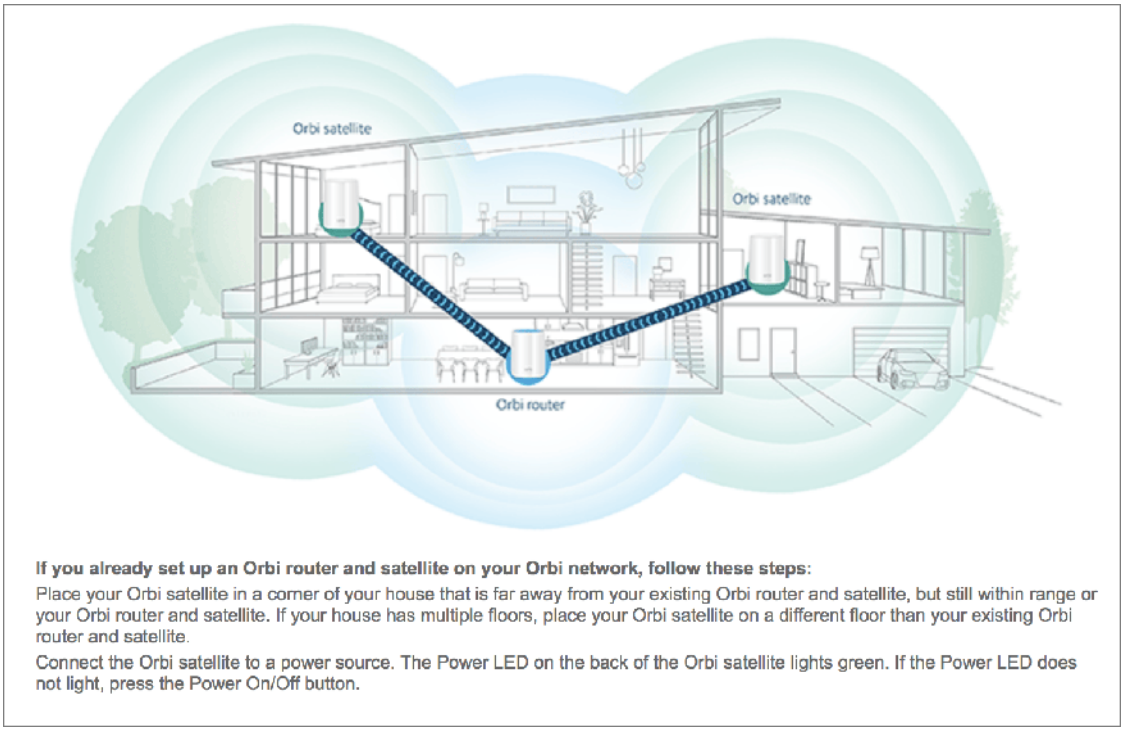


Figure 10: Orbi's administrative interface offers advice on where to place additional "satellite," or less-expensive extender, nodes.

How Mesh Works

Instead of using the hub-and-spoke or daisy-chained approaches of standard Wi-Fi, Ethernet, and other technologies, mesh networks rely on independent nodes. Each node can "talk" directly to any other node on the network. Sophisticated software handles routing data among nodes, which reduces the amount of retransmission of data and other problems that slow down communication (**Figure 11**).

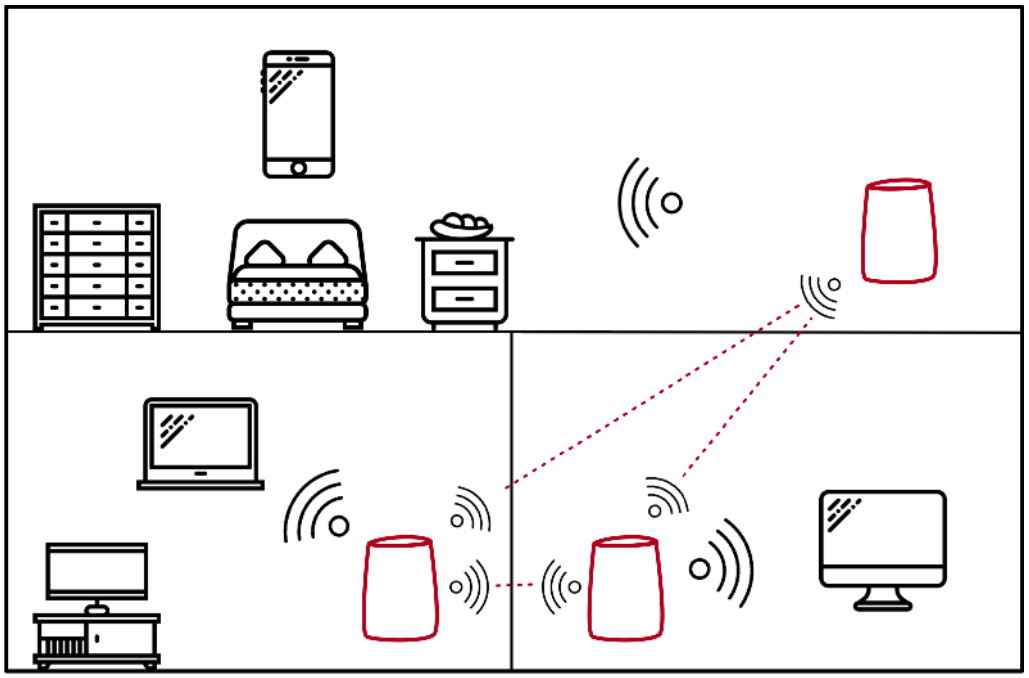


Figure 11: Mesh nodes (in red) can exchange data directly among each other (dotted lines) instead of relaying through intermediates or requiring a central coordinating gateway.

Mesh nodes have three options for *backhaul*, the term for how they shuffle data among themselves, as opposed to handling Wi-Fi connections to and from wireless clients:

- **Backhaul over the same 2.4, 5, and 6 GHz networks used for Wi-Fi with wireless clients.** While today's mesh networks are more efficient than pre-mesh gateway-to-gateway wireless links, this still steals throughput from your network's devices.
- **Add a third radio system devoted to backhaul with other nodes.** This additional radio picks a 5 or 6 GHz channel that's not in use by the node for Wi-Fi for that purpose. This is commonly

called *tri-band*, even though two of the radios might both be in the 5 GHz range, and it might be more accurate to call it *tri-radio*. With the addition of the 6 GHz band, newer tri-radio mesh routers shift all intra-node backhaul to the 6 GHz band.

And, yes, there are even *quad-radio* mesh models! NetGear's Orbi 960 series, for instance. These devices have user-side 2.4, 5, and 6 GHz radios and connect nodes via a fourth radio over 5 GHz. This high throughput is paired with cost: a three-pack is $1,300.

- **Backhaul using Ethernet.** This sounds contradictory! Why use Ethernet with wireless mesh? Because it can add 1 to 10 Gbps of backhaul in places you have Ethernet connections for nodes, and lets you extend a mesh network using a node that's too far away to "hear" the wireless signals of the rest of the network, like in a back-yard cottage or shed.

> **Note:** I mentioned in Wi-Fi Spectrum earlier in the book that each band requires a separate radio. This is also true when simultaneously using separate channels within a band. So a tri-radio router that uses 5 GHz for backhaul devotes two distinct radios to 5 GHz: one for wireless clients and another for intra-nodal data.

Let's look at a detailed list of what mesh networks' benefits are next.

Why to Pick Mesh

Although I wouldn't say that mesh networking is as easy as "plug and play," it does handle many details you'd have to sort out for yourself if you were using a standard Wi-Fi network:

- **Easy configuration:** While you still have to enter some networking values to connect to the internet, a lot of the fussy settings for multi-hub networks just disappears, because they configure themselves automatically.
- **Low-stress device placement:** You don't have to put in a lot of effort to locate nodes, because the hardware and software that come with mesh systems offer varying kinds of help to achieve optimum

results. If you're not using Ethernet with them, you can easily move them if the initial positioning isn't optimal.

- **No-worry changes:** The network self heals if a unit crashes or dies—or a cat knocks its plug out of the wall.
- **Invisible channel selection:** You ignore this entire topic, because mesh network devices silently and automatically handle it on their own. In fact, they have to, because they need to be able to shift among channels based on current needs among all the nodes.
- **Wireless backhaul:** Mesh nodes don't require Ethernet, allowing for the pure joy of wireless connections when connecting them up.
- **Wired backhaul:** While this is the opposite of the previous point, as I note just above, using Ethernet to enhance communication can produce even higher throughput without sacrificing coverage. Some even include "daisy-chained" Wi-Fi, so the nodes don't have to connect Ethernet back to a central switch, but can connect one node to the next.
- **No-sweat adjustments to density and coverage:** Is your Wi-Fi coverage or throughput poor? Did you just add another floor to your house? Buy and plug in more nodes, and everything is magically better.

This all sounds terrific, but let me detour briefly to temper your expectations with some of the drawbacks.

Why Not To Pick Mesh

Mesh networking is still new enough that there are some significant downsides to buying in now, despite the quality of systems on the market:

- **High cost for some versions:** Mesh networking equipment has dropped dramatically in price by 2024 for Wi-Fi 6 systems with two or three radios. However, if you need a lot of nodes or want advanced features, such as tri-radio or quad-radio with 6 GHz backhaul, you can pay over $1,000 for your setup.

- **No mixing and matching:** Mesh devices use proprietary protocols, which means you can't mix and match systems.

Note: A 2018 standard from the Wi-Fi Alliance, Wi-Fi EasyMesh, intended to help push the industry towards interoperability. But I can't see any adoption or movement since it was announced.

- **Company drops product line:** If a maker of a mesh system decides to stop producing equipment and eventually discontinue support, you could be out in the cold if you need to add a node, a critical Wi-Fi security patch is required, or a cloud-based aspect ends. Standalone Wi-Fi gateways and extenders are unlikely to have many of these problems, as the market remains robust for them.

Note: At one point, startup companies dominated mesh networking. They were acquired or disappeared early. The last major independent firm, Eero, was bought in early 2019 by Amazon.

If you're now thinking of purchasing a mesh network, it's time to read reviews at publications I noted above and detailed specifications at the major mesh makers: eero, Linksys, Netgear, and TP-Link.

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.

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**).

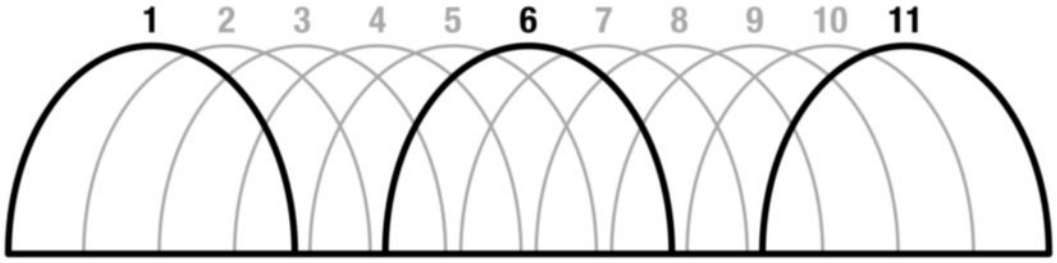


Figure 12: The 2.4 GHz band has overlapping channels, and in America, only three can be used effectively at the same time. (Channel separation exaggerated here for clarity.)

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.

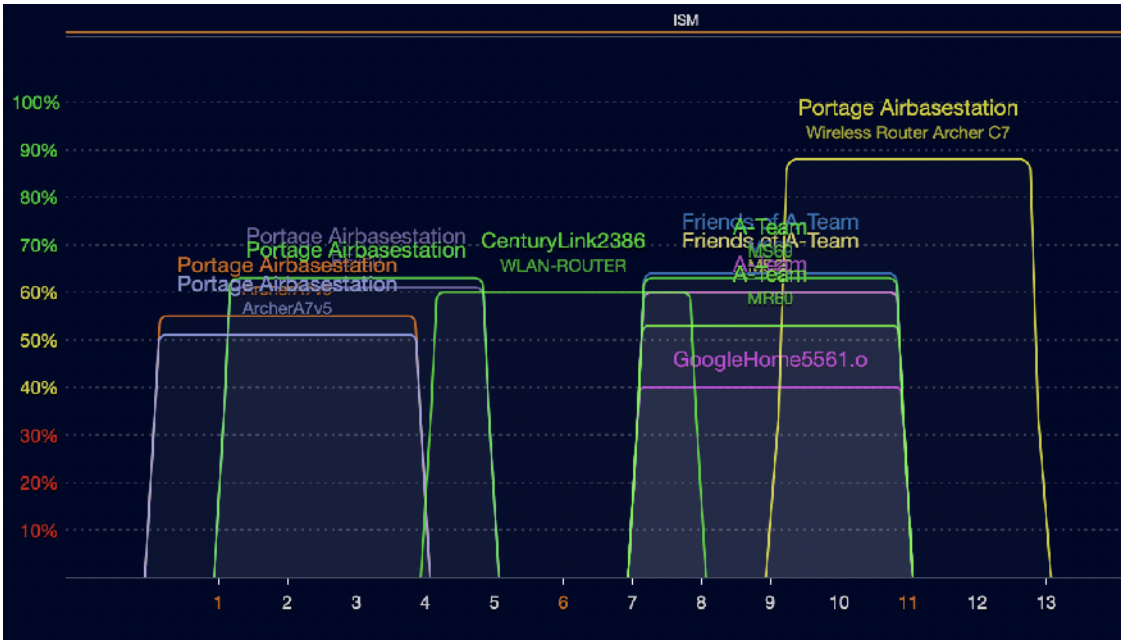


Figure 13: Wi-Fi Explorer shows usage in a busy 2.4 GHz area.

In the 5 GHz band, Wi-Fi standards only use non-overlapping channels, which makes the band easier to work with (**Figure 14**). However, the complexity of channel allocation, division into segments, and the use of wide channels can be overwhelming, as you can see in the figure. The good news? You don't have to manage nearly any of this: the devices (and the protocol) limit the choices you have to make.

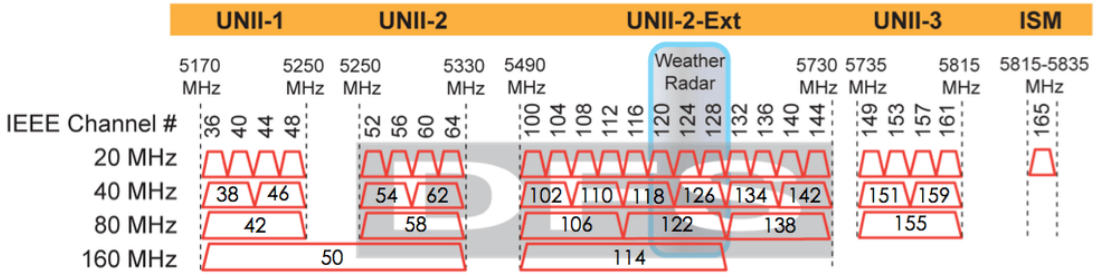


Figure 14: The 5 GHz band looks complicated, but is actually simpler to use. In the first row of the graphic, you see all the 20 MHz channels among which you can choose. The wider channels in the next row are automatically picked. (Graphic by Andrew von Nagy.)

Again, this is much easier to understand with WiFi Explorer's visualization of 5 GHz networks in use around my house (**Figure 15**). In this case, almost all the routers are using 80 MHz channels centered on channel 153 or 157! They appear to occupy the same space, because they span the entire 80 MHz that's available, but would fall back to 153 or 157, if congestion required it.

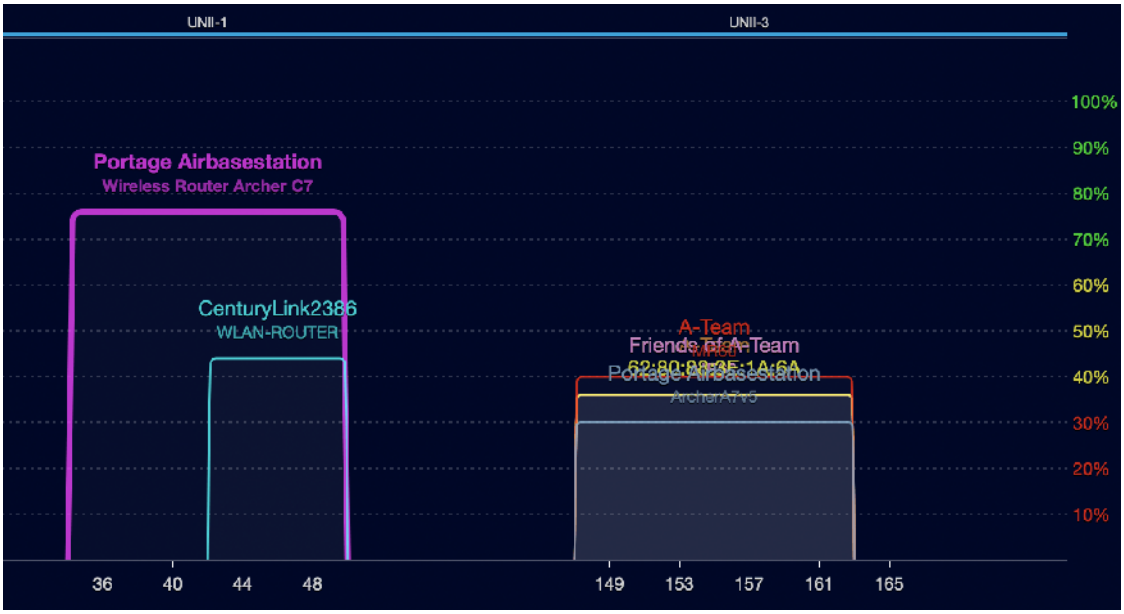


Figure 15: Routers automatically selected a very narrow set of bands to fit the radio needs around them.

6 GHz Band

The 6 GHz band has twice as much bandwidth allocated as 5 GHz in the United States and several other countries—1200 MHz in all! (The European Union and a few others are reserving just 500 MHz.)

Wi-Fi makes use of the 6 GHz band in almost an identical fashion as 5 GHz. But because it's a bigger stretch of bandwidth in many countries, the channel configuration offers dozens upon dozens of regular-width channels and a substantial number of wider channels. **Figure 16** shows how most countries who have opened up or are planning to open up 6 GHz divide it up.

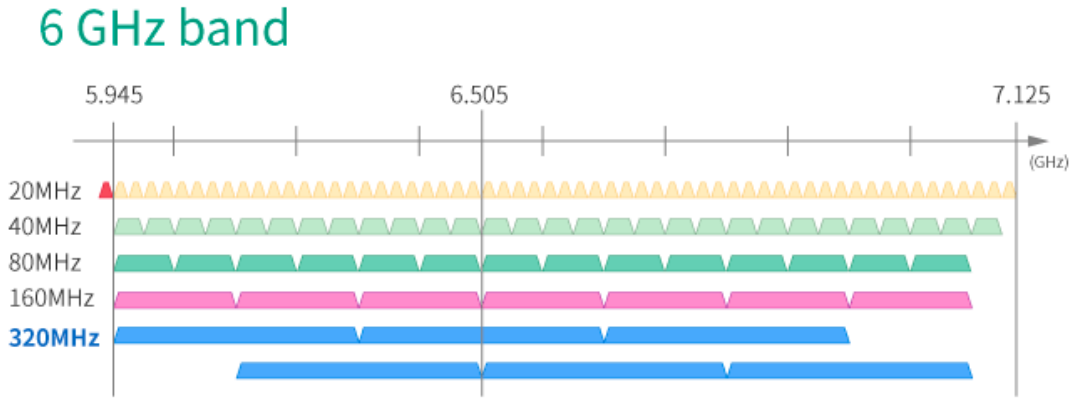


Figure 16: 6 GHz offers a lot of channels. (Source: Anritsu)

Other Uses of Wi-Fi Bands

The 2.4 GHz, 5 GHz, and 6 GHz bands weren't empty before Wi-Fi networking came along. 2.4 GHz is known as a "junk band" because it's full of approved uses that can conflict at times. Industrial sealers, for instance, use heating processes that emit 2.4 GHz radiation.

The 5 GHz band is broken up into several parts with different rules, and some parts overlap with military and other radar uses. Thus, 5 GHz radios are designed to listen for and avoid channels in which they detect such usage.

With 6 GHz, the FCC lists "fixed microwave, radio astronomy, and fixed-satellite operations" as purposes that overlap two chunks. For those pieces, routers have to consult a centralized database authorized by the FCC and use geolocation to determine which channels are available for use in the area it's operating in.

Maximizing Throughput

The 5 GHz and 6 GHz bands offer consistent *throughput*—the amount of actual data passing over the network exclusive of overhead used to transmit it. With 2.4 GHz, however, throughput is all over the place. When other technologies interfere in the 2.4 GHz band, Wi-Fi devices and access points are forced to slow down.

The highest possible Wi-Fi 4 rate happens when a wireless adapter and access point use the 5 GHz band with 40 MHz; the highest WiFi 5 and 6 rates can take place in 5 GHz and at 160 MHz, as well as in 6 GHz at 160 MHz with Wi-Fi 6E—rising to 320 MHz with Wi-Fi 7.

Starting in Wi-Fi 6, a router can individually target subsections of a channel to specific devices, improving efficiency; before that, the router had to devote an entire slice of time in a channel to a device, no matter how much data was involved.

There's another technique for maximizing availability frequencies, too: Multi-Link Operation (MLO), introduced in Wi-Fi 7. Instead of using just a single band at a time, a Wi-Fi router can send a single data stream across two or more radios. This allows more efficient use of all

available spectrum at any given time. (As with other features, both the client and the router have to support Wi-Fi 7.)

Multitask Across Space and Time

Wi-Fi gateways can not only use wide channels, but also transmit multiple streams of data at the same time using techniques that send the data across different spatial paths over the same frequencies as separate *streams*.

Multiple antennas for sending and receiving are required, as well as separate *radio chains*, or all the silicon and hardware necessary to encode and decode data—it's like having multiple access points inside the same gateway.

This technology is called MIMO, for multiple-in, multiple-out, and it's often described in technical specifications for a gateway in the form AxBxC, where A and B are sending and receiving antennas and C is the number of streams, like 2x2x2 or 4x4x4.

MIMO was improved in Wi-Fi 5 (802.11ac wave 2) and Wi-Fi 6 through MU-MIMO (multi-user MIMO), which allows individual data streams to target specific devices, particularly mobile ones that can't pack in the same quantity of antennas and radios as a gateway.

If a gateway can send four streams but a mobile device can only handle one, the gateway is wasting 75 percent of its bandwidth all the times it's sending data to the phone, tablet, gaming handset, or other device. With MU-MIMO, it could transmit and receive from four one-stream devices at once, improving throughput.

This all happens behind the scenes! But it explains how Wi-Fi has been able to dramatically increase its speeds beyond just using wider channels.

Dealing with Distance

Wi-Fi performs at its highest rates the closer you are to an access point. For newer flavors, this can be even more extreme, because they offer their fastest performance only when there's relatively little background noise relative to signal strength. The busier and more chaotic the spectrum between an access point and a wireless adapter—because of other networks in the vicinity or just plain noise in the

spectrum from other kinds of hardware—the worse performance will be. But distance is also a good predictor.

As noted in the previous chapter, Wi-Fi signals can pass through seemingly solid objects, but the fewer walls and cabinets and such, the better. If you can *see* your access point from the device you're using, your throughput is generally better than if you can't. Use that guideline when you're planning the right spot for a Wi-Fi gateway or mesh node.

In practice, you need the best throughput between a digital TV or laptop, tablet, or phone and the source of the streaming media. Most other devices are more "tolerant" of varying levels of throughput or less throughput.

Choosing a Channel

By default, gateways assign channels automatically based on which one is experiencing the least congestion. With modern hardware, you shouldn't have to intervene.

However, there may be occasions or locations when you need to lock your Wi-Fi network on a specific gateway or other device to a specific channel. Read on for those details.

2.4 GHz

The 2.4 GHz channels are numbered 1 to 14, although just 1 to 11 are available in the United States. Channels 1, 6, and 11 are typically chosen in the United States because they lack any substantial overlap with each other. (In countries in which 14 channels are available, 1, 6, 10, and 14 may be used with a little overlap, but not enough to cause noticeable problems.)

What that means in practice is that if you want to control multiple gateways' 2.4 GHz channel assignments, you should lay out your network so that gateways within range of each other use either 1, 6, or 11. If you have three gateways, that's easy! Pick one channel for each. If you have four or more, plan to have gateways that use the same 2.4 GHz channel be farthest apart.

You may also discover terrible performance—bad throughput or lots of network connections dropping—in a given channel. That could be because of some competing 2.4 GHz use, or even an old baby monitor, some of which used to spew out a lot of noise in transmitting audio or video over 2.4 GHz (not using Wi-Fi, but proprietary or analog specs). That might make you choose a channel specifically to lock out that problem.

Note: Beware the many myths about channels. When I had a fiber connection installed a couple of years ago by the local phone company, a remote tech support person said that I absolutely needed to set the 2.4 GHz network to channel 10. There is no reason why that advice should be given in the United States; I was perfectly polite, but went ahead and chose a different channel after I was off the call.

5 GHz

In the U.S., the 5 GHz band offers 25 non-overlapping 20 MHz channels. (See earlier discussion and **Figure 14**.) These are grouped together as adjacent channels:

- 36, 40, 44, 48 (grouped as Unlicensed National Information Infrastructure 1, or UNII-1)
- 52, 56, 60, 64 (UNII-2)
- 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144 (UNII-2 Extended)
- 149, 153, 157, 161 (UNII-3)
- 165 (ISM, a generic term for industrial/scientific/medical)

Tip: Up until 2014, the U.S. restricted the output power of the UNII-1 band to 1/20th of the power available in higher UNII bands. That changed, but if you have older gear, you should keep this in mind when setting channels manually. If you pick 36, 40, 44, or 48, you might be broadcasting at 5% of the potential maximum power.

Because Wi-Fi 4 to 7 can all dynamically stretch from 20 MHz to as wide as to 320 MHz in the later standards, it's unlikely you have a

reason to pick a channel! Only certain channels can gang up with adjacent channels to make these wider swaths, and automatic assignment will be the best unless you have very particular requirements or specific kinds of interference.

Because of certain restrictions in the 5 GHz band to avoid interference with government and military uses in some countries, modern access points automatically move their broadcast channel around—and tell associated wireless adapters to do so, too. This allows for much greater flexibility and interference avoidance.

If you live elsewhere in the world, you'll find that the 5 GHz band is much less available. Some countries allow a small slice of 4.9 GHz spectrum to be used instead.

6 GHz

The 6 GHz band has largely settled down in countries that have agreed to open it up, but there's still a lot of negotiation happening globally as it rolls out. In the United States, channels look like this:

- UNII-5: 24 channels (indoor/outdoor)
- UNII-6: 5 (indoor only)
- UNII-7: 17.5 (indoor/outdoor)
- UNII-8: 12.5 (indoor only)

Note: The reason for .5 in the list? One 20 MHz channels spans UNII-7 and UNII-8, but because the two allocated bands are adjacent there's no gap. So one 20 MHz channel simply cross the boundary of those two names.

Indoor use in 6 GHz comes with power limits to prevent signals from penetrating very far (if at all) outside of a building. Routers operating in low-power mode can't have external antennas attached.

Both indoor and outdoor routers operating in 6 GHz can use power levels similar to 5 GHz in the UNII-5 and UNII-7 bands, but they have to be designed to consult a geolocation-based database authorized by

the FCC to ensure the router doesn't use channels that have competing licensed uses nearby.

Create Distinct 2.4, 5, and 6 GHz Networks

Simultaneous multi-band gateways allow devices that connect to switch among bands as seamlessly as roaming among multiple gateways with the same network name and security settings.

However, you may find cases in which you want to separate your 2.4 GHz, 5, and 6 GHz networks. This used to be more common, because bandwidth was limited enough, even in 5 GHz, that people would want to shunt slower, older, and less-time-critical devices to 2.4 GHz.

Gateways still largely retain this capability of creating two or three networks, separated by band. With a different network name for each band, you can choose which devices connect to which network by name. A device will not roam among bands with different names unless you connect it at some point to each network and let the device store the password for future connections.

Note: It's more likely you would want to separate your 2.4 GHz from 5 GHz or 5 and 6 GHz than separate 2.4, 5, and 6 GHz networks if you have all three. Throughput limitations will hit you most strongly in 2.4 GHz.

Look for a tab or link in your gateway admin software labeled Wireless Networking or Wireless Setup. If you don't see checkboxes and labels for each network, as in this NetGear example in **Figure 17**, click an Advanced Options or Wireless Options button (or consult the manual).

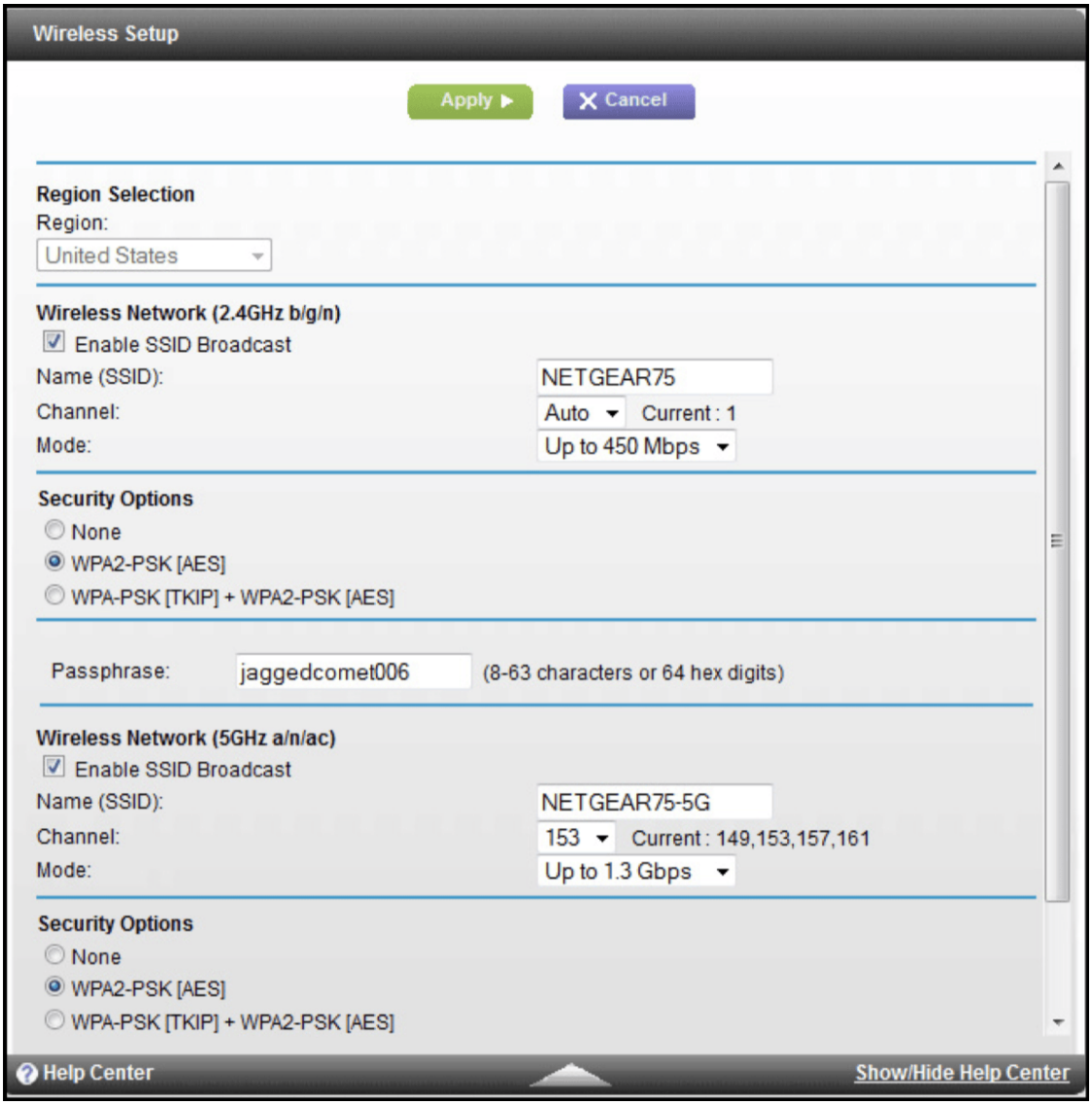


Figure 17: Most gateways let you opt to set different network names for the different frequency bands. (Shown here, a NetGear gateway configuration.)

You typically set up two separate networks in either of these ways:

- In a single view, as in the figure, you name the networks differently by band in separate fields.
- In a single view or a separate dialog, you choose an option from a popup menu or check a box to create separate networks per band.

Once you've named the networks differently (and restarted the gateway if prompted), you can figure out which of your devices should be locked to a given band.

Troubleshoot Your Connections

In Make a Plan, I discussed placing your Wi-Fi hardware. Now that you understand more about spectrum and channels, here's some advice that can help you when your network isn't working as expected. Ask yourself these questions:

- **How fast am I connecting?** Wi-Fi automatically drops down through many intermediate data rates. It starts with the maximum that a wireless client and access point can communicate with using the best standard they both agree on, such as Wi-Fi 5. The devices then drop down through slower and slower speeds until they find a mutually reliable one. You probably are experiencing a problem, for instance, if you have an 867 Mbps 5 GHz network, but you're only connecting at 54 Mbps.
- **What standard is in use?** You might also experience slower connection speeds if the client and access point aren't using the same Wi-Fi standard. The pair might have dropped down to an older (slower) standard, or something might be misconfigured on the gateway or mesh router.
- **How noisy is it?** All radio systems teeter between signal and noise. Signal is useful information, whether it's a human voice or data bits. Noise is chaotic and reduces the quality of the information content. Wi-Fi's signal-to-noise ratio (SNR) and separate signal and noise components may appear in software monitoring tools I describe below. You want as high a signal and as little noise as possible. The SNR defines the space in which information passes.

How Noise Is Defined

Noise and signal are measured in decibels below 1 milliwatt (dBm), which provides a baseline for signal (or noise) strength. You'll almost always see a negative number, because the measurement is *below* 1 milliwatt, thus negative. A better signal number is closer to zero—that is -85 dBm is worse than -45 dBm, because there's more signal present. A better noise signal is further below 0, so -95 dBm is better than -80 dBm, as it means there's *less noise*.

The Bizarre Brick I Bought Two of

Months after upgrading to a TP-Link AX3000 router in 2023, I started having peculiar network failures. I thought the ISP's hardware might be at fault, but after an enormous amount of troubleshooting, I narrowed it down to the TP-Link.

After swapping in an identical unit with the same latest firmware, the same problems occurred! I found some accounts online of people experiencing the issue with no solution. I replaced it with a NetGear R6700AX and have never had a moment of trouble since.

I trust TP-Link's products and still have seven other TP-Link routers, extenders, and powerline adapters on my network that are absolutely reliable. It's baffling.

Testing from Device to Access Point

If you're trying to understand network performance, you must be able to gauge how fast and well network-connected devices are performing.

To check for problems using your computer's built-in tools, first connect to the network. Then, follow directions for each platform:

- **In macOS:** hold down the Option key and select the Wi-Fi menu on the system menu bar. Under the current network, you'll see some salient details like Tx Rate, or transmission rate (the maximum throughput at your current location for your device), and the PHY Mode (the type of 802.11 protocol used). You'll also see RSSI, a form of signal measurement, and noise (**Figure 18**).

  For even more detail, hold down the Option key, select the Wi-Fi menu in the system menubar, and choose Open Wireless Diagnostics. Use items in this diagnostic tool's Window menu to see details. For instance, if you choose Window > Info, you see the same information as in the Option-click Wi-Fi menu. Choose Window > Performance to monitor Wi-Fi performance over time by data rate, quality (a somewhat arbitrary number, the higher the better), and signal to noise.

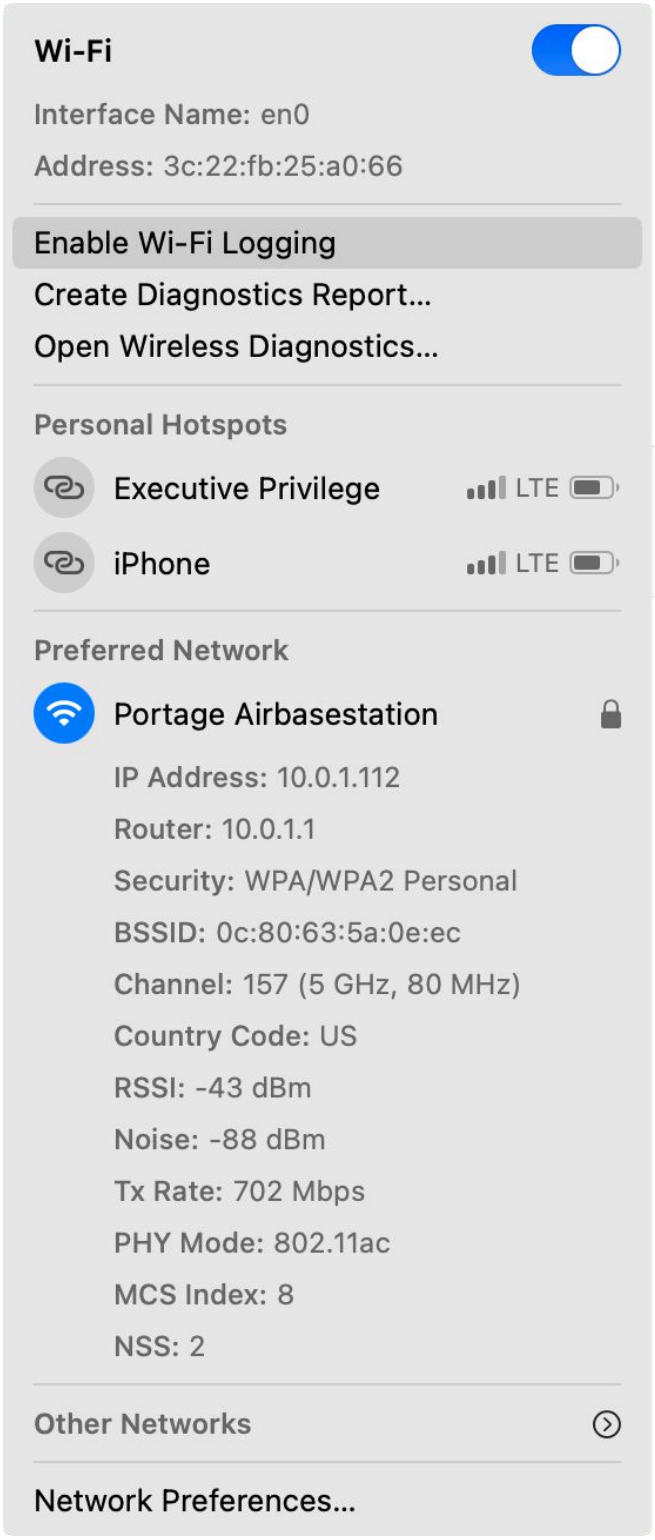


Figure 18: If you hold down Option before clicking Wi-Fi on your Mac's menubar, you'll see a lot of useful information.

- **In Windows 10 or later:** The Wi-Fi status dialog shows the current data rate (**Figure 19**). To find it, click Start, then select Settings > Network & Internet > Status > Network and Sharing Center. Next to Connections, select your Wi-Fi network's name.

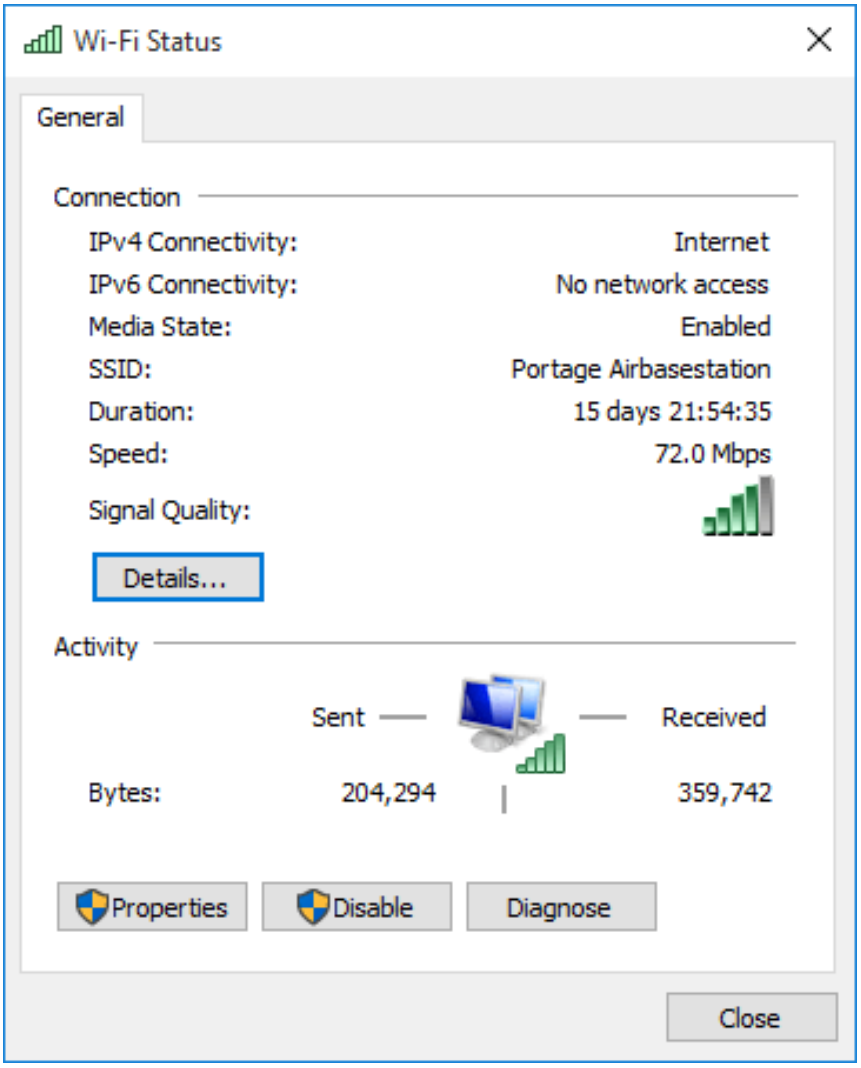


Figure 19: Open Wi-Fi Status via the Network and Sharing Center to see more detail about your Wi-Fi network.

A free and well-reviewed app, WiFi Analyzer, available in the Microsoft Store, provides more detailed monitoring and data.

- **In iOS or iPadOS:** When you're using an iPhone or iPad, third-party apps are the way to go. The folks at NetSpot have compiled a handy list of Wi-Fi scanning apps—including their own!
- **In Android:** Again, the OS offers little insight—just the connection speed if you dig down deeply. Unfortunately, no free or inexpensive apps updated in the last several years seem to provide much utility; turn to NetSpot, described next, which isn't cheap, but has a full-featured offering.

NetSpot Helps with Wi-Fi Planning and Troubleshooting

If you're regularly setting up and monitoring Wi-Fi networks, look into NetSpot. This sophisticated and easy-to-understand Wi-Fi scanning software for macOS and Windows displays data about every access point it can detect, and visualizes channel usage as a physical layout on a map you provide or using other drawing options (**Figure 20**).

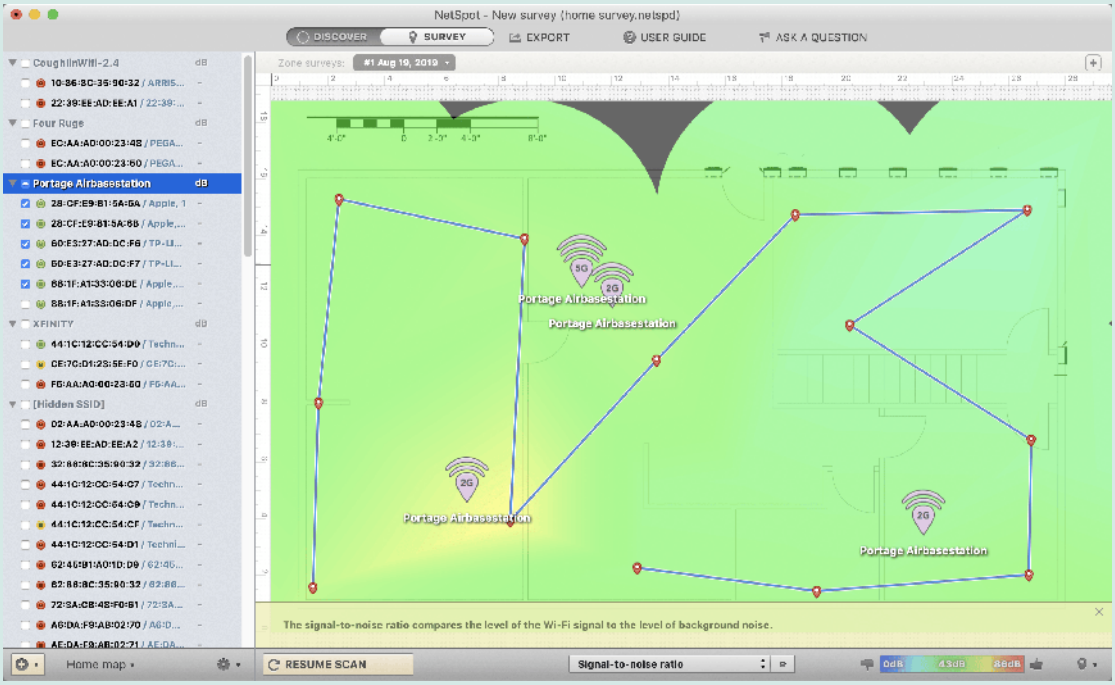


Figure 20: *NetSpot lets you map out coverage areas of an existing network, and see incursions from nearby networks.*

NetSpot has a limited free version, a $49 home version, a $149 pro edition, and a $499 enterprise flavor.

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.

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.)

You'll need to understand DHCP in particular when configuring your gateway to connect to a broadband modem or a larger network, as described next.

The Future of the Internet Is Today? IPv6

As early as the mid-1990s, it was clear that the basic addressing protocol for the internet, Internet Protocol version 4 (IPv4), was inadequate. Among other problems, the *address space*, or the number of potential addresses in the "dotted quad" system of four numbers from 0 to 255 separated by a period (like `36.44.0.6`) wouldn't encompass billions of devices.

The IETF, which handles internet standards, got to work and developed IPv6 (don't ask me where version 5 went to), and released a draft in 1998. It can support handle nearly 3.4×10^{38} addresses, among other improvements. Routers and operating systems slowly incorporated supporting across the 2000s, and ISPs began using it in earnest for their internal networks in the early 2010s.

But for endpoint networks in homes and small offices, you may never encounter an IPv6 address, even though ISPs rely almost entirely on IPv6 and most of the internet besides endpoints employs it. That's due to private-networking address assignment, explained in Hand Out LAN Addresses. A billion local networks reuse the same private IPv4 addresses, which puts no strain on the global system. ISPs tunnel IPv4 traffic inside IPv6 routing without any complications, too.

In configuring your Wi-Fi network or devices, you can effectively ignore IPv6 unless your ISP provides instructions on how to enable it in your router. At some point, it will be ubiquitous and replace IPv4 entirely, but that still appears to be a decade away and holding.

Get a WAN Address

To communicate with the rest of the world, you need to hook the wide area network (WAN) port of your gateway to the internet.

With most networks, especially those in homes, that means connecting to a broadband modem. However, you could also have a network router that provides network services over Ethernet and is already

connected to your broadband modem. In that case, you connect your gateway to any port on the Ethernet network.

Start with an Ethernet cable and plug it into the WAN port on your gateway, which typically has a special label or icon, or is set apart from any Ethernet LAN ports. (Consult your manual or online support if it's unclear.) Connect the other end of the cable to the LAN port of your broadband modem, or to an Ethernet switch for a larger network.

Now that you've made the physical connection, you can configure your gateway to handle the connection. The many different possible configurations can be broken down into two categories: those that use *dynamic addressing* and those that use *static addressing*.

If your internet connection is a home broadband connection, you'll probably use dynamic addressing. You may need to ask your ISP for more information if you're not sure whether they provide you with a dynamic address or not. For configuration details, read Dynamic Addressing, next.

A static address is more typical for small and large offices. For setup information, see Static or Fixed Addressing, a few pages ahead.

Dynamic Addressing

A *dynamic address* is an Internet Protocol (IP) address that is assigned through DHCP, as discussed earlier in this chapter. Dynamically assigned addresses over DHCP can be either public or private.

On a gateway's WAN port, it requests an IP address from the *DHCP server* that's either built into the broadband modem or that's passed through to the modem or via a network router. (The gateway acts here as a *DHCP client*.)

By default, most gateways obtain an IP address as a DHCP client when they initially start up and are connecting to a broadband connection (**Figure 21**).

In some cases, you might need to enter the IP addresses for the DNS servers (Domain Name Service) manually, or you may choose to override ISP-provided values.

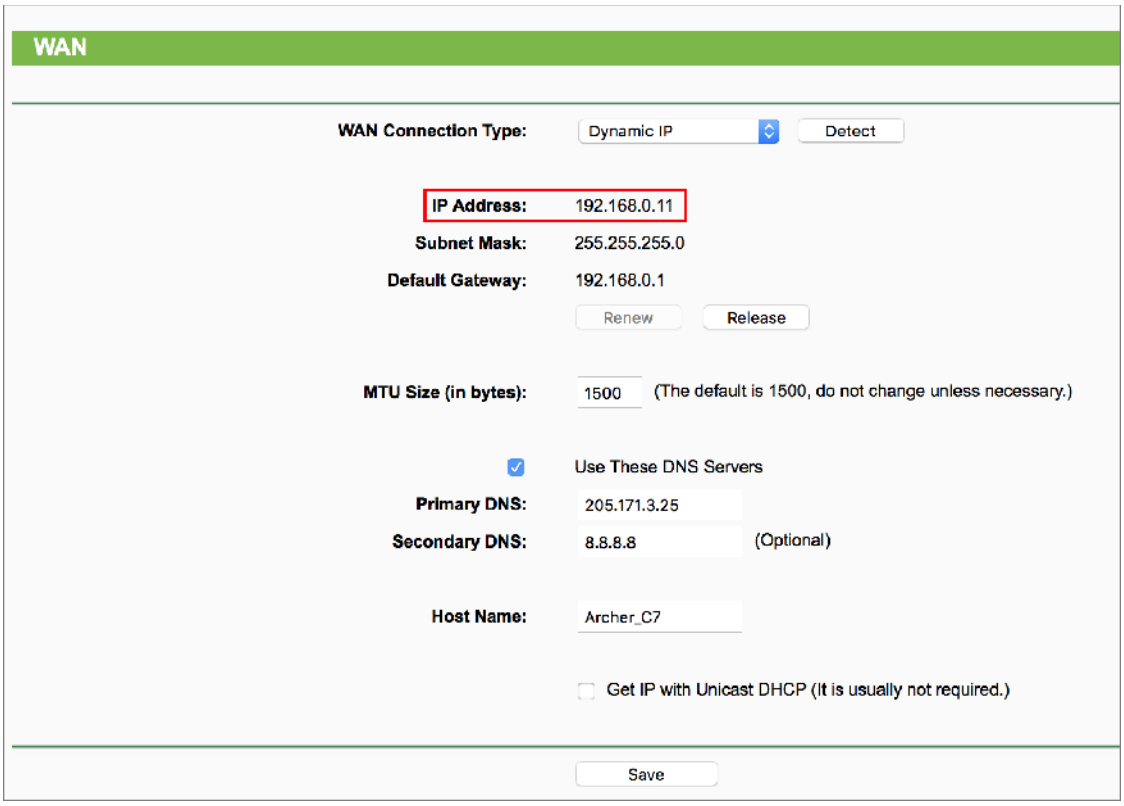


Figure 21: In most cases, your gateway will automatically acquire an address via DHCP (highlighted) for you.

DNS Converts Names into Technical Details

DNS is a decentralized system that lets devices on the internet use human-readable domain names, like `takecontrolbooks.com`, instead of underlying numeric addresses. DNS software takes the name and looks up the machine-usable information, such as an IP address, used to make a connection.

If your gateway obtains its address via DHCP, it likely also gets the ISP's default DNS values. You may want to override these provided servers with other DNS servers by using a so-called *public* DNS services. These include Google Public DNS, Cloudflare (1.1.1.1), and Quad9, all of which are free and fast.

Static or Fixed Addressing

In some network configurations, your ISP may offer you a static address. This could be part of a private network that the company operates or it could be a public IP address.

If the address is from a private network, your gateway (and by extension, your network) may not be easily reachable from the rest of the internet. If it's a public IP, the gateway typically becomes directly reachable by any other point on the internet.

In either case, this static (or "fixed") address gets entered directly into the gateway's WAN network configuration. You typically select either "manual" or "static" address from a popup menu that likely reads "DHCP" or "dynamic" by default (**Figure 22**).

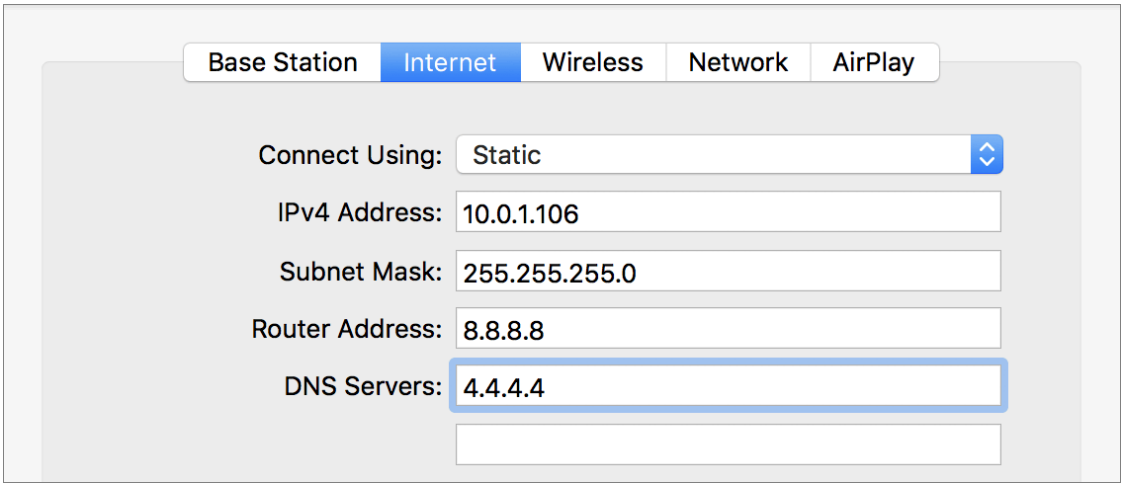


Figure 22: Setting a static address can be as simple as selecting Static from a pop-up menu and entering necessary values.

To set up a static address, you'll need to enter some information provided by your ISP or network operator:

- **The static IP address**: This is the unique network address used by your gateway on the internet or the ISP's network.
- **The subnet mask:** A number full of mystery, the *subnet mask* merely defines the size of the local network that the static address comes from, with "size" expressed as the number of addresses in that local range.

- **The router address or gateway:** This is the address to which any outgoing traffic that's not bound for other machines on the local network is sent. It's then *routed* to higher-level networks, such as a larger office LAN or the internet.
- **DNS server(s):** You need the IP address for at least one DNS server, which handles turning domain names into IP addresses. Two is better; that avoids slowdowns if the first DNS server is unavailable or overloaded.

Hand Out LAN Addresses

With the WAN link connected, it's time to look at your own network—the LAN. The LAN can be configured to assign IP addresses to client computers in one of four ways:

- **Dynamic private addresses:** The gateway uses a single public or private IP address assigned by the ISP and shares that all the machines on the LAN. The gateway assigns addresses to computers on the LAN from a private range; you can almost always modify that range. These addresses rely on NAT for connections outside the LAN. See Dynamic Private Addresses.
- **Dynamic public addresses:** With this setup, your gateway shares multiple, publicly routable internet addresses with devices on the LAN.
- **Reserved addresses:** With this feature, you can assign specific private or public addresses to individual computers on the LAN. See Reserved Addresses.
- **Passthrough and bridging:** You can set up a gateway to let another device on a larger network dynamically assign addresses or allow static addresses, which require no intermediate DHCP server to route traffic to and from the internet. With this set up, the access point doesn't operate a DHCP server at all or manage addressing. See Passthrough and Bridging.

The first option is by far the most common, in which devices on the LAN receive addresses that can change from time to time—whether that's every hour or every few weeks—and which exist solely to give the devices access to the internet. You'd typically use the other options when computers on the LAN side of the network are providing services to other devices on the same network or need to be reached by devices on the internet.

Let's look through each of these in turn.

Note: DHCP works by having a device send a message asking for an address over a network. A DHCP server hears this message and provides an address. The DHCP client configures itself to use the address that the DHCP server provides. The DHCP server assigns the each address to a single active device.

Dynamic Private Addresses

To use a dynamic private address on a LAN, you typically have to set up your gateway:

1. Find the "LAN," "Network," or "Local" configuration section in your gateway's admin interface.
2. Most gateways enable DHCP and NAT by default. If those services aren't turned on, select DHCP/NAT from a popup menu or check a box. (NAT may not be listed, but it's implied.)
3. The DHCP server settings may offer lease options, such as the duration of time that a device can retain an IP address before requesting or being assigned a new one. On most networks, disable the lease period (if that's an option), or set it to as long a duration as possible, like a few weeks.

The DHCP server settings may also let you choose a range of private addresses and how many addresses to assign dynamically. I explain those choices in detail next. You may wind up mixing dynamically assigned addresses with DHCP reservations, explained later in this chapter.

Why To Choose a Different Private Address Range

Some gateways offer the capability to control which private address range is used, sometimes with a lot of options. You might want to use this option if you have network conflicts in which multiple devices are handing out addresses, if you need more than 200 to 250 addresses, or if you just prefer to use something unique.

> **Note:** With more than one DHCP server on a network you can get unpredictable results.

Private addresses are drawn from one of three reserved ranges: `10.0.*.*`, `172.16.*.*`, or `192.168.*.*`. The `*` refers to a number between 1 and 254, although depending on the gateway, you may have a smaller subset available.

These prefixes are reserved by the global numbering authority, and they are guaranteed to not be in use on any public internet network. Depending on the gateway you may be obliged to use only one range. Most gateways default to `192.168.0.*`, although Apple's Wi-Fi base stations default to `10.0.1.*`.

> **Note:** The number 0 at the end of an IP address denotes "the whole network." The number 255 is reserved for *broadcasts*, or data that every device on the private network may receive. Broadcast messages are used for under-the-hood network information exchanged among adapters. Broadcast messages are also used for *discovery*—when hardware like a printer regularly announces its availability to other devices.

The only reason to change the range of numbers is if you want to create and assign *private* addresses that remain static. Otherwise when a computer or device requests an address via DHCP addresses are allotted arbitrarily from a large pool. These statically assigned addresses start with the first three numbers in the access point's private network range, but you enter them manually on each computer. This used to be the only way to create a fixed private address, but now I suggest you avoid this method by using Reserved Addresses, discussed later in this chapter.

Tip: Some gateways let you set a static address for a device without using DHCP as long as the address falls outside a range that the network's DHCP server manages. So, if the gateway controls a block of 200 addresses starting with `192.168.0.1`, you can assign addresses manually and statically from `192.168.0.201` to `192.168.0.254`.

Dynamic Public Addresses

Some ISPs offer public addresses, usually for an extra fee, if you need them for your LAN computers or other devices. This allows each device to be reachable from the public internet without any intermediary address translation. This can be useful for certain kinds of servers and services, even though it enhances risk, because suddenly *anyone*, including *any automated hacker bot,* can reach those devices, too.

Most of the time when you want to use a public IP address, you also want that address to remain static for each computer or device. In that case, DHCP isn't involved at all. However, some networks use public addresses for all connected devices and don't require that each device have a static address. For that scenario, you configure an access point to hand out public addresses from a defined range using DHCP.

Tip: As described a few pages earlier in a tip about Dynamic Private Addresses, in addition to using automatic DHCP assignment, you can set manual addresses on devices on the network outside that range.

Reserved Addresses

Reservation allows a given device on a network to obtain the same IP address, whether public or private, each time it joins the network. This works whether or not you share the access point's connection or distribute a range of addresses, but it does require DHCP service to be turned on.

The reserved address is never assigned to another computer, and if the computer in question restarts or shuts down, the next time it powers up and its network adapter is active, it receives its reserved address.

Reserved addresses work well if you want to connect from the WAN side of an access point to computers, printers, and other devices that are connected via the LAN side.

If your gateway supports DHCP reservation, you have to connect a device identifier with an IP address you've chosen from the pool of addresses used by the LAN. On some gateways, that IP address has to come from an unassigned range. On others, you can pick any address in the private range, and the gateway keeps it in reserve (**Figure 23**).

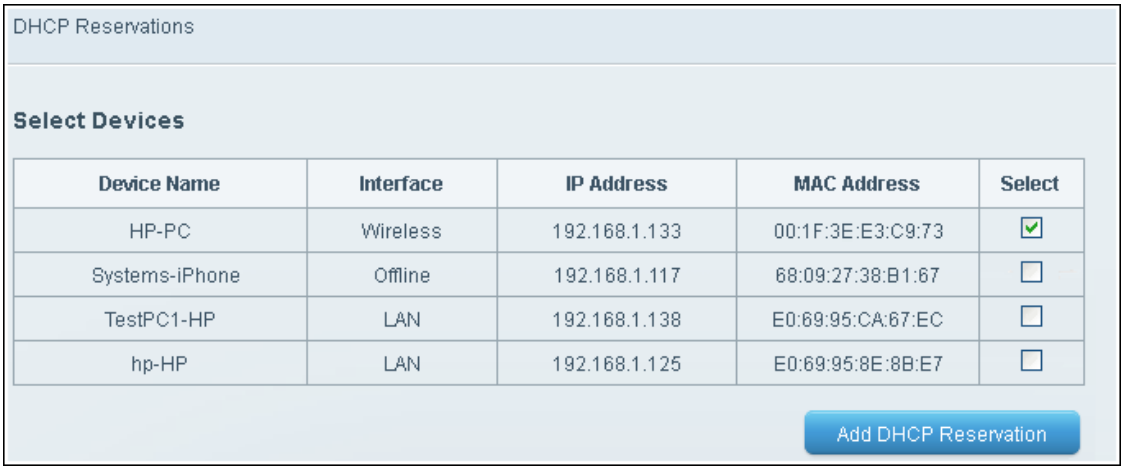


Figure 23: If you want a device to always use the same address, use DHCP reservation. In this Linksys example, you can mark devices and reserve their addresses within the admin interface.

The device identifier is almost always the MAC (Media Access Control) address. This address has nothing to do with an IP address or Macintosh computers. Rather, it's a unique, factory-assigned address attached to every distinct network adapter. If you have a computer with Ethernet and Wi-Fi, those two network adapters each have their own address. It's a set of eight pairs of hexadecimal characters that looks like `81-4F-A1-25-5E-1E`.

Tip: Where you'll find a MAC address varies by device. Since this address is often required for other gateway configuration, I've included a short appendix that gives instructions for finding it on various operating systems and hardware: see Appendix A: What and Where Is a MAC Address?.

Some gateways may allow other information unique to a specific device or operating system. For instance, Apple's macOS lets you specify a DHCP ID as a text identifier in System Preferences > Network under TCP/IP settings.

You may need to restart the access point after setting up DHCP reservations. After you restart, all devices you reserved addresses for receive those IP addresses from the DHCP server.

Passthrough and Bridging

For networks in which the access point is connected to a larger LAN or you rely on a broadband modem that has gateway features, you may already have a DHCP server running that handles address distribution. In many cases, you might be adding Wi-Fi gateways specifically because you want this access point feature.

In any case, you need to disable DHCP and NAT, and allow those messages to pass through. If you leave them enabled, you'll get unpredictable results.

Note: The dreaded *double NAT* is something you want to avoid: that's when your device gets assigned a private address that's routed via a NAT gateway that, in turn, gets its private address routed through NAT. Double NATed networks are often unreachable from the rest of the internet for remote-access services, like remote screen control or smarthome device control.

The term used in each gateway will vary for disabling DHCP and NAT. In some cases, you'll be able to set "DHCP" to "off" via a radio button or button menu. In others, you'll need to select an item that reads "Bridging" or "Passthrough."

When you disable DHCP on the LAN side, gateways will be assigned a LAN network address that's in the same range as the rest of the devices on the LAN.

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.



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.

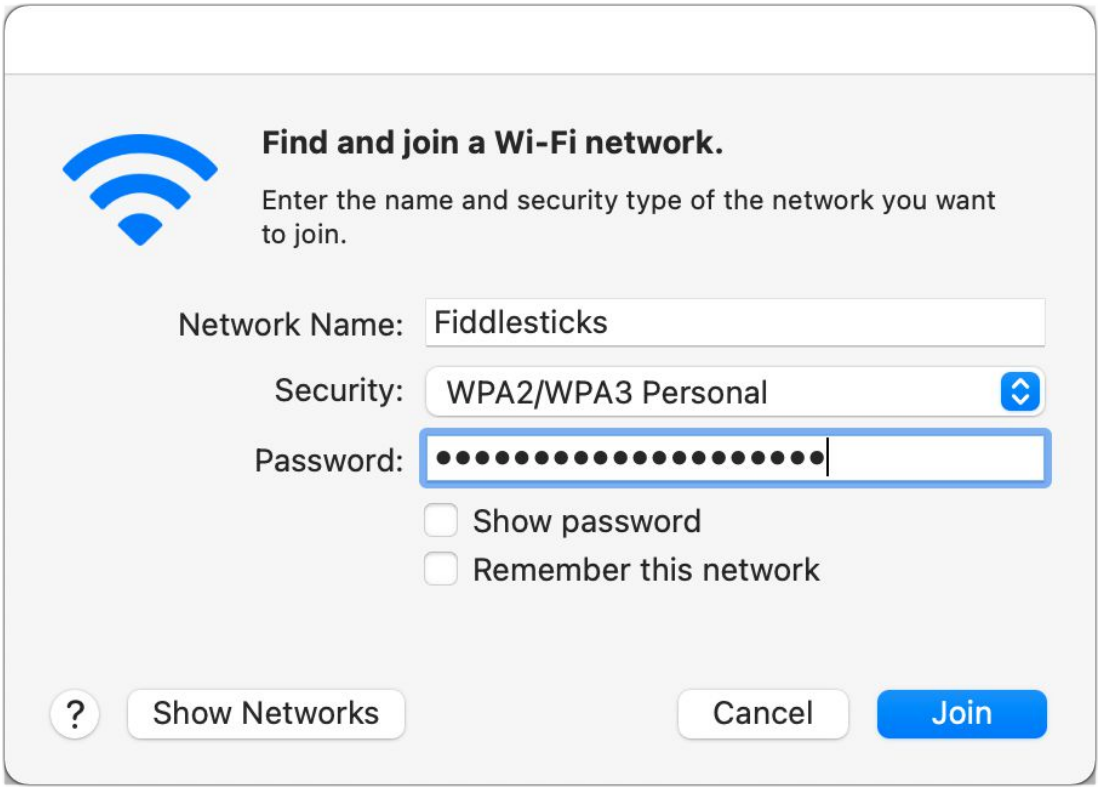


Figure 25: For hidden networks, enter a name and manually choose its security method.

After the connection is completed, the Wi-Fi menu's icon switches from gray to black, with the number of black waves indicating signal strength by their quantity. It switches to two overlapping chain links if you've connected to a personal hotspot.

Although you should now be able to access the internet normally, if the network is an unencrypted hotspot, you may see a floating window that shows a hotspot login screen. After agreeing to the hotspot's terms or entering login details, if the window doesn't close by itself, click Done. This window can be dismissed by clicking Cancel.

Note: If you don't see this window and can't access the internet from the hotspot connection, launch a web browser and try to visit a website. This should cause the hotspot access page to appear.

The next time you're in range of that network, if you've checked "Remember this network" (as noted in the sidebar above), your Mac will automatically reconnect. Here's how to change that:

1. Go to Apple > System Settings > Wi-Fi.
2. Click the Advanced button at the bottom of the Wi-Fi pane.
3. In the Wi-Fi tab, scroll to the network name in the Known Network list.
4. Click the More icon to the right of a network name. If Auto-Join is selected, choose it to disable. it.
5. Click Done when complete.

You can instead click Remove from List in step 4 to remove the network, but then you lose its stored password. You're immediately disconnected. If you delete the entry and use iCloud Keychain, the Wi-Fi network entry is removed from all connected devices.

While still in range, disconnect manually by clicking the Wi-Fi menu and then clicking the blue icon to the left of the currently connected Wi-Fi network. After a moment, it will disconnect and the blue icon will change to gray. Your Mac will not re-join that network unless

you select it again or the device leaves the range of the network and returns. Click the Wi-Fi switch in the Wi-Fi menu to disable the device's network connection entirely.

Connect in iOS and iPadOS

iOS and iPadOS let you join any Wi-Fi network with a few taps. If the Ask to Join Networks option is on in Settings > Wi-Fi, then whenever you're in range of any open Wi-Fi network and not already connected to one, the operating system pops up a dialog asking if you want to join. Tap the network you want, and enter a password if prompted.

You can also join a network by tapping its name in a list:

1. In the Settings app, tap Wi-Fi to open the Wi-Fi view (**Figure 26**).



Figure 26: The Wi-Fi view in iOS lets you tap a network to join.

2. Select the network from the list by tapping it. (If the network you're trying to find doesn't appear, tap Other.)

3. Enter a password if prompted.

You're now connected. Tap the info ⓘ icon next to the connected network for TCP/IP details, such as the assigned IP address.

There's another way to select a network, too. Swipe to reveal the Control Center, hold down on the network panel, then hold down on Wi-Fi. A list of networks appears and you can tap one to join.

Tip: You can also join a network if you're near someone with an iPhone, iPad, or Mac who is already connected and they have the email address you use as your Apple ID login for iCloud in their contacts. Simply tap the network name to join and that person receives a request to share the password. If they agree, it's securely sent to your device via Bluetooth and you're joined.

A Chain-Link Icon Indicates a Personal Hotspot

Apple uses a chain-link icon to indicate when a Wi-Fi network has been created using the Personal Hotspot feature via an iPhone or iPad. Personal Hotspot lets the phone or tablet act like a cellular router for other devices.

The Personal Hotspot appears in the Wi-Fi list under its own label, while also showing the chain-link icon.

Private Addresses in iOS or iPadOS

Some Wi-Fi networks use the unique Wi-Fi adapter address that's part of your connection to track you physically. They collect and pass that MAC address (see Appendix A: What and Where Is a MAC Address?) back to a central ad-tech network or other service and may also associate behavior that can be determined from your activity on a network. When the same Wi-Fi adapter appears on another network served by the same ad-tech network's back end, more information can be gathered and targeted ads served. There's typically no way to opt out of this data collection.

Apple has a typical privacy stance of blocking unwanted or intrusive collection of personal data. Starting in iOS 14/ iPadOS 14, that appears

as the Private Wi-Fi Address option for a Wi-Fi network. (It also appears for other kinds of network connections.)

After connecting to a network, tap the info ⓘ icon next to the next name, and in the view that appears, not the Private Wi-Fi Address switch, enabled by default (**Figure 27**). This switch creates a random Wi-Fi address that's fed to this particular network. (The address has to remain constant during a session, because it's part of the addressing protocol for Wi-Fi so that data flows to and from your device.)

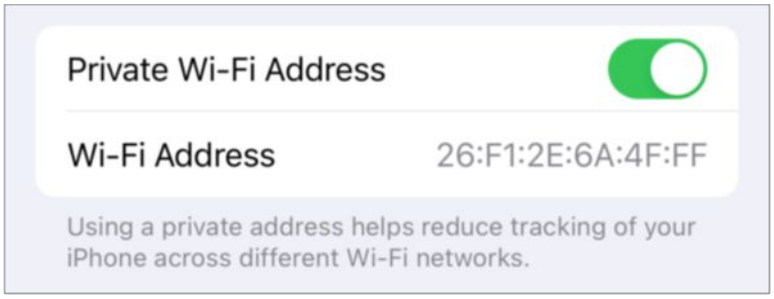


Figure 27: The Private Wi-Fi Address option deters cross-networking tracking and behavior tracing.

For networks you control or that are used for work, you may want to or even need to disable Private Wi-Fi Address, because you may have to provide a fixed MAC address to the IT department for access—or the IT department's intrusion-detection tools might identify your device as malicious because it connects with different MAC addresses when you log in with corporate credentials.

Forget a Network in iOS or iPadOS

iOS and iPadOS will automatically connect to this network every time it's in range. You can change that behavior by taking these steps:

1. Tap Settings > Wi-Fi.
2. Tap the currently connected network.
3. Tap Forget This Network and tap Forget to confirm.

The operating system immediately disconnects you, and you will remain disconnected. If you're using iCloud Keychain, it also deletes the network entry from all of your connected machines.

Disconnect in iOS or iPadOS

To disconnect while in range of the network, do either of the following:

- Swipe to bring up the Control Center, and then tap the blue (connected) circle with a white Wi-Fi icon within it. The symbol changes to a white circle with a black Wi-Fi icon. Tap again to reconnect; it will also be reenabled automatically the next morning.
- Tap Settings > Wi-Fi and turn off the Wi-Fi switch to disable the Wi-Fi adapter. While it remains off, you're disconnected.

Connect in Windows 11 or Later

To connect to a network in Windows 11 or later, follow these steps:

1. Click the System Tray network/speaker icon.
2. Click the right-pointing arrow next to the Wi-Fi icon in the Available item to reveal Wi-Fi networks (**Figure 28**).

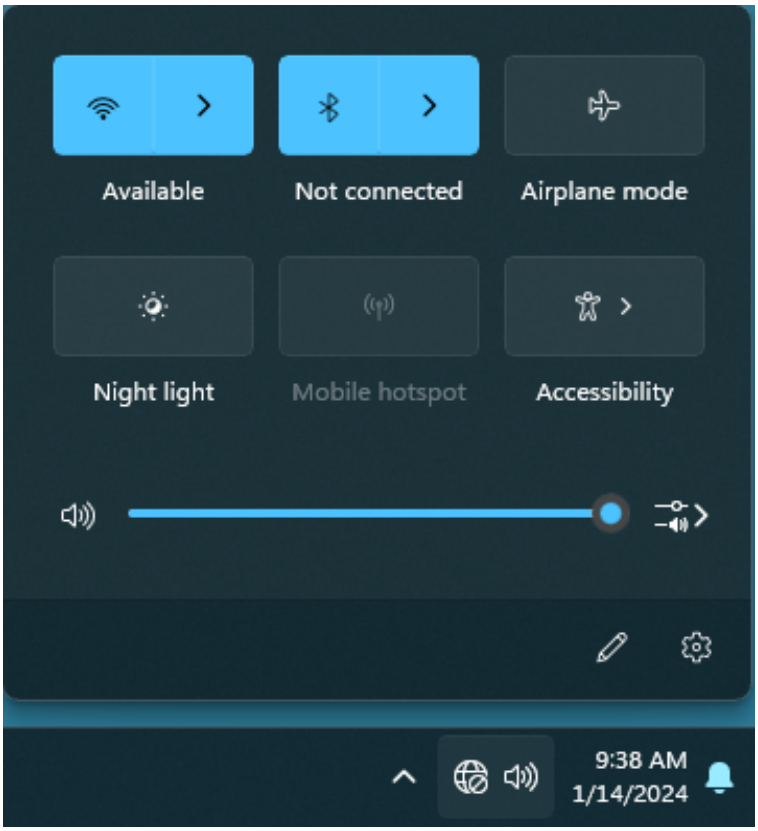


Figure 28: Click the system tray to reveal the Available option.

3. A list of available Wi-Fi networks appears (**Figure 29**).

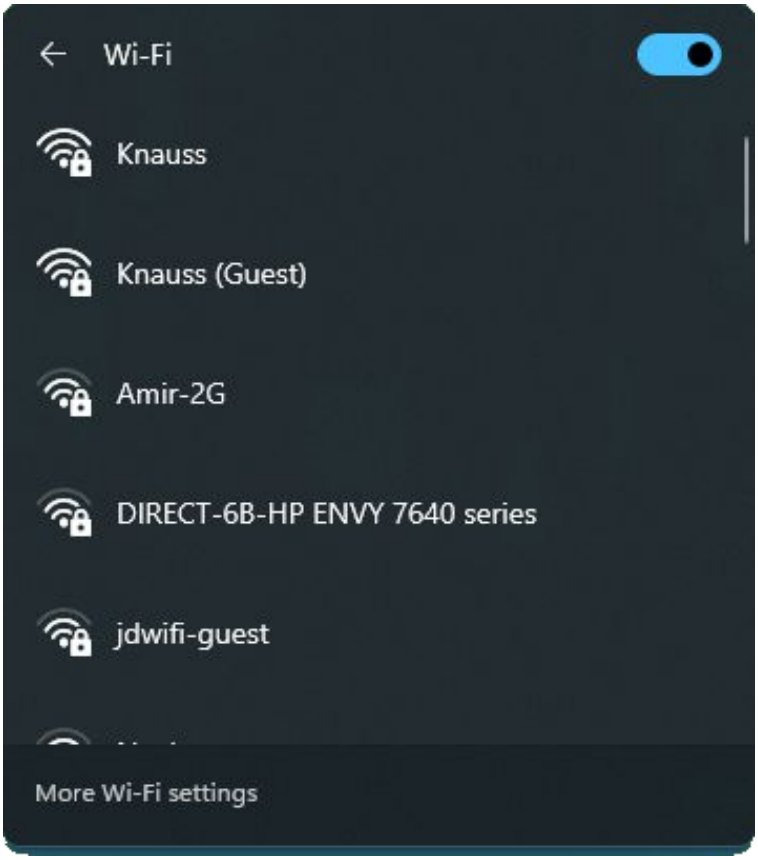


Figure 29: The Windows Networks pane shows which network is connected (if any), and the names of other available networks.

4. Click the network to which you want to connect, and optionally select the "Connect automatically" checkbox. Then, click the Connect button (**Figure 30**).

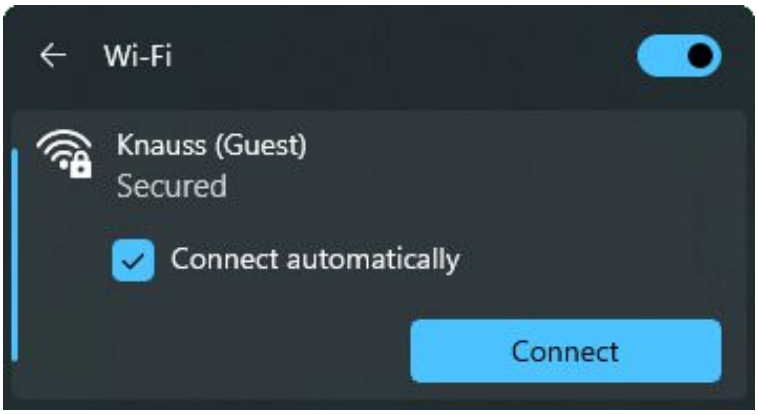


Figure 30: Choose a network to connect to.

5. Enter a password, if prompted, and click Next (**Figure 31**). Windows automatically figures out the right type of passphrase to send.

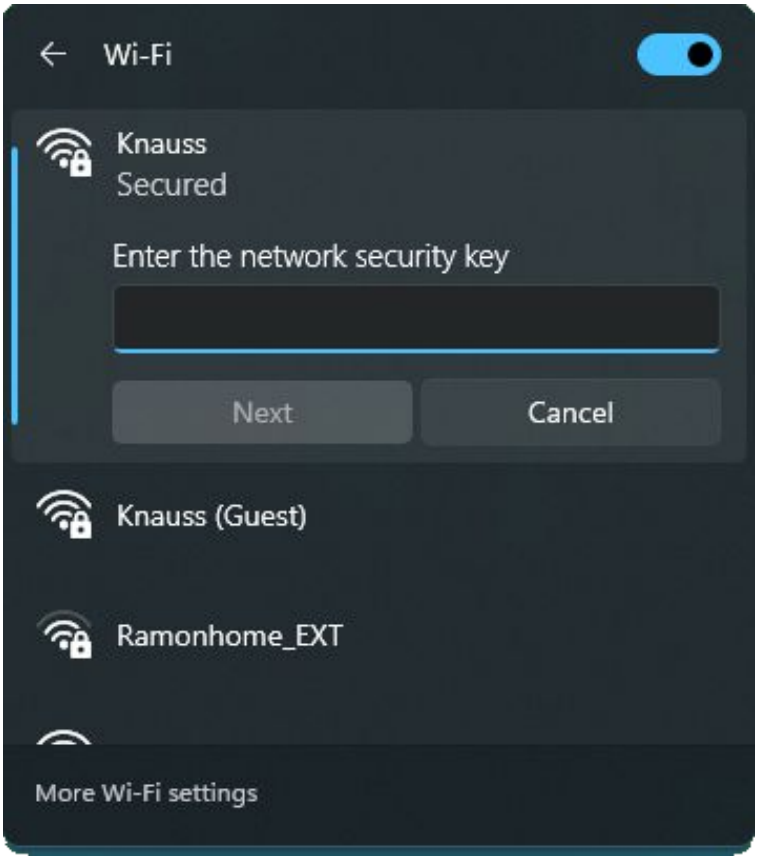


Figure 31: Enter the network's security key and click Next.

If the connection is successful, you'll see a Connected label appear beneath the network's name in the Networks pane.

Forget a Network in Windows

Windows 11 or later will automatically connect to this network every time it's in range in the future. You can change that behavior by forgetting the network using these steps:

1. Go to Settings > Network and internet > Wi-Fi.
2. Click the Forget button next to the Wi-Fi network you want to remove.

Windows immediately disconnects from the network.

Disconnect from a Network in Windows

To disconnect from a network in Windows 11 or later, you can choose either of the following methods:

- Click the System Tray network/speaker icon and click the Wi-Fi icon in the Available item.
- Click the System Tray network/speaker icon, click the right-pointing arrow next to the Wi-Fi icon in the Available item, select your active network, and click Disconnect.

Connect in Android

It only takes a few steps to connect to a Wi-Fi network in Android:

1. From the home screen, tap Settings.
2. Tap Network & internet > Wi-Fi. A list of networks should appear, including the one to which you're connected (**Figure 32**).

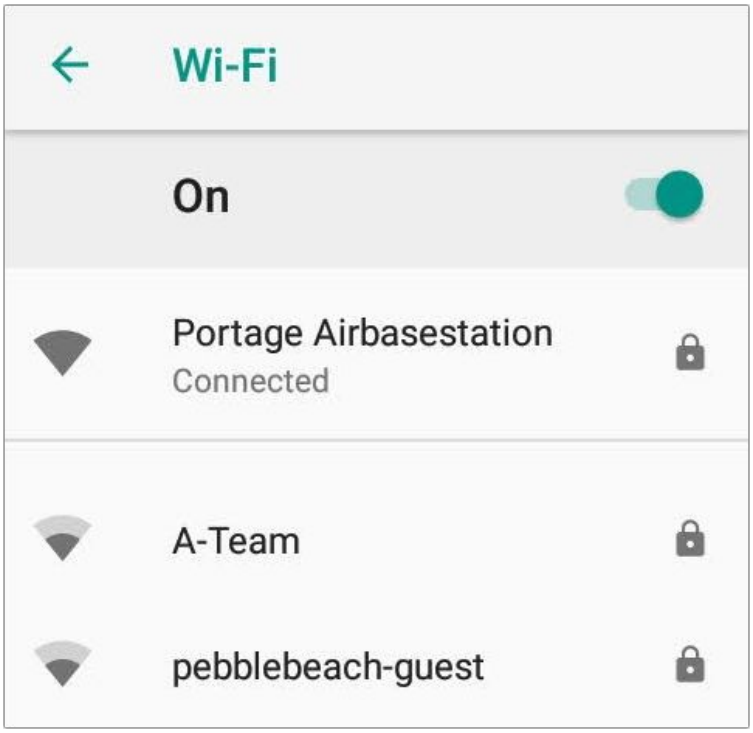


Figure 32: Android shows the list of available networks.

3. Tap the network you want to join.

4. If it's password protected, you will be prompted to enter the security key (**Figure 33**). Tap it in, and tap Connect.

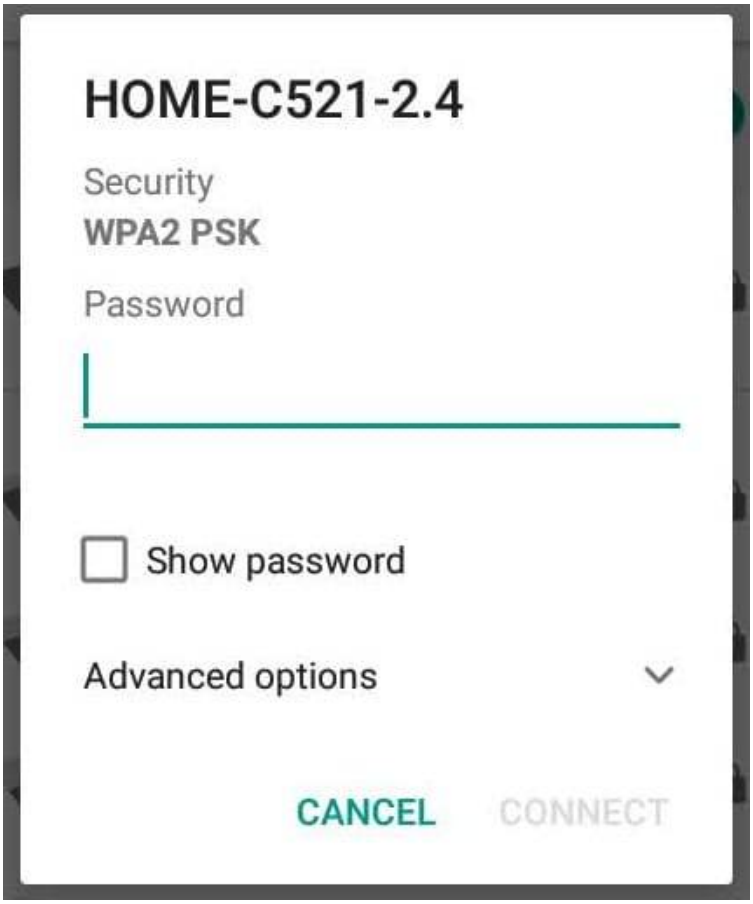


Figure 33: Enter the password and click Connect.

If you connect correctly, the network appears at the top of the Wi-Fi list with the Connected label beneath its name.

Forget a Network in Android

In the Wi-Fi list, hold down on the network name and select "Forget network," or tap the network name and tap Forget. You're immediately disconnected (**Figure 34**).

Disconnect from a Network in Android

There's no way to force a disconnection from a Wi-Fi network in Android without forgetting it or disabling Wi-Fi. For the latter, tap the switch at the top of the Wi-Fi list, which turns Wi-Fi off and disconnects the network.

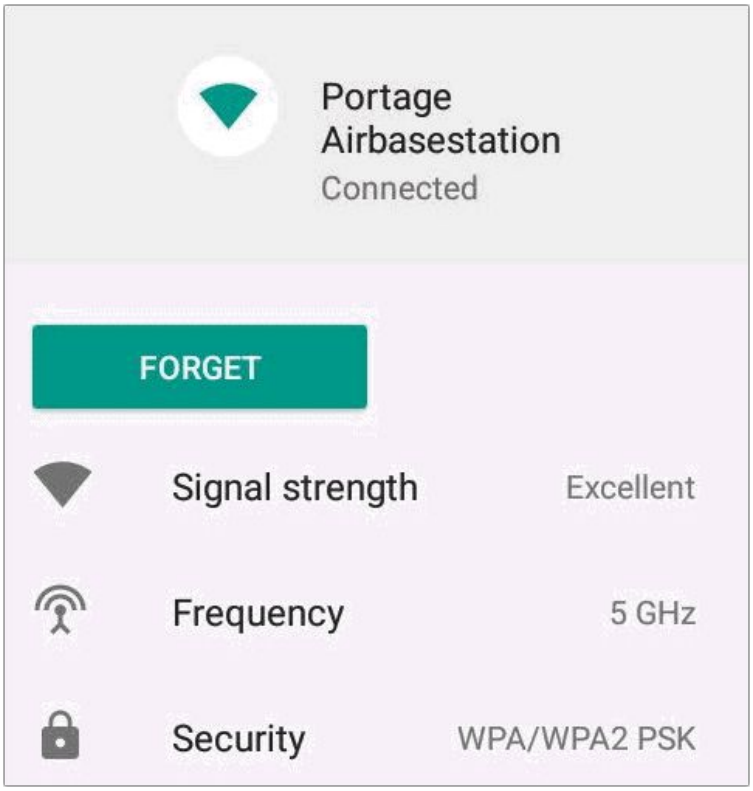


Figure 34: In the network details, tap Forget to disconnect and prevent automatic reconnection.

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

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.

Warning! If you aren't clear about whether your mobile plan includes personal hotspot use, has limits after which it stops working or is throttled, or you're charged an extra fee based on turning it on or for data usage, check that first!

Enable in iOS or iPadOS

On any device capable of acting as a Personal Hotspot, Apple automatically enables access for all of your Apple hardware logged into the same iCloud account. Simply select the Personal Hotspot from your Wi-Fi menu in iOS, iPadOS, or macOS, and it turns on. Personal Hotspot is always on standby for you.

You can also allow members of a Family Sharing group to have access in the same way. In the Settings app, tap Personal Hotspot, tap Family Sharing, and enable access. You can then set for each individual whether you are prompted to allow access or they can just use it.

Apple lets you enable a broader access method, too. In iOS or iPadOS, open Settings, tap Personal Hotspot, and tap Allow Others To Join. The operating system sets a default password the first time you tap this switch; you may want to change this to something more memorable or easy to enter. iOS and iPadOS always set the name of your hotspot to the device's name (**Figure 35**).

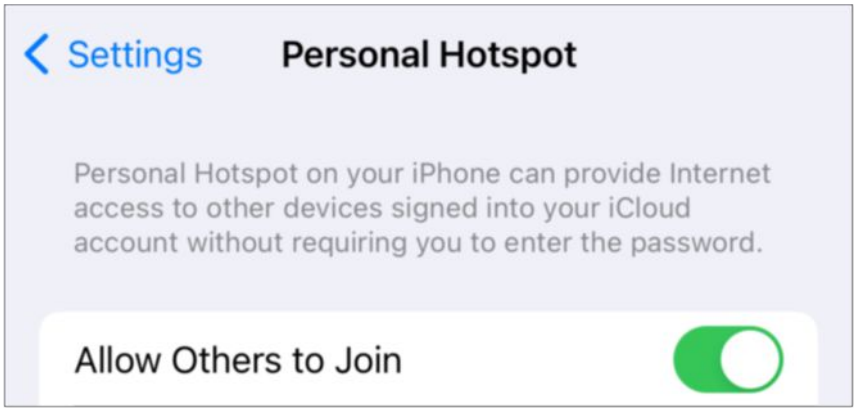


Figure 35: iOS and iPadOS lets you allow people or devices not logged into your iCloud account or part of Family Sharing connect to your Personal Hotspot.

Allow Others To Join also enables tethering via USB and Bluetooth.

Enable in Android

Android requires a few more steps, which vary by the version of Android you're using. In Android 8 or later, go to Settings > Network & Internet > Hotspot & tethering. Tap "Wi-Fi hotspot" and then tap the switch at the top to turn it on. Tap "Set up Wi-Fi hotspot" to change the network name, security method and password, and frequency band, if available (**Figure 36**). In the main view, you can also view and block users. (Depending on your phone model, you may have other choices as well.)

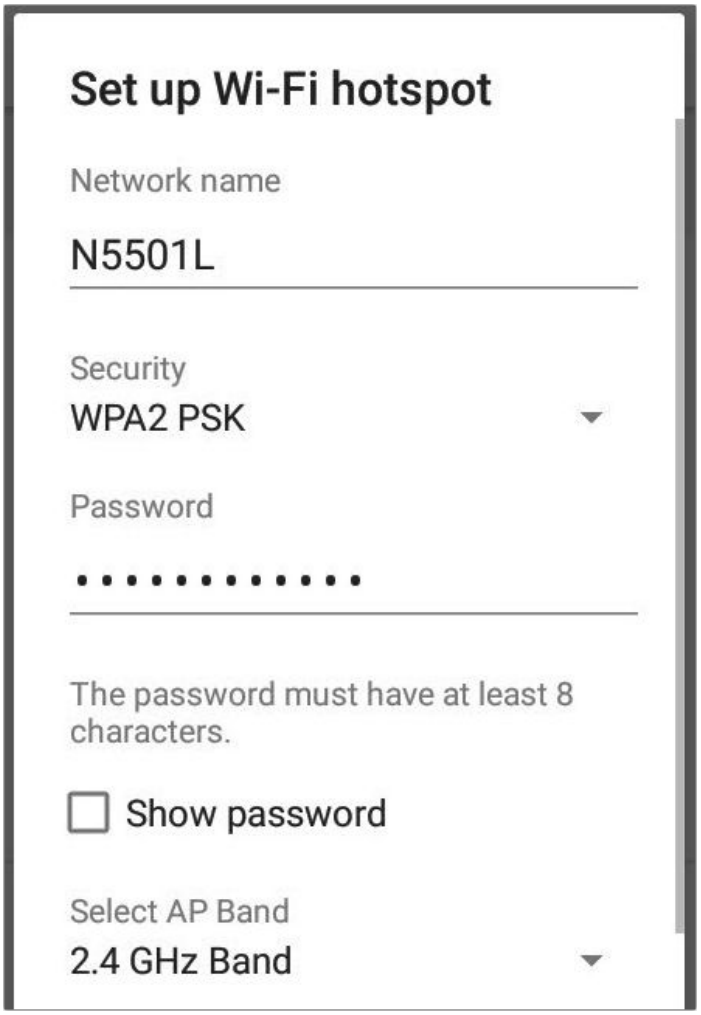


Figure 36: Android's Wi-Fi hotspot lets you set basic parameters.

To tether via Bluetooth or USB, you may have to enable these features via the same "Mobile network sharing" view:

- Tap "USB network setting," and you can switch from None to one of three options. "Smart network sharing" effectively picks the right

option from the next two as the phone senses it. “USB tethering” locks the phone into sharing its cellular connection to the connected device, while “Internet pass-through” shares a network connection *to* the phone from a computer.

- “Bluetooth tethering” is a simple checkbox you can turn on or off.

Disable Sharing

To turn off the hotspot on the device that’s sharing its connection, tap to reverse the option above.

You can also change the Wi-Fi password or disable USB tethering (Android), disable Bluetooth sharing (Android), or turn off the Wi-Fi or Bluetooth radios (iOS and Android). Changing the Wi-Fi password prevents devices with a stored password from reconnecting automatically or manually until you provide the changed password.

Connect to a Personal Hotspot

Generally, connecting to a personal hotspot is just like connecting to any internet connection, but there are a few minor differences, telltale symbols, and one-time setup factors you should keep in mind.

Access via Wi-Fi

Using Wi-Fi to connect to a Personal Hotspot network is the easiest case because no special setup is required. You use whatever method you normally employ to connect to a Wi-Fi network from the device.

In iOS, iPadOS, and macOS, an iPhone or iPad hotspot appears in the Wi-Fi list in a special place (under a Personal Hotspot(s) label) and with a special icon interlocked chain icon (**Figure 37**).

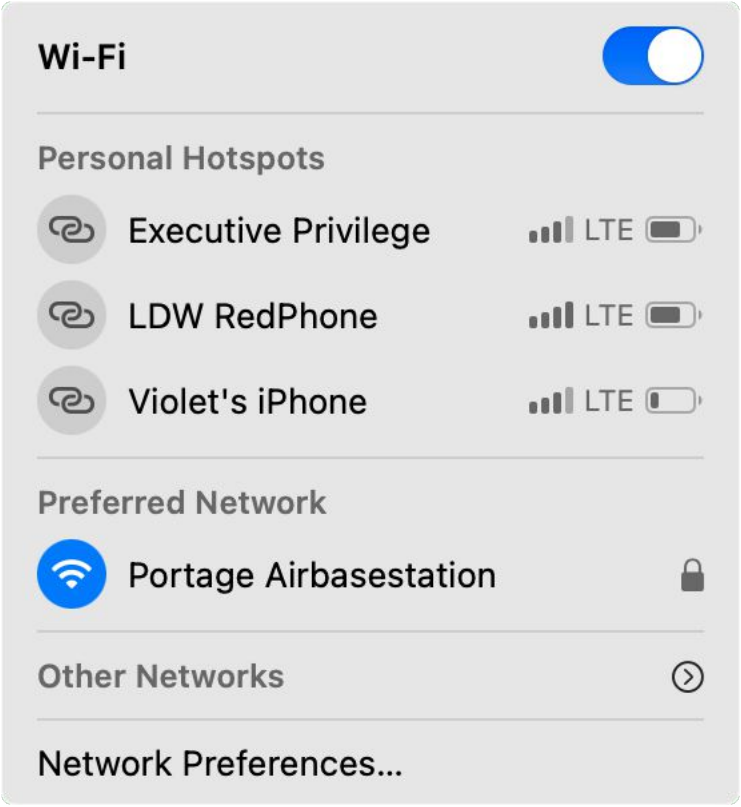


Figure 37: Select a hotspot listed under Personal Hotspots.

Tether with USB

With a personal hotspot enabled, connect your hotspot device to your computer with a USB cable. To halt the active USB tethering connection, disconnect the USB cable.

Configure with macOS

The first time you enable Personal Hotspot's Allow Others To Join option and plug the device in to a Mac via USB, macOS alerts you that the interface is added and the Mac adds an adapter entry. It appears in System Settings > Network on the main pane. macOS automatically activates a tethered link. When active, that red dot turns green.

Note: If you're not seeing this, you may need to click the device's icon in the Finder's Locations list.

You can disable the iPhone or iPad adapter profile to prevent a reconnection: go to System Settings > Network, select the iPhone USB or

iPad USB adapter, and click Make Inactive. To reactivate, click Make Active.

Configure with Windows

The tethered USB device will appear in Network Connections as an "Ethernet" device, likely labeled Mobile Device Ethernet. It should connect automatically, but you can double-click that adapter to modify settings. You can remove the profile to disable a connection.

Tether with Bluetooth

Bluetooth devices have to be paired in order to communicate, thus the first time you use a computer, tablet, or phone with your personal hotspot, you have to use Bluetooth settings on both devices to create a connection.

How To Pair

Here's how to make sure you're set up to pair, and then confirm pairing:

- On the mobile device, make sure Bluetooth is enabled in Settings > Bluetooth (iOS, iPadOS, and Android). Also, make sure it's *discoverable* in Android in Settings > Bluetooth, by tapping "Not visible to other Bluetooth devices" to enable them to see it. iOS and iPadOS keeps discoverability turned on whenever Bluetooth is enabled.
- On the other device, check that Bluetooth is on. (Check the Bluetooth system menu item in macOS or the Bluetooth system tray item in Windows.)
- Select the smartphone on your computer:
    - In macOS, open System Settings > Bluetooth, hover over the discovered device, and click the Connect button that appears.
    - In Windows, click the Action Center and then click Bluetooth. Click Connect and pick the phone's name.
    - In iOS or iPadOS, tap Settings > Bluetooth, and tap the device's name under Other Devices.

- In Android, tap Settings > Bluetooth, and then tap the device under Available Devices.

- When prompted on each device, check the pairing PIN shown on each—they should be identical. Then tap Pair or Connect on each device (**Figure 38**). You may only have to tap or click on the device initiating the pairing to approve the connection (**Figure 39**).

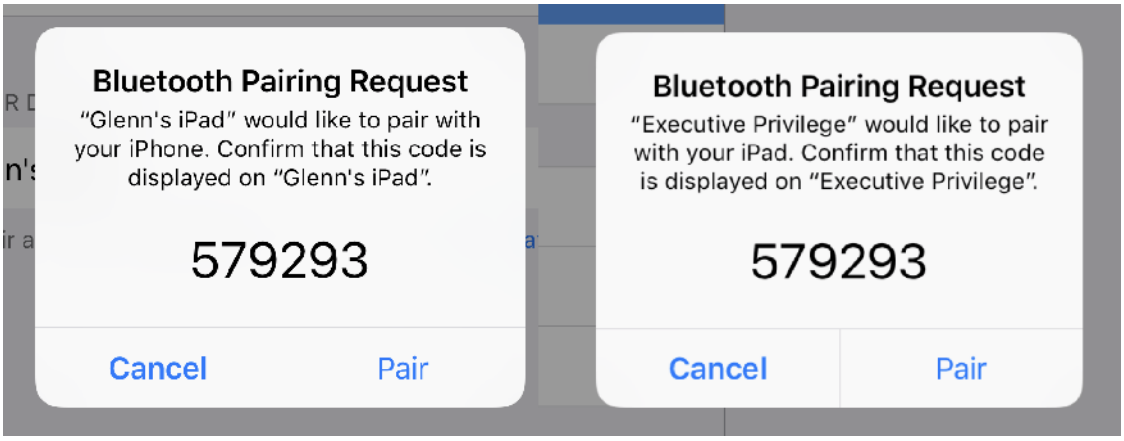


Figure 38: Two devices pairing should each display the same code and tell you the name of the other device. Confirm before pairing!

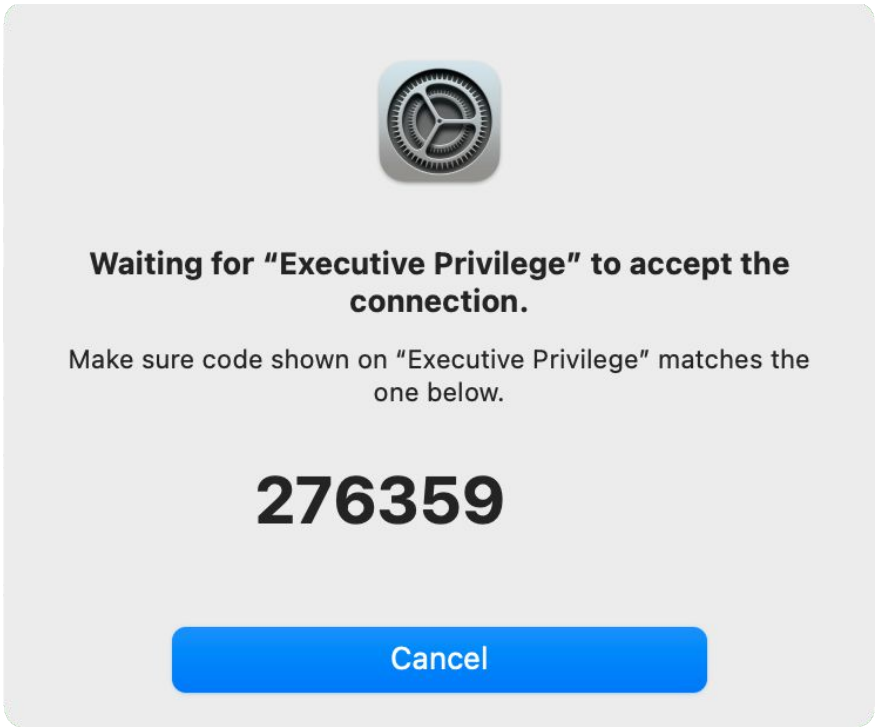


Figure 39: When macOS initiates a connection, it shows the code displayed on another device, and lets you cancel the pairing. But only the other device has to approve it.

Once you're paired, you can tether to the personal hotspot by using the Bluetooth settings view (iOS, iPadOS, and Android), system menu (macOS), or Action Center (Windows) to connect and disconnect.

How To Unpair

You might want to discard a stored Bluetooth pairing if, for instance, you're using a friend's device or you don't want someone else using your iPhone or iPad with the paired connection:

- In macOS, Control-click/right-click the device name in the Bluetooth preference pane, select Forget, and confirm.
- In Windows, open Settings > Devices > Bluetooth & Other Devices, select the device you want to remove, click Remove Device, and confirm.
- In iOS or iPadOS, tap Settings > Bluetooth, and tap the device's name under Other Devices. Tap the info ⓘ button, tap Forget This Device, and then confirm.
- In Android, tap Settings > Bluetooth, and then tap the device under Available Devices. Tap Unpair; there's no confirmation!

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!

- **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.

Map Ports for Remote Access

Port mapping relies on network address translation (NAT). *NAT* acts as a gateway between a WAN IP address for a router reachable from a larger LAN or the public internet, and the private addresses hidden behind NAT on the access point's LAN.

Tip: See the sidebar Understanding Ports if you don't quite understand what ports are yet.

NAT Maps Private to Public Connections

When a computer within the LAN wants to connect to the internet, the NAT software creates an association between that computer's outgoing connection and a public port on the WAN IP address of the access point.

When, for instance, a LAN-connected computer wants to retrieve a webpage, that computer might send a request from its IP address (192.168.1.100) using port 5509. (Ports for outbound connections are arbitrarily numbered above 1024; numbers below that are reserved for well-known services.)

The NAT server receives that connection and creates a request over the internet using the WAN IP address and, typically, a different port. So the NAT gateway's request might originate from a public address such as 36.44.0.6 with a port of 12087.

The web server receiving the request doesn't know about the original computer behind the NAT. Rather, the web server responds by sending HTML for the requested webpage to port 12087 on IP 36.44.0.6. The NAT server retains a list of associations between public and private ports and addresses, and hands that web connection over to the machine that requested it. This process is ugly, but it works reliably, almost all the time.

Understanding Ports

Every kind of network server you might run—from a personal web server to your side of a multi-player online game—uses a *port* to communicate with the rest of the machine, network, or world. You can compare a port number to an apartment number in a typical postal addressing system. A computer has an IP address like an apartment building has a street address; each service used by a computer has a port number, like each apartment has its own number (**Figure 40**).

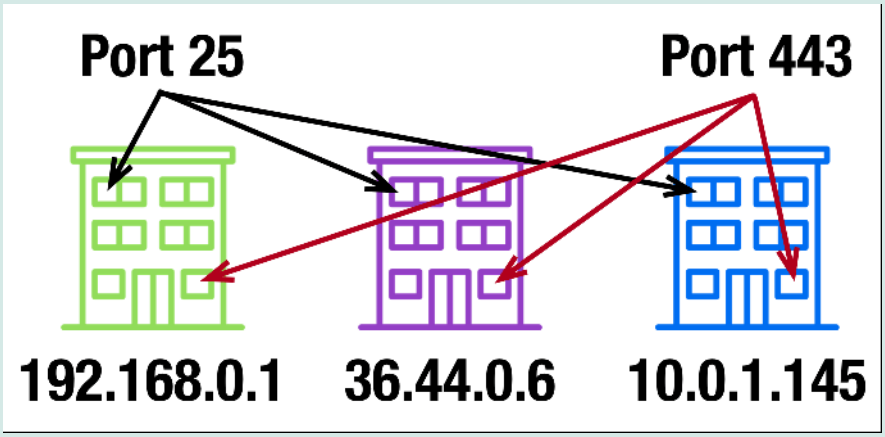


Figure 40: *Ports are like apartments within a building, where the building is an operating system, and the IP address is the building address.*

It's as if every apartment building had the manager in unit 1, the mailroom in unit 25, a lounge in unit 80, and so forth. Port numbers for common servers and services are the same on all devices.

Taking our metaphor one step further, if you have a static IP addresses, that's like having a street-front address. In contrast, NAT-provided private addresses are like buildings within a gated compound, where nobody on the *outside* knows the building numbers, but you have a private courier you can call to your apartment.

If you were inside the compound, you would ring to get a letter sent to the outside world by having the courier take it from you to the compound's mailroom. Then, the mail carrier would pick up your letter from there. Return mail, addressed to a mailbox number in the mailroom, is delivered only to that outer mailroom, where the courier picks it up and walks it to your private door.

Port Mapping Maps Public to Private Connections

With port mapping, you create a persistent connection that allows computers outside the LAN to connect to computers inside it. Port mapping lets you expose limited services in a way that you control.

When you map a port, you make the gateway connect one of its internet-accessible ports to the same (or a different) port on a computer on the otherwise-private inside network.

> ***Warning!*** Anything you do to punch through ports or computers from the private network to the outside world reduces security. You may want to provide better security on computers that you expose in this fashion by installing active firewall and intrusion-monitoring software.

The gateway listens for traffic on the specific port on its public, WAN interface. When traffic arrives and a connection needs to be opened, the gateway reroutes the traffic from that public interface port to the appropriate private address on its LAN interface, whether that's a Wi-Fi LAN or a wired LAN. In **Figure 41**, I show how two separate port mappings are passed through the gateway. Two people, one at Indiana University and one on the local network, connect to play TeamFortress 2 (thin blue lines), while a browser in Kuala Lumpur requests a web-page from the network's web server (thin red lines).

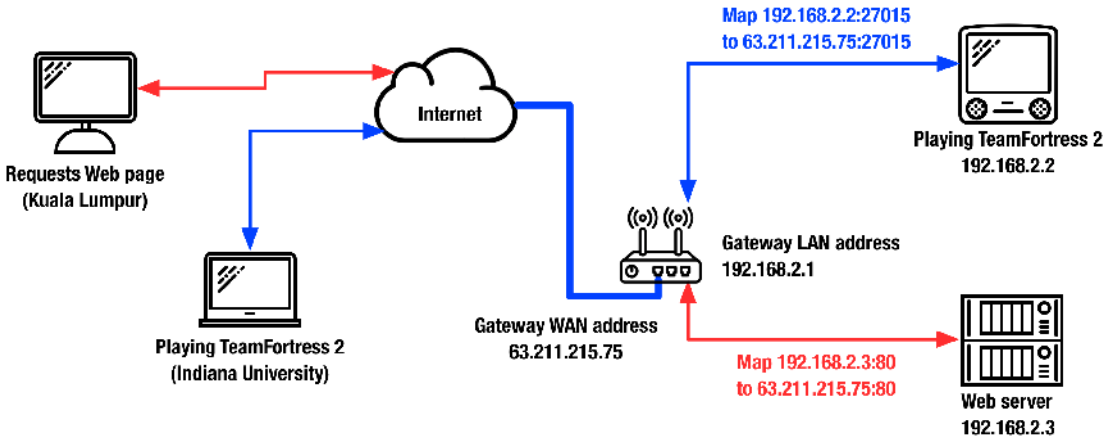


Figure 41: The gateway rewrites addresses and maps ports on the fly to connect inside and outside services and users.

To set up port mapping, you have to define two parts you set on your gateway: a persistent private ("reserved") IP address for a computer on the LAN, and a persistent port mapping between a port on the access point and a port on the LAN computer. In the topics ahead, I explain how to complete both of these tasks.

Set a Reserved Address

For each computer with which you want to use port mapping, you should create a DHCP reservation, which I described in Reserved Addresses, earlier. As you work, I suggest that you create a text file or other list that includes the name of each computer (described by its owner or its unique name) along with the corresponding reserved addresses. Once you've reserved addresses, you can set up effective port mapping.

> **Note:** Port mapping ties a public port to a specific private IP address, so if you don't use a DHCP reservation, you can't easily keep port mapping working without constantly making changes to the access point configuration and restarting—which changes the IP addresses assigned dynamically!

To use port mapping, you need to know which ports to map. This can be trivial. You could map port 80 on the public side to port 80 on a given computer on the private LAN, and establish a web server connection, for instance. For games, streaming media, and other purposes, you might need to set up a bunch of ports.

> ***Warning!*** Port mapping works only on an access point that's distributing addresses. One that's set to bridging can't (and doesn't need to) handle port mapping. Instead, connect to the access point that's feeding out addresses for the network.

Example: Set Port Mapping for a Web Server

With a web server running on a computer on the network, we need to set up the access point to pass traffic to the newly configured port:

- Set up the server on the LAN-based computer and figure out its private, reserved IP address. Pick a port other than the one used for

plain web access (80) or secure web connections (443) if you're configuring it differently.

- On the gateway, find the section for port mapping or virtual servers and enter:
  - The outside port number, which might be 80 or 443 or another port (see the sidebar, next). For more complicated servers, you may be able to select from a pop-up menu that populates all the necessary ports if it's more than one.
  - The inside port number from your LAN computer.
  - The private IP address from your LAN computer.
- Apply the changes and restart the gateway if that's required.

Now try to connect from outside your network to the web server you enabled. This is easiest from a mobile device that has that service available. Turn off its Wi-Fi radio and connect via the cellular side.

If the connection doesn't work, recheck your ports. Also make sure the computer running the service doesn't have an active firewall that is blocking incoming connections.

One per Port

Every commonly used internet service—things like web servers, FTP servers, mail servers, and so forth—have uniquely assigned ports that by default are used by software that accesses those servers. So when you type in `https://takecontrolbooks.com/` there's an implicit `:443` at the end. The colon says, "a port follows," and 443 is the assigned port for secure connections.

What happens if you want to run two or more web servers behind a gateway? You can only use port mapping to assign one of them to the gateway's port 80, and thus that leaves out general web access for other hidden sites.

However, there's a workaround for private sites that you know someone will always type in the URL or use a link to get to: you can assign a *different* port to these other web servers. Unsecured web servers listen by default at port 80 and secure ones at 443, but a web server can be configured to listen to any port.

It's typical to use ports 8000 and higher for alternative web severs. From outside the network, someone connects by using this format: `http://serveraddress.com:0`, such as `http://tidbits.com:8001`.

Set a Default Host for Full Access

The alternative to creating reserved addresses and port mapping for each service on each computer you want to expose from your private network is to appoint a single computer as your public machine. This exposed machine could serve any kind of service over any port without the necessity of adding port mapping rules. If one computer runs FTP, web, and Samba servers, and no other computers on the LAN have any public services, this might be the right option.

Some gateway makers call this machine the *default host*; others call it the *DMZ host*. This may be self-evident, but a default host setup works only when NAT is active on the gateway, as all ports are being mapped to the private IP address you specify. Use a default host with a fixed address, too: if DHCP is active, set the address manual in an unreserved range or, if your gateway supports it, use DHCP reservation.

Warning! If your access point has a public IP address, your default host is as exposed as if it were on the public internet.

It's simple to enable the default host. On every gateway I've configured, you need to find the default host or DMZ host setting, enable it, and then enter the private IP address you want to use in that fashion.

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

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**).

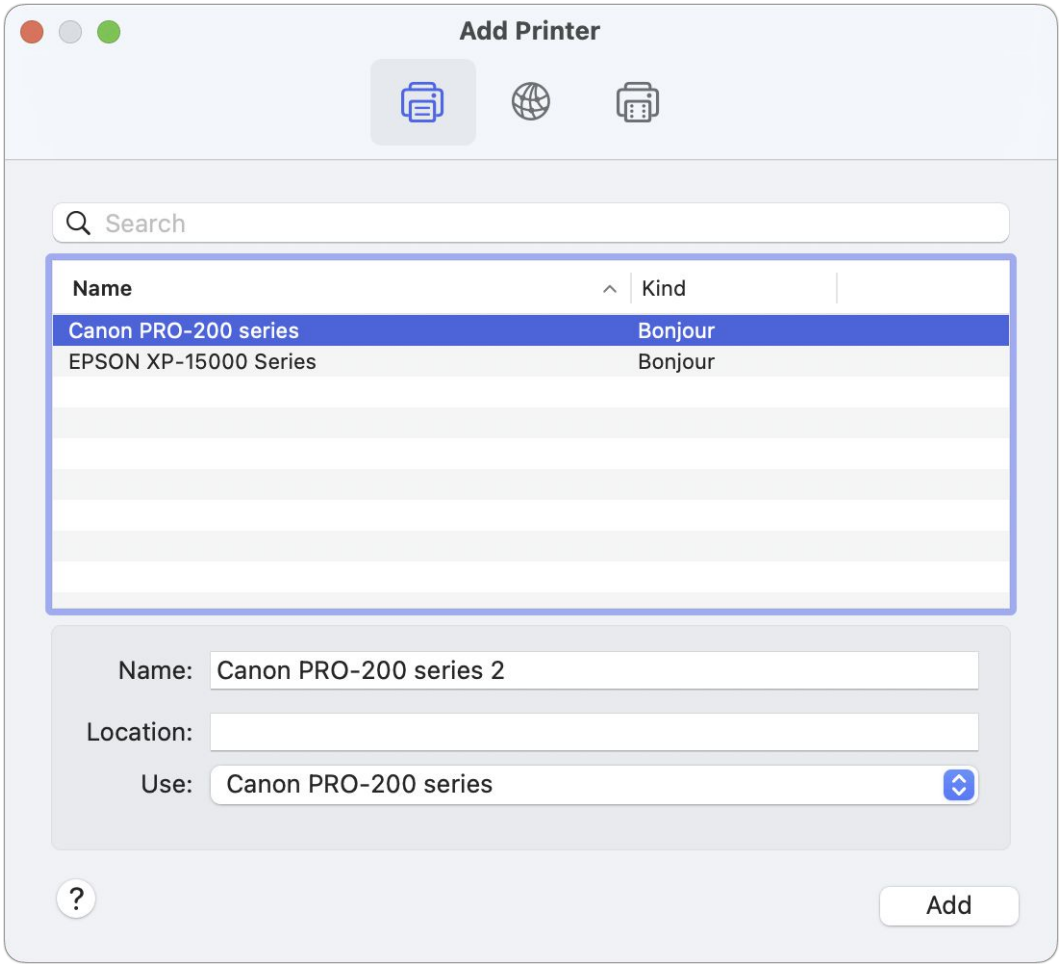


Figure 42: The Add Printer dialog shows discoverable printers.

4. Select the printer in the list. After a moment, the Mac should recognize the printer and display its driver in the Use pop-up menu. It may note the name of the access point in the Location field. If the Use menu doesn't fill in, choose the driver from the pop-up menu.

5. Click Add. Your Mac may automatically download printer drivers.

The printer should now be available from the Print dialog in your various Mac applications. If not, consult Troubleshoot an Unavailable Shared USB Printer, later in this chapter.

Tip: iPhones and iPads can only use printers that support AirPrint, a special protocol. If you have an iPhone or iPad and a Mac, and your printer lacks AirPrint support, you can use the $19.99 Printopia, which acts like a gateway between networked or directly attached USB printers and AirPrint.

Add a Gateway Printer in Windows

Here's how to connect a shared printer in Windows 11 or later:

1. Open Settings.
2. Go to Bluetooth & devices > Printers & scanners.
3. Click "Add device."
4. At this stage, your printer may appear and you can select it and click "Add device" (**Figure 43**).

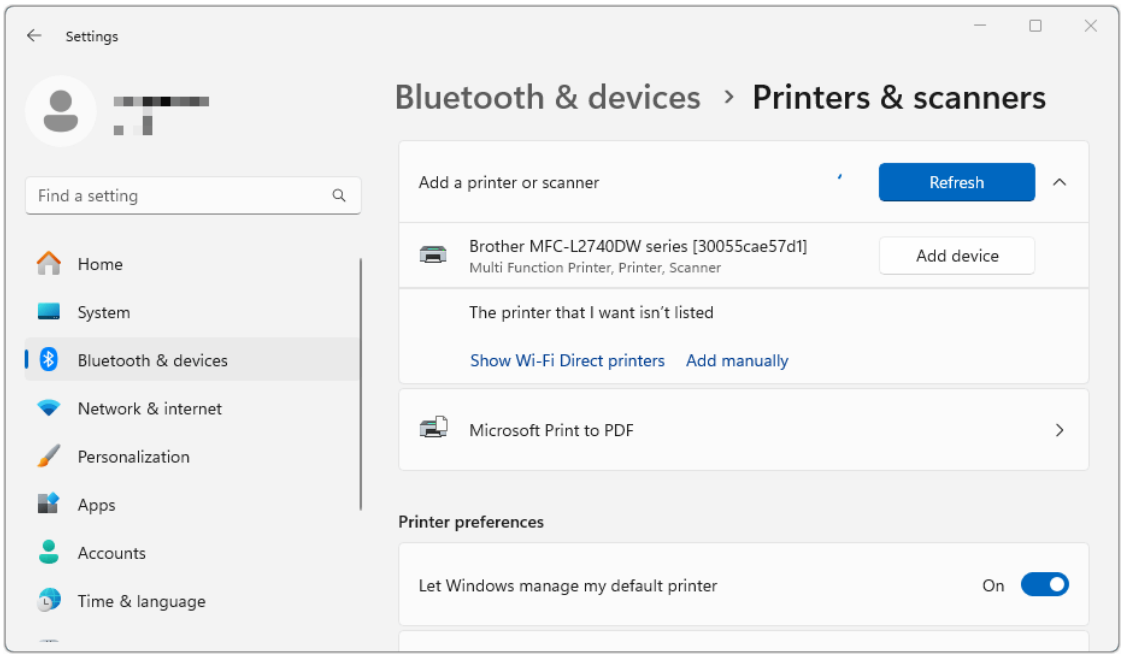


Figure 43: If a printer is recognized automatically, you can just select it and click "Add device."

5. If your printer doesn't appear, click "Add manually."
6. Pick the correct option from the list, which is typically "Add a Bluetooth, wireless, or network discoverable printer," and click Next. You can also select "My printer is a little older" (**Figure 44**).

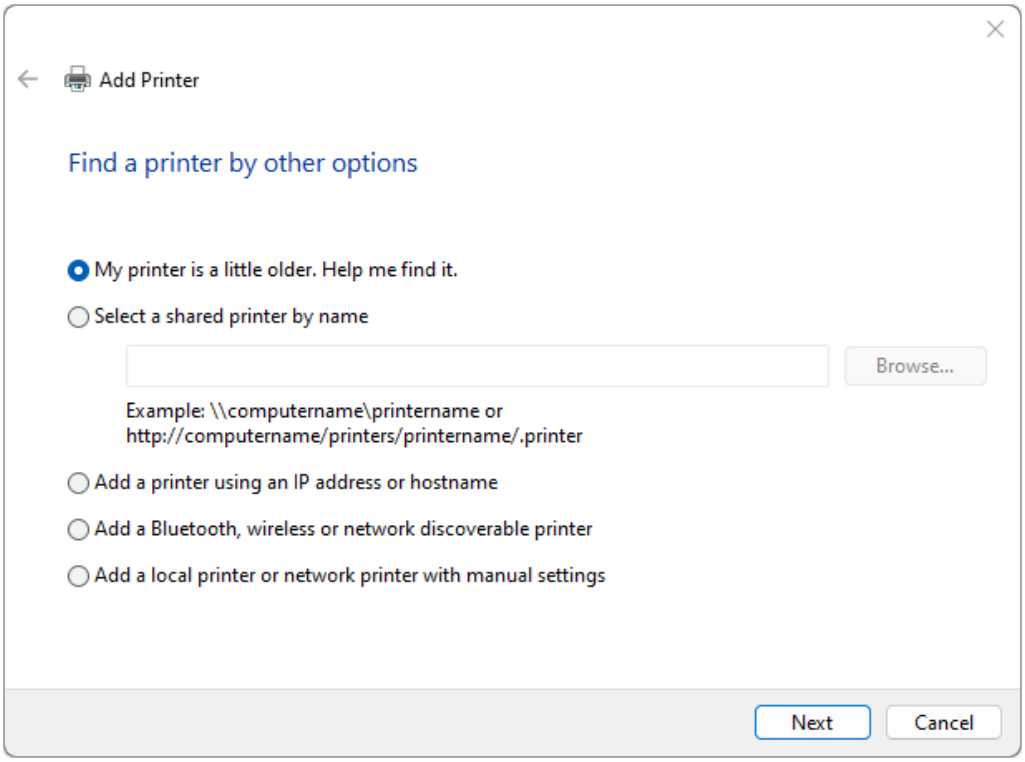


Figure 44: The Add Printer dialog lets you find "older" printers.

7. After a moment, "Choose a device or printer to add to this PC" should appear. Select your printer and click Next.

8. A dialog appears that says "Installing printer." Click Close to complete the set up.

The printer is now available to all applications.

Troubleshoot an Unavailable Shared USB Printer

If you followed the directions earlier in this chapter and you still can't print to your shared printer, one of the following suggestions should shed light on the problem:

- Make certain that the printer is powered up, not in standby-power mode (which sometimes prevents an initial connection), and not in an error condition (such as out of paper or out of ink).
- Check if the computer is on the same network as the access point by examining the front panel of the printer, which should let you navigate to Wi-Fi settings and show the network name; or via the gateway admin interface, which should show connected devices by name and MAC address.
- Restart your gateway.

Set Up a Shared Disk

As noted earlier, an easy way to share disk access across a network is by using network-attached storage (NAS). NAS units can cost a fair amount of money, though, for which they offer the kind of high performance typically need for video streaming or intensive small-office use. An alternative is connecting a USB drive to a gateway that offers disk sharing.

Here are a few things to consider when deciding between the two:

- If you share the network with other people, can you limit access to a shared drive through a password or user accounts? Many gateways can't; there's only universal access. Others may allow a single user (**Figure 45**).

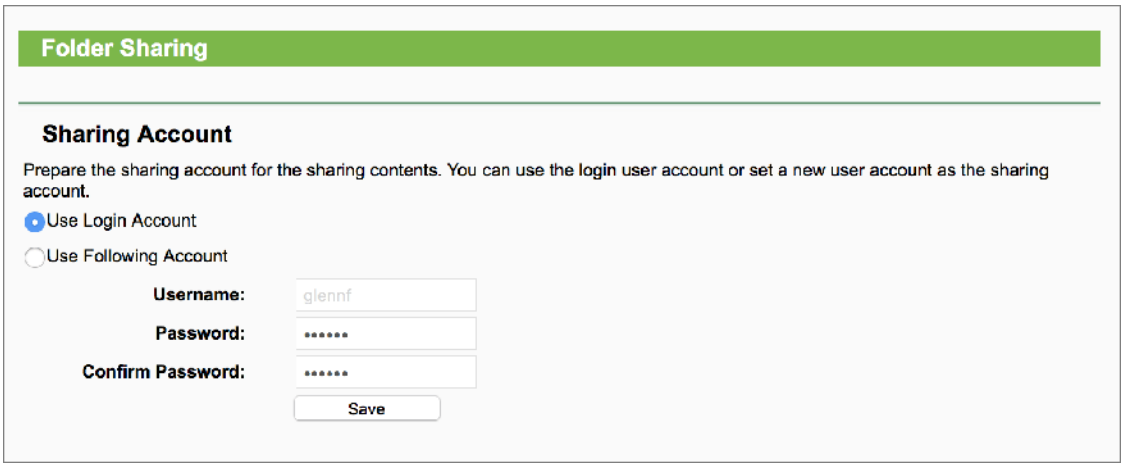


Figure 45: Some gateways can only create a single user for disk and folder sharing (here, a TP-Link model).

- Do you want to share the entire drive; selected drives; or selected drives with specified users? Depending on the gateway, you may only have one or two of those three possibilities available.
- Do you have a USB 3 drive and a USB 3 port on the gateway? This makes sure you have the fastest performance. USB 2.0 is relatively slow.
- Do you need to format the drive—to FAT32 or another file system—to provide access to the operating systems on the network that need

to reach it? Typically, gateways must use compatible formats to share, but not all gateway manuals will explain that to you.

While there used to be a variety of file-sharing protocols, the industry has generally standardized around Samba, which can be accessed via Windows, Linux, and macOS.

Mount on a Mac

You can mount a shared drive through the Finder, just like any other network volume. Open any Finder window, and look in the sidebar's Shared section for a list of servers.

The sidebar shows any servers on the local network with Samba volumes available for mounting, as well as FTP servers that use Bonjour to advertise their availability.

Tip: If you don't see the drive in the sidebar, choose Go > Connect to Server (⌘-K) and type in its IP address. After clicking Connect, you'll be presented with one of the dialogs in step 2 below.

To mount a volume from one of these servers, follow these steps:

1. Select the server name in the Shared or Locations section of the sidebar.
2. Click Connect As in the upper-right corner.
3. You may be prompted with a message explaining you're about to connect and asking you to click Connect to proceed. Do so.
4. A dialog appears with options to identify yourself. Select Registered User, enter your credentials, and click Connect (**Figure 46**).

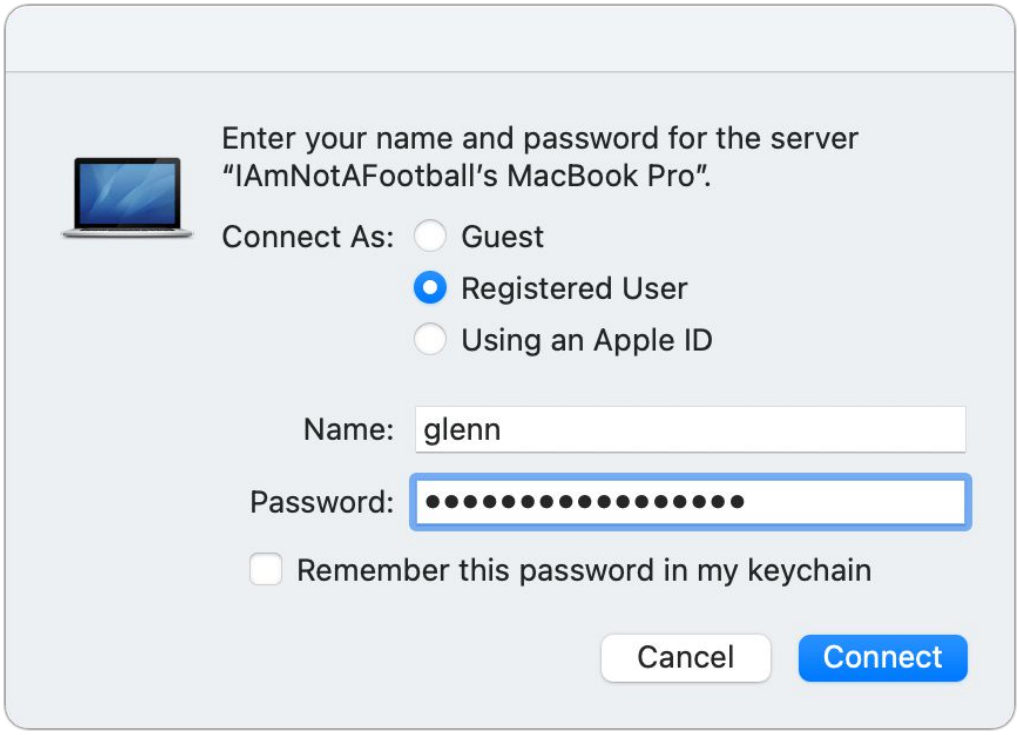


Figure 46: Enter your login credentials to proceed.

5. If only a single volume is shared, it will now occupy the window and be mounted on your Mac.

   If there are multiple volumes, double click a volume that’s shown in the mounted server window to mount it on your system.

Unmount a Volume

To unmount a network volume, select the volume on the desktop and press ⌘-E, or choose File > Eject “volume name.” Or, to unmount all volumes associated with a server, in a Finder window sidebar, click the Eject icon by the server’s name, or in the server’s Finder window, click Disconnect.

A disk icon turns gray while macOS removes its associations; it disappears when the process is complete. If a file is in use by an app, the Mac tells you which one.

Mount in Windows

In Windows 11 or later, follow these steps:

1. Use the gateway’s admin page to determine the local network IP address of the access point, which will be something like `10.0.1.1`.

2. Click the Windows menu and launch the File Explorer.
3. In the location field, enter `\\` plus the IP address (like `\\192.168.86.48`) and press Enter.
4. In the Name field (**Figure 47**):
    - If you don't have a user account because the access point has a single password and no user account name, enter any short bit of text or leave the field blank.
    - If you have a user account name, enter it.

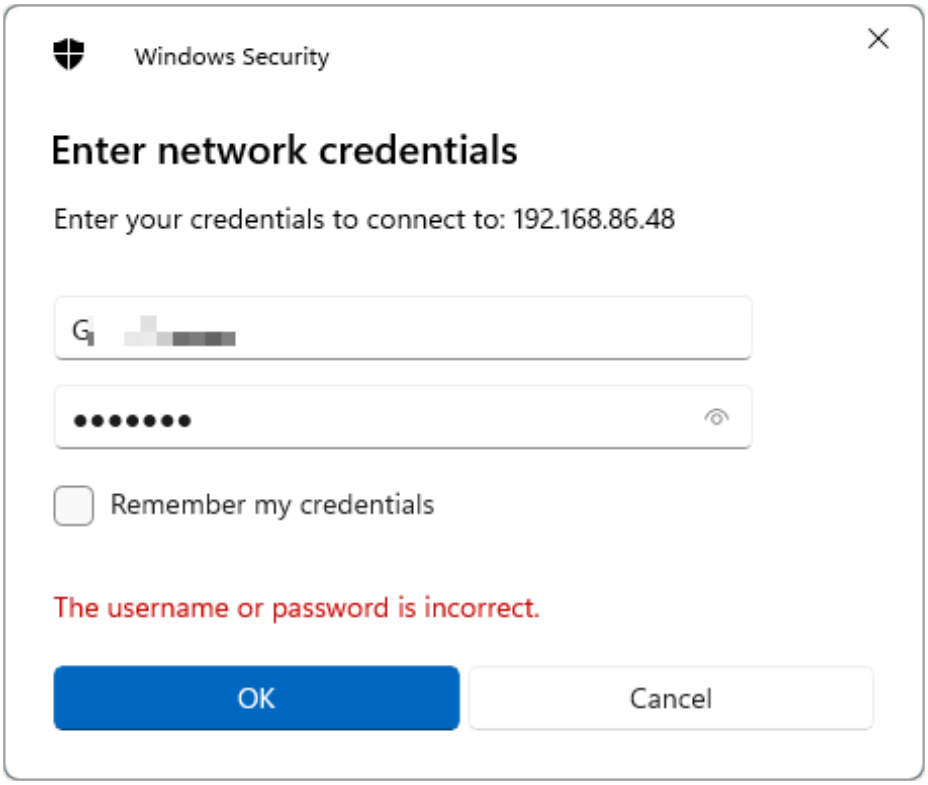


Figure 47: Enter your credentials to log in.

5. In the Password field, enter the access point, disk, or account password.
6. Select the volume or volumes you want to mount, and click OK.

To unmount a disk, find the volume under My Computers or on the desktop, right-click the volume, and select Disconnect.

Punch Through Automatically

UPnP allows software and firmware to talk to a gateway and ask it for ports, which the gateway then automatically configures and opens up. It's port mapping without any manual configuration.

The UPnP option is generally enabled by default in any gateway that offers it. You can check by using the admin interface and looking for the setting, which may be under Forwarding, NAT, or Remote Access. This section of the interface should also show active UPnP connections.

Note: UPnP also offers *discoverability* for services and devices, which is the announcement over a local network that given services are available. This allows UPnP-equipped software and hardware to spot those services and connect to them. If you launch VLC, for instance, it will show you all audio- and video-streaming software that's available on the LAN.

For access outside the LAN, on some gateways you will need to enable UPnP forwarding as well as plain-old UPnP. The former only passes traffic, while the latter lets it open ports.

With everything working, you shouldn't have to take action at all. You can consult the software or device you're using to determine the IP address and port combination it's expecting incoming traffic to come over, or you can use the admin interface on the gateway to find both those values too.

The IP address will be the public-facing address the router relies on, and the port should be listed in this list. However, you may be unable to find the service by name, because unless it uses specific UPnP registration, it will show up as a generic name along with the IP address and port combination from which it originates over the local network.

Some gateways can also act as UPnP servers for local and remote access, such as acting like streaming media servers using the DLNA protocol from attached hard drives.

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

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

uses to generate or retrieve a key. Sharing the password reduces security by allowing others to see the same network traffic.

Since 802.11b started appearing in hardware in 1999, three different encryption methods have been offered, each superseding the previous one. The earliest two, WEP and WPA, are effectively dead, as explained in the following sidebar and the next section.

WEP's Long-Ago Demise

WEP (Wired Equivalent Privacy) was Wi-Fi's first encryption standard and the only option from 1999 to 2003. It was so weak that people long speculated it was designed that way intentionally, and some security experts maintain that's the case. WEP had to work on the slow silicon of the day, and couldn't be too robust due to issues surrounding U.S. export policies and encryption.

Starting over a decade ago, effective attacks rendered WEP protection essentially useless, and it was abandoned beginning in 2003 with WPA (Wi-Fi Protected Access) and then in 2004 with a more robust replacement, WPA2, and, in 2018, by WPA3.

WPA, WPA2, and WPA3 Background

The Wi-Fi Alliance released *WPA* (Wi-Fi Protected Access) in 2003. It was an interim measure because the IEEE's work on the 802.11i security update for Wi-Fi was taking too long and it was known that WEP (see sidebar above) was insecure. WPA was considered to be quite strong and was designed to allow support from even the earliest Wi-Fi gear via firmware upgrades.

WPA2 was the final version of WPA security. It includes all the work done in the 802.11i committee. WPA2 replaces the weaker WEP key with a government-grade method of encryption favored by corporations. Any equipment released in 2003 or later can handle WPA2.

In 2018, the Wi-Fi Alliance announced the next flavor of security: *WPA3*. It upgrades the encryption algorithm to something even stronger and more modern. It also automatically creates an encrypted connection on an open network between each client and the gateway,

preventing sniffing even if there's no Wi-Fi network password! WPA3 has made its way into gateways and clients, and most devices sold in the last seven years shipped with WPA3 or could be updated via firmware to support it.

> **Note:** For the rest of this chapter, I talk only about WPA2 and WPA3, as WPA is effectively no longer used on modern networks, because it carried over some of WEP's weaknesses.

WPA2/WPA3 comes in two versions, typically referred to as Personal and Enterprise:

- **Personal:** This version allows the use of *passphrases* or long sequences of text—minimum 8 characters, maximum 63 characters. Passphrases can include letters, numbers, spaces, and punctuation. These are converted into the source material for generating an encryption key.

  The option to create a long phrase gives a WPA2/WPA3 passphrase the potential to be memorable, but adding more characters in the phrase also adds *entropy*. In other words, it becomes increasingly difficult for someone to predict the key. A passphrase could look like `my d000gs have lite_brite_hair!` I kid you not.

- **Enterprise:** The Enterprise flavor of WPA2/WPA3 requires a central server that handles account information and logins, and presents to a user something that looks like a server or desktop login. Some Wi-Fi gateways include the settings necessary to use one of these. It's unlikely you'd want to run such a server yourself, but there are companies, such as NoWiresSecurity and IronWiFi, that offer this as an internet-based service.

  The advantage of using an Enterprise login is that you can provide unique logins to each user, each of which have automatically generated unique encryption keys. That prevents any users from sniffing the traffic of any other. You can also revoke access to individual users—such as contractors at the end of a project—without having to change a common passphrase everyone uses.

Turn On WPA2/WPA3 on Your Gateway

Most gateway interfaces have a section or tab titled Security, but this sometimes—as in TP-Link's admin utility—refers to security protocols that can pass through it, especially for VPNs. If that's the case for you, look in Wireless and Network settings until you find an option labeled WPA2 or WPA3.

Depending on the age of the gateway and other factors, you might be able to select WPA2, WPA2/WPA3, or WPA3:

- Start by enabling WPA3 only.
- If some devices cannot connect, look up their specifications. Can they be updated via firmware to support WPA3?
- If not, switch to WPA2/WPA3.

Tip: Older gateways will still show WPA or WPA/WPA2 and may list TKIP, WPA's outdated encryption algorithm. Choose WPA2 if you have the option. You should also considering upgrading to a newer gateway for effective security.

Some gateways may require you to enter a passphrase separately for the 2.4 and 5 GHz networks that they create. If you're naming your networks for both bands the same, also set the passwords to the same.

A passphrase for a Wi-Fi network should be easy to enter, remember, and hand off to someone else. But avoid making one easy enough to guess. The best passphrase is a few words long. (Better yet, never enter a password, but use a password manager to create and retain it.)

Strong Passwords Aren't Complicated, Just Long

You may have heard that passwords should always be randomly generated and full of a mix of letters, numbers, and punctuations. That's outdated advice. A longer passphrase is better than a shorter one, and complicated passwords tend to be short or created in a weak fashion. For example, `apples11!` would pass many strength tests, but is easy for crackers to break.

If you don't believe me (and the security experts who have been telling me this for years), read the guidelines from the National Institute of Standards and Testing (NIST). These note that software that provides restrictions on passwords "SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets."

You can hand this password out to other people who use the network, but there's also a nifty way in Android and iOS to join a secured Wi-Fi network: using a QR Code. The site QRCode Monkey can generate a Wi-Fi QR Code that you print out or keep as an image on a device. Any recent Android phone or tablet, iPhone, or iPad can scan it and join (**Figure 48**).



Figure 48: A QR Code is a neat shortcut for letting people join your network. Using a smartphone, they can scan it with just a few taps.

Allow Guest Networking

If you want to preserve the security of your network while still allowing visitors and others to access it, you can take advantage of a feature

available on many modern gateways: a guest network. This exceedingly nifty feature splits your Wi-Fi network into two separate networks (technically creating two *virtual LANs*) while using all the same actual hardware.

A guest network provides users with internet access, but doesn't pass any traffic to or from the main network. People connecting to a guest network generally can't access computers or devices on your main network, including printers, although some gateways offer a LAN access option that can be turned off and on. Some may let you set 2.4 and 5 GHz networks separately, while others only let you create setting that automatically work over both networks.

Another advantage of a guest network is that it has a different password from your main network password, which you may not want to share with guests, especially if you use that password in other places too. Or, if you don't password-protect your guest network, guests can gain wireless internet access with no hassle, and you've not put other network resources at risk.

Depending on the gateway, you may also be able to:

- Throttle inbound and outbound bandwidth usage.
- Set a maximum amount of time a device can be connected.
- Set day of week and time of time limitations.

These limitations let you ensure guests don't overwhelm your main network, something useful more for small businesses and retail locations.

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.

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

decipher your messages. In fact, it's so secure, governments around the world—including the U.S. and China—aren't happy about it.

- **Other instant-messaging and audio/video chat services:** These have varying levels of protection, but Signal from Whisper Systems is the best. WhatsApp from Facebook can be configured and used very securely, too, for the moment.
- **Dropbox, Box, iCloud Drive, Google Drive, and others:** File-sync services use encrypted transport for all the data that moves between your various devices and central sync or storage servers.

Encrypt Files and Email

It may seem surprising, but there's no built-in or simple way to use strong encryption to lock a file that you send to someone. There's also no straightforward way to handle this in email.

Note: Some email apps and services support the PGP format—created nearly 30 years ago—for public-key encryption of messages, but it requires making sure recipients are using the same or similar approach so that they can decrypt messages sent to them.

Even when you have a method, typically limited to a single platform (and often Windows only), you have to figure out how to exchange a key or password/passphrase with someone else securely, too!

This is why so many people rely on WhatsApp, Signal, iMessage, and similar messaging tools, which use end-to-end encryption without configuration, and let you attach or transmit files along with messages.

Note: A loose definition of strong encryption is that it encompasses well-known and well-tested cryptographic algorithms that effectively can't be broken using brute-force techniques. This should remain true even if a user selects a weak password. Weaker systems rely on passwords or other secrets that, given a reasonable amount of time (from seconds to days), can be figured out.

Umbrella Protection with a VPN

A virtual private network (VPN) connection is a nifty way to prevent any sniffing of your local network hookup. A VPN encrypts all the data coming from and going to a device—such as an Android phone, iMac, or a Windows laptop—creating an encrypted *tunnel* that extends between the device and a VPN server somewhere else on the internet.

Think of this tunnel as a Willy Wonka-like boat journey, in which to everyone outside the tunnel, it appears like a meaningless blur of unconnected details, while those inside arrive intact and safely at their destination.

The VPN tunnel lets your information traverse any local network and hubs, as well as every node on the internet between the two points, with protection. For corporations, VPNs extend the aegis of corporate security to remote devices. With a company, the VPN server is within the corporate network and any data leaving that server is protected by company firewalls and intrusion prevention.

But for individuals, that's not the case, because there's no definitive end point. Your encrypted tunnel ends (or *terminates*) typically in a well-protected data center. From that data center to its destination, data is unprotected (unless wrapped in an encrypted method, like TLS on the web, described earlier), but that's typically fine. The main locus of risk is the local link, like a café, school, or other shared network.

And because major internet sites—like Google, Apple, and the rest—have distributed sets of computers and even private links to big data centers, the hop from the VPN server to the destination network may be within the same building or close by.

Because it's exceedingly inexpensive for an app developer to set up VPN service, many thousands of offerings proliferate, and it's difficult to figure out which ones to trust. I recommend turning to Macworld, PCWorld, and Wirecutter for recommendations, as they both not only tested the technical requirements and looked at price versus services offered, but also dug into company backgrounds and privacy policies.

Every major operating system has a section for setting up a VPN connection, and all the best VPN services provide step-by-step instructions for every platform. Some even include downloadable profiles that you can install to manage all the configuration.

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.

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.

2. Select Settings > Network & Internet > Status > Network and Sharing Center.
3. Next to Connections, select your Wi-Fi network's name.
4. In the Wi-Fi Status dialog, click Details.
5. In the Details window, the MAC address is listed as Physical.

Find the MAC Address in Android

Android nests the MAC address down just a couple of levels, so follow this method:

1. Open Settings.
2. Tap Wi-Fi.
3. Tap the three-vertical-dot button and then Advanced. The MAC Address appears in that view; you may need to swipe down to find it.

Find the MAC Address on Gateways

Every gateway will have a different place in which it lists a device's MAC address. But all the gateway hardware I've tested over the years also has a custom-printed label on the back or bottom that includes the device's serial number, and MAC and SSID addresses.

You can also open the admin interface for your router and look through the interface. It's usually found in a status page or quick start page. The TP-Link Archer C7, for instance, puts the wireless LAN, Wi-Fi, and WAN port MAC and BSSID addresses front and center on the first page you seen.

Apple hides the information in its AirPort Utility for macOS, but if you hold down Option when clicking the Edit button, a Summary screen appears that shows all the MAC and BSSID addresses.

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.

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

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.

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.