

EBOOK EXTRAS: v1.0
Downloads, Updates, Feedback



TAKE CONTROL OF
WI-FI
NETWORKING
and **SECURITY**

by **GLENN FLEISHMAN**

\$12.99

Table of Contents

Read Me First	4
Updates and More	4
Note for Previous Readers	5
Introduction	6
Wi-Fi Quick Start	7
Learn Wireless Basics	8
Adapters and Access Points	8
Wi-Fi Spectrum	11
Wi-Fi Standards	14
Pick Wi-Fi Network Gear	17
Make a Plan	19
Build a Standard Network	22
Build a Mesh Network	29
Pick a Wi-Fi Channel	40
Spectrum Trade-Offs	40
Troubleshoot Your Connections	45
Configure Your Network	52
Learn About Dynamic Assignment and Private Addresses	53
Get a WAN Address	54
Hand Out LAN Addresses	58
Connect to a Network	64
Connect in macOS	64
Connect in iOS	67
Connect in Windows 10	69
Connect in Android	71
Connect in Chrome OS	73
Connect with a Personal Hotspot	76
How to Share a Personal Hotspot	76
Turn on Hotspot Sharing	77
Connect to a Personal Hotspot.....	80

Reach Your Network Remotely	84
Know Your Options	84
Map Ports for Remote Access	86
Punch Through Automatically	91
Set a Default Host for Full Access	93
Share Printers and Disks	94
Add a Printer	94
Set Up a Shared Disk	99
Secure Your Network	103
Simple Tricks That Don't Work	103
Use Built-In Encryption	104
Allow Guest Networking	108
Secure Yourself	110
Protect Particular Services	111
Encrypt Files and Email	112
Umbrella Protection with a VPN	114
Appendix A: What and Where Is a MAC Address?	116
About This Book.....	119
Ebook Extras.....	119
About the Author	120
About the Publisher.....	121
Copyright and Fine Print	122

Read Me First

Welcome to *Take Control of Wi-Fi Networking and Security*, version 1.0, published in May 2018 by alt concepts inc. This book was written by Glenn Fleishman and edited by Scholle Sawyer McFarland.

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, Windows, Android, and ChromeOS.

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

Copyright © 2018, 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](#).

Note for Previous Readers

The current book has a relationship to a series of titles dating back almost 15 years. From the first title until an edition updated in 2015, and under various names, each version of the book focused largely on Apple's ecosystem. This included detailed advice on configuring its AirPort family of base stations, partly because it was the best course for most people using Apple hardware.

However, the world has changed:

- Almost everyone contends at home and work with a huge number of competing Wi-Fi networks and devices. Apple's equipment worked best in less-complicated times.
- Apple stopped updating its AirPort Extreme and Time Capsule models in 2013 and its AirPort Express extender in 2012. In April 2018, it confirmed it had stopped producing them entirely.
- Most of us are working in much more mixed ecosystems of phones, tablets, computers, smart home devices, smart TVs, gaming systems, streaming media players—and more!

As a result, I wrote this new book using a few selected parts from *Take Control of Your Apple Wi-Fi Network*, but much of the book is entirely new and it's all overhauled for the new reality.

This new book focuses more broadly to provide advice applicable to any router and all the major operating systems: macOS, iOS, Android, Windows 10, and ChromeOS. It will still be deeply useful to people in the Apple ecosystem, however.

Get a Free Book on Apple's Last Generation of Gateways

Do you still rely on older Apple networking hardware? Buyers of this book can download *Take Control of Your Apple Wi-Fi Network* at no cost by clicking the Ebook Extras link (in [About This Book](#) or on the cover of the PDF version) and then looking under the Blog heading.

Introduction

Wi-Fi is nearing two decades old. It's much easier to set up and use than in the past, but the intricacies of creating a robust home or small-office network that has solid and fast coverage everywhere you want it can remain a struggle. This book is designed to offer guidance at every step of the way, and reduce your frustration with the terminology and arcana required to make decisions.

Because we all now use many different kinds of equipment on a modern Wi-Fi networks, I provide detailed, illustrated advice on connecting and configuring hardware running macOS, iOS, Android, Windows 10, and ChromeOS to work with various Wi-Fi features. After surveying popular Wi-Fi gateways, I provide advice compatible with nearly all hardware on the market.

If you're trying to understand the difference between standard Wi-Fi networks and new mesh wireless networks, I go into great detail, and help you decide which may 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](#).

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 with Wi-Fi stamped on them work with other Wi-Fi devices following the same standards, or are faithful to one another.

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 left of this Linksys WRT1200AC.

The device that hosts 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, while on Android, you launch Settings, tap Network & Internet > Wi-Fi, 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 will pick the strongest signal. When you move away from an access point, the operating system will 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.

When a device's wireless adapter connects—or *associates*—with an access point, the device can send and receive data with it. If the access point has encryption enabled, then the device must provide either a passphrase (on home and small-office networks) or a user name and password (for corporate or enterprise networks) before the access point allows the device access to its network.

Once a device's adapter connects to an access point and its optional authentication is accepted, the device's operating system proceeds to the next steps. That typically involves the device's operating system requesting an Internet Protocol (IP) address before the device can send data via the wireless network.

Note: With newer adapters, a connection can be made directly to another device 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*.)

Network Basics

You should learn a few other 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 the latest flavor of Wi-Fi, 802.11ac, 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 802.11ac 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.

Wi-Fi Spectrum

When wireless transmissions—originally Morse code 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 require a license in certain circumstances. For example, you might need a license if you're a business or if you want to use Wi-Fi outdoors. If you're not in one of the countries I note, check with the manufacturer of gear you use and the regulator in your country to see if and when your country might require one.

Spectrum *bands*—specified ranges of frequencies with a beginning and ending point—are divided into smaller portions called *channels*, which allow many devices to use the same band within “hearing” distance of each other, ideally without too much frequency overlap. Because unlicensed bands are intended for broad use by individuals and businesses, there's no guarantee that interference won't reduce the speeds you can achieve.

The rule is that in these unlicensed bands, devices use low signal power, which means signals can't differentiate from background

noise and other networks. So the devices also have 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.

In the United States and in most countries, two bands are available for use, the 2.4 GHz (gigahertz) band and the 5 GHz band. The precise frequencies and channels vary enormously by country. Each band requires a different radio systems, and hardware that can communicate in both bands has two radios.

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

Since you may own and encounter different generations of gear (as well as gear at different price points), it's good to understand that not all devices have the same spectrum capabilities. Wi-Fi gateways went through three stages of evolution in how they handled the two bands:

- **One band only:** Early equipment was designed solely to use a single band, almost all of it relying on 2.4 GHz, as 5 GHz equipment was largely intended for corporate networks. (Some inexpensive or compact travel Wi-Fi routers may still be single band.)
- **Switchable dual band:** A single access point could be set to work in either band, offering more flexibility in building and revising networks, but you could only use the access point as a single band (without restarting). Switching between 2.4 and 5 GHz requires changing settings and restarting the gateway. Some very cheap gateways and extenders still have one-band-at-a-time dual-band support.
- **Simultaneous dual band:** Gateways that simultaneously handle data over both bands have been the standard for several years. All the routers I recommend considering for your network work in both bands at the same time.

Note: Mesh networks, described in [Build a Mesh Network](#), offer simultaneous dual band networking, but some models also have an additional radio that uses a separate 5 GHz channel devoted entirely to communicating with other mesh nodes. I discuss this further in that section.

Early adapters had a similar limitation: they started out as single band, almost always 2.4 GHz, but shifted over time to support either 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. Nearly all mobile and desktop Wi-Fi equipment can connect over either band now.

For more on 2.4 and 5 GHz bands, see [Spectrum Trade-Offs](#).

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 802.11a or 802.11g, 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.

Note: Not all the 802.11 lettered standards refer to data rates. Many are defined for other purposes, like security or automatic coordinated channel switching.

These successive 802.11 standards cover the improvements to Wi-Fi data rates from the beginning:

- **802.11b and 802.11a:** The original flavors of Wi-Fi from 1999 worked only in the 2.4 GHz band and 5 GHz band respectively. 802.11b had 11 Mbps of bandwidth and 802.11a, 54 Mbps. You may still find 802.11a in use, but 802.11b should be long gone.
- **802.11g:** Released in 2003, this somewhat faster version of Wi-Fi for 2.4 GHz was coupled with a security improvement, and a top rate of 54 Mbps. It's more common to find older hardware that still relies on 802.11g.
- **802.11n:** 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. New hardware with 802.11n is still sold in 2018.
- **802.11ac, wave 1:** Faster again than 802.11n, this version of Wi-Fi appeared in 2012, but only works in the 5 GHz band. It has many variables manufacturers can choose from to configure, making its bandwidth hard to pin down. Some devices that use it are branded "AC1300" or "AC1450," where the 1300 is 1.3 Gbps and the 1450 1.45 Gbps, as the bandwidth available combining both bands.
- **802.11ac, wave 2:** This even faster flavor of 802.11ac started to appear in mid-2015. It can achieve multi-Gbps throughput with high-end consumer and business devices alongside the right network adapters.
- **802.11ax:** Coming in 2019, this revision dramatically increases throughput yet again by employing several techniques, some of which haven't appeared previously in Wi-Fi. Some access points may be able to push more than 10 Gbps through—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. Unlike 802.11ac, this standard once again functions in both 2.4 and 5 GHz bands.

Coming Soon: 802.11ad

The IEEE has a standard on the horizon for short-range, super-high-speed wireless networks—802.11ad. It will use spectrum way up the dial at 60 GHz for rates as high as 7 Gbps over very short distances, such as within a room. The 802.11ad standard doesn't update Wi-Fi; it's a complementary standard that works alongside it.

Companies have been poised to incorporate 802.11ad into their hardware for years and you'll find a couple of very high-end Wi-Fi gateways that use it alongside 802.11ac. For instance, there's the [Netgear Nighthawk X10](#).

Still, I'm not aware of any major consumer electronics maker that's built 802.11ad into their hardware for streaming to a TV or a streaming-media player that plugs into a TV.

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 those that pass. These tests allow the many makers of Wi-Fi equipment to ensure that all Wi-Fi gear, regardless of manufacturer, can communicate and carry out a common set of tasks in the same way.

Typically, every older version of 802.11 can be used with even the newest access points, although there's a performance cost for that backwards compatibility. Some routers let you turn off support for older standards, particularly 802.11a, b, and g, which are unlikely to remain in use, since almost no hardware that relies on 802.11g has been sold in more than a decade.

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 XR500 has a fancy design, but there's a standard Wi-Fi gateway inside. Most modern gateways have a lot of external antennas.

- **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 may cost two or three times as much as standard gateways and extenders, but they typically require almost no effort (after some 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 of the Linksys Velops mesh nodes.

The Modem You Got from Your ISP

Many internet service providers either offer, support, sell, or require you to use a broadband modem that has Wi-Fi gateway functionality built in. I tend to dislike most of these, because they're designed around what the ISP needs rather than what you need. Also, none of them offer *mesh* as an option.

If you're forced to use one, you must make the same choices as you would with a standard gateway. I recommend disabling the Wi-Fi function on a required broadband modem/gateway. If you can't, lock it down and don't use it. Instead, plug in your own gateway or mesh system.

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 not penetrate walls or floors with enough strength to be useful (**Figure 6**).

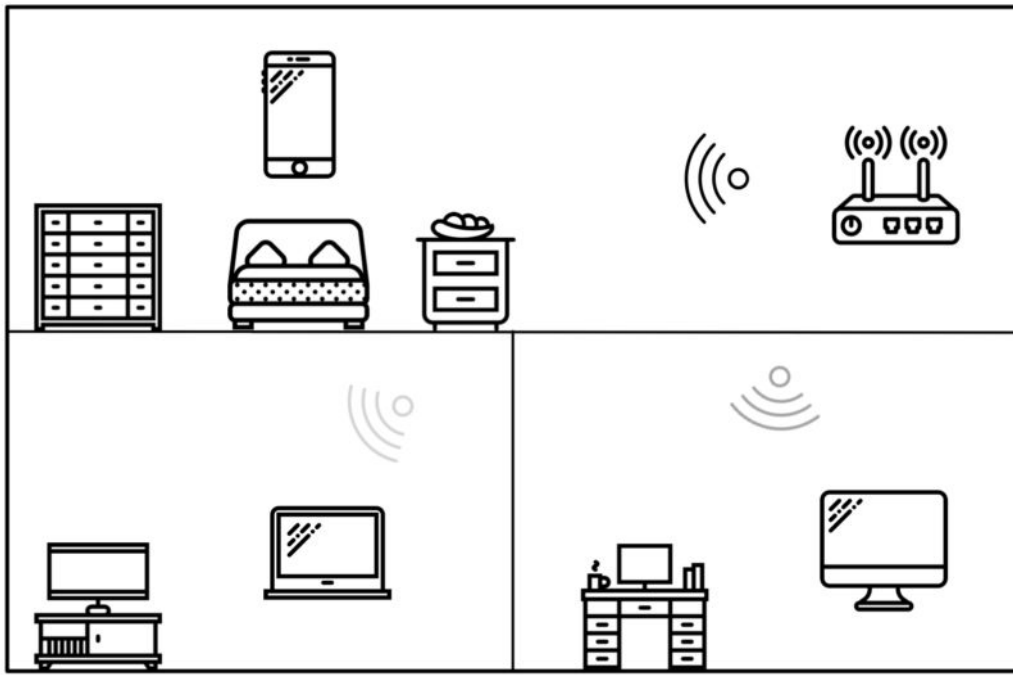


Figure 6: Wi-Fi signals pass through walls and floors more weakly than they do through open space.

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 increasingly the case 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, you might be able to get away 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.
- 2.4 and 5 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. Can you get the faster 5 GHz 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**)?

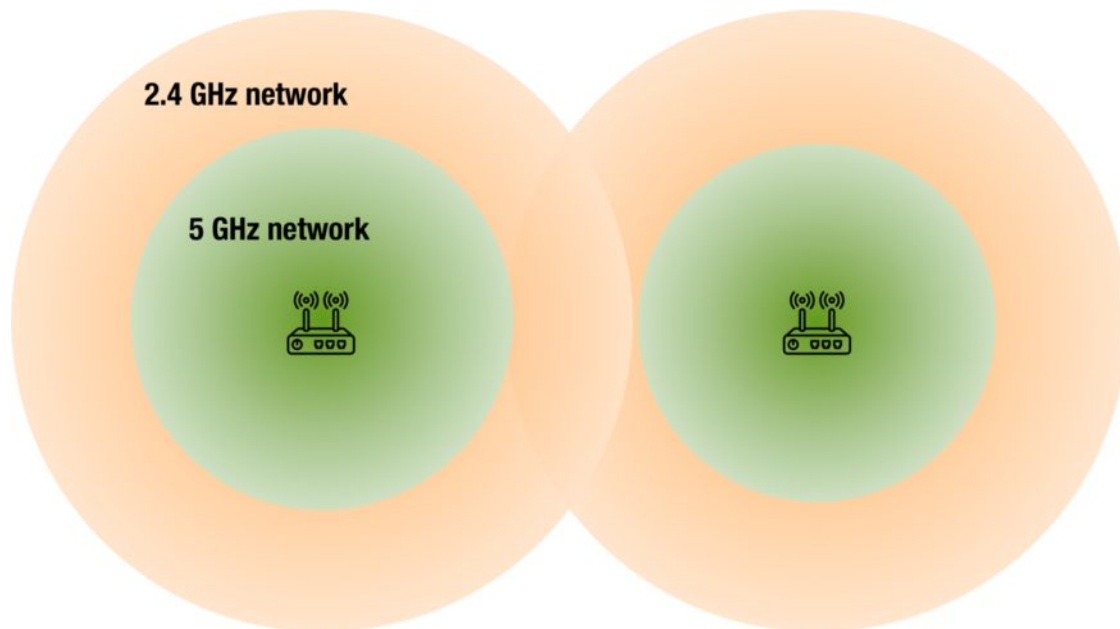


Figure 7: 2.4 GHz networks have greater coverage areas, but 5 GHz networks provide higher throughput.

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 an 802.11ac or later gateway isn't obstructed: it should have

a clear line of sight around it, and not be in 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 gateways—with 802.11ac, and superb throughput—can be very inexpensive.

If you need more than a single gateway, however, standard networks can get complicated. You need to create more configurations that can even involve different kinds of central Wi-Fi stations.

<https://sanet.st/blogs/polatebooks/>

Understand Wi-Fi Network Devices

While I talk generally about *gateways* in this book, when setting up a standard network, you might wind up using a mix of two kinds of Wi-Fi devices:

- Gateways, which as I've already described, combine an access point, network router, and (usually) an Ethernet switch. They're an all-in-one solution, have the best coverage and throughput, and you might only need one per network, near the broadband modem. These gateways can cost as little as \$100, and typically no more than \$150 to \$250 for the fanciest current generation that doesn't have unnecessary extras.
- Range extenders (**Figure 8**) typically lack the routing features of gateways, and have just access point features, sometimes including an Ethernet switch. They cost in the \$25 to \$100 range, and are designed to feed off a main gateway. There are also range extenders that can connect wirelessly by acting as a wireless client and then relaying that single connection to Wi-Fi devices that connect to it. But I highly recommend either a wired connection via Ethernet or powerline connection (see [Connect via Ethernet and Alternatives](#) for details).



Figure 8: A range extender, like this inexpensive TP-Link RE200, has fewer features than a gateway.

Probably Not an Access Point

Corporate networks still rely on access points, which typically are “dumb” devices that accept Wi-Fi connections, sometimes feature several Wi-Fi radios, and pass all routing and other networking tasks back to a central controller. It’s unlikely you want one of these—stick to range extenders.

You will often see gateways, range extenders, and other Wi-Fi hardware all referred to as “access points,” as there’s no strict definition in the marketplace.

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. However, if cost is your principal concern or you’re not concerned about how difficult set up may be, read on.

Picking the Right Hardware

There’s no one right answer here, although unfortunately there are a lot of wrong answers. I used to have a few go-to brands and models aside from Apple’s defunct AirPort line. Now, companies not only introduce new models at an absurdly frequent rate, but they also will keep a model number the same and change out the entire hardware innards of a well-regarded unit, sometimes to increase profit margins and sometimes when original components are no longer available.

As a result, here are the guidelines that I follow:

- Find reviews on sites you trust. I’ve worked for and with [Wirecutter](#) (part of the New York Times); IDG publications [TechHive](#), [PC-World](#), and [Macworld](#); [TidBITS](#); and [Six Colors](#). You may have other sites you read regularly and find their reviews match up with your experience.
- 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.

- If a product has good Amazon and other site reviews, but *none* at major review sites, I typically 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.
- These days, 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.) At this writing, Wirecutter recommends the Netgear R7000P Nighthawk, which marks itself "AC2300," meaning a potential top data rate between both its frequency bands of 2.3 Gbps. While its street price is \$165, the gateway also provided the best throughput across its coverage area of units it tested.

Wirecutter previously recommended the Netgear R6700, which retails for about \$100, but because of a recent update to the hardware, it's unclear if it still performs well.

If you're looking for a range extender, you can pick one of the following:

- For coverage, but not throughput, the \$25 [TP-Link RE200](#) offers 802.11ac (up to 300 Mbps in 2.4 GHz and 433 Mbps in 5 GHz), but only has a 10/100 Mbps Ethernet port. It can connect Wi-Fi devices speedily, but not interlink them at gigabit rates to the rest of your network. But it's well reviewed—and cheap! It has an integral AC plug that may block two outlets due to its shape.
- For better throughput and coverage at a higher price, the [Linksys RE6700](#) (\$65) manages up to 300 Mbps (via 802.11n) in the 2.4 GHz band and 867 Mbps via 802.11ac in 5 GHz. It has a single gigabit Ethernet port, and has an integral AC plug, but a passthrough AC outlet. (The plug may block the second outlet in a two-outlet plate.)

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 (but not all extenders) feature it. However, if you have existing wiring, check what "category" it is: Ethernet wiring from a few years ago might be Cat5, which typically cannot pass more than 100 Mbps Ethernet reliably.

If it's Cat5E or Cat6, you're fine, but also pair that with Cat5E or Cat6 patch cables—the cords that go from the wall into a port on a device—or you'll find yourself having erratic network performance as well.

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.

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 House

We lacked Ethernet in my house. So, when we had some basement refurbishing done, we asked our contractor to pull Ethernet from one end of the house to the other, and between our main floor and our basement. This allowed us to set up three gateways for better coverage with a wired connection via a central switch.

Because my contractor wasn't a network technician, I opted to buy prefab cables and a special kind of wall plate and connector. The wall plate had just a space to snap in a connector, and I purchased an Ethernet inline coupler (female-to-female).

This eliminated any wire crimping. I snapped the inline coupler into the wall plate and plugged a standard Ethernet jack (male) into the side behind the plate. The front side of the wall plate presented a standard Ethernet jack to plug in an Ethernet 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 \$85 (**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.

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.

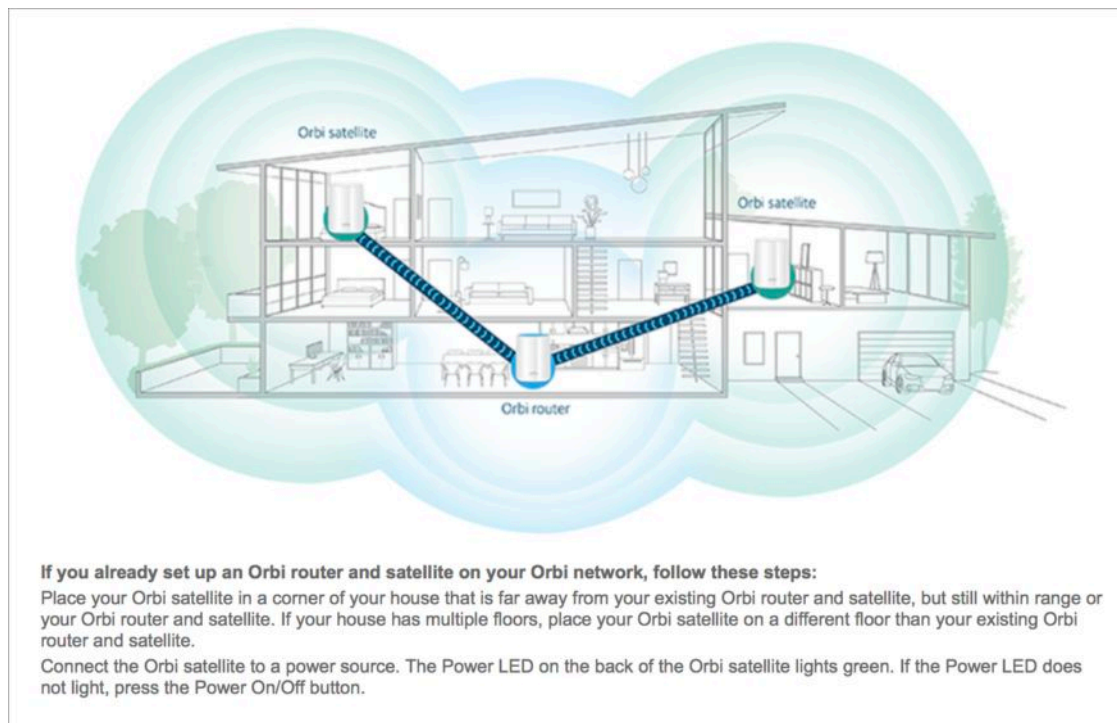


Figure 10: Orbi's administrative interface offers advice on where to place additional "satellite," or less-expensive extender, nodes.

Let's take a quick look at how mesh works, its pros and cons, and which system you might want to pick.

How Mesh Works

Before mesh networks, Wi-Fi had a protocol for connecting access points wirelessly called Wireless Distribution System (WDS). WDS was part of the 802.11b Wi-Fi protocol, but it was never implemented in a standardized way, and didn't become part of the Wi-Fi certification.

Apple offered WDS, and other companies often included it as a feature, but it rarely worked if you were using more than one manufacturers' equipment. Not only was it unreliable, frequently losing connections, but also it had a terrible problem: because it worked over the same Wi-Fi system that wireless adapters connected to, it reduced the throughput available for regular networking.

Even worse, each additional access point through which data hopped had to repeat the data it carried onward. This meant clogging the network with even more data, reducing throughput at a time Wi-Fi already had limited bandwidth.

Mesh lets you do away with most of these problems. Instead of using the hub-and-spoke or daisy-chained approaches of standard Wi-Fi, Ethernet, and other technologies, mesh networks instead 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**).

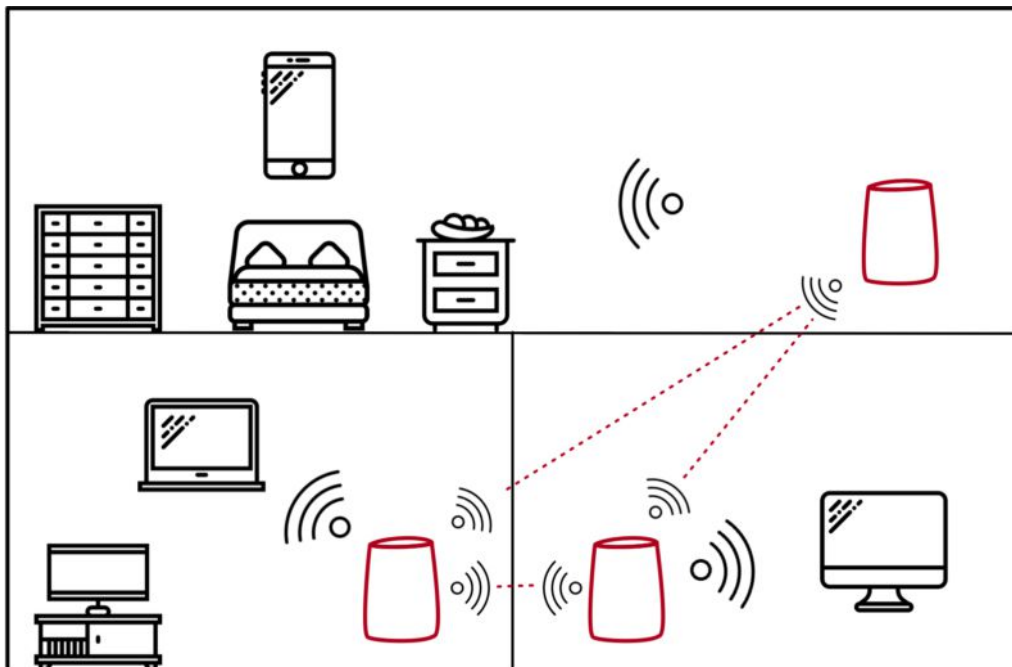


Figure 11: Mesh nodes (in red) can exchange data directly among each other (dotted lines) instead of relaying through intermediates or requiring a central coordinating gateway.

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 GHz and 5 GHz networks used for Wi-Fi with wireless clients. While today's mesh networks are more efficient than WDS ones, 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 GHz channel that's not in use by the node for Wi-Fi for that purpose. (In the mesh system descriptions below, I note the bandwidth each system says its third radio can handle backhaul, if they provide it at all.)
- Backhaul using Ethernet. This sounds contradictory! Why use Ethernet with wireless mesh? Because it can add 1 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 backyard 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 for separate channels within a band. A tri-radio node interacts with wireless clients on a 2.4 GHz channel and a 5 GHz channel, but uses its third radio to transmit data to other nodes on a separate 5 GHz channel.

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. (Some mesh node models can additionally use Ethernet to enhance inter-node communication, as noted above.)
- **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:** I've discussed this tradeoff before, but it's always an issue. You could easily pay two to four times as much for a mesh network as you would for the equivalent, fussier coverage of a standard Wi-Fi network. (You'd also require Ethernet or powerline

networking to interconnect, which has a cost, however.) That said, the price of mesh networking nodes and bundles has dropped and I expect it to become cheaper still.

- **No mixing and matching:** Mesh devices use proprietary protocols, which means you can't mix and match systems. That's poised to change, as a new standard just appeared from the Wi-Fi Alliance, [Wi-Fi EasyMesh](#). This will eventually find its way into future or updated mesh nodes, but not in the immediate future.)
- **One-product, new companies:** Some mesh systems are made by startup companies that have to turn a profit and prove themselves in order to keep making and supporting your gear. The downside of that is that you may be stuck without cloud-based backend device administration tools or lacking security updates if the companies fail. Since mesh devices from one company can't be used with those from other, you'll also be stuck if you want to add nodes and the company's gone out of business. (A company might also sell itself to a bigger firm that creates new, incompatible versions of the hardware or stops updating the bulk of older devices.)
- **The fear of adopting too early:** Even though these mesh systems have 802.11ac networking, the most affordable systems and nodes within the system communicate with other nodes over the same Wi-Fi channels used to handle wireless clients. That reduces throughput. You can purchase more expensive tri-radio nodes, which have an extra radio system that dedicates a separate 5 GHz Wi-Fi channel just to this inter-node backhaul. However, as the price of radio chips and hardware continues to drop, you might be able to get a tri-radio system or one with even more radios for the same price of a two-radio node today. Future mesh nodes could also handle other protocols, like 802.11ad/Wi-Gig for superfast, very close-range networking that allows for ultra-high-definition (UHD) 8K video streaming. Such nodes could also support [ZigBee](#) and other smarthome standards for short-range, low-power control, which currently require a separate coordinating hub.

Which Mesh Systems To Consider

That said, here are three things to think about when picking a mesh networking system:

- Can you tolerate buying from a startup? If so, you'll have more options. If not, there are several mesh systems on the market made by long-established and well-regarded network hardware companies, saving you some of the worry about losing support.
- Do you want or need the maximum possible throughput for transferring extremely large files, handling backups, or streaming high-definition video? That requires either nodes with three radios or nodes that allow Ethernet for backhaul, some of which can be simultaneous with a radio for even better performance.
- How much money do you have in your pocket? You can spend roughly from \$50 to \$150 per node.

At this writing, the four systems that fit these criteria in different combinations are Netgear Orbi, Eero, Linksys Velop, and TP-Link Deco M5. Let's take a look at each one.

Disclosure: I Don't Have a Mesh Network

I have to be fully honest about my home network: it relies on standard equipment. While I've tested Wi-Fi hardware for nearly 20 years, I have a working network with two Apple base stations, one TP-Link gateway, and a CenturyLink-provided gateway required to work with its fiber network.

With great coverage across my home and a gigabit internet connection, I haven't needed to switch over. At some point, I'll be making the leap, but I demonstrate one of my earlier points: if you have a working network, there's really no need to spend hundreds of dollars to put together another working network.

To inform this section, I've relied on Take Control owner Joe Kissell, (who loves his Orbi), reader recommendations, Wirecutter, and reviewers at Techhive/PCWorld.

Note: Model numbers and prices change rapidly. What you see here reflects the best information available in May 2018.

Netgear Orbi

The [Netgear Orbi](#) is made by a major hardware maker with decades of experience creating and supporting networking equipment for the consumer market. For this reason, it's often the first and best choice when you want a mesh system, but it's not inexpensive (**Figure 12**).



Figure 12: If you want to create a mesh network, the well-established Netgear Orbi comes in several models. This is the RBK50 starting kit.

The Orbi system has several models, and some are only sold in packs of two, making figuring out what you need a little more confusing as you get started, because you have to make the right choice out of the gate.:

- The RBK50 kit (\$300) includes two tri-band devices: a router and what Netgear calls a “satellite,” which is a smaller, but fully independent mesh node. Its Wi-Fi connections achieve up to 400 Mbps in 2.4 GHz and 866 Mbps in 5 GHz. Both devices in the kit have four gigabit Ethernet ports, one of which is a WAN port on the router. They have 1.7 Gbps wireless backhaul and support backhaul over Ethernet. Netgear says that signals from the two can cover 5,000 sq. ft.
- The RBK30 kit (\$250) is nearly identical, except it offers 866 Mbps wireless backhaul and slightly less powerful antennas, with a coverage area (says Netgear) of about 4,000 sq. ft.

- You can also buy various tri-band satellite models, including the ones that ship as part of the two kits above (the RBS50 [\$215] and RBS40 [\$200], respectively). There's also a version that has an integral AC plug (model RBW30, \$140). Netgear also offers a \$300 kit that includes the RBK30 router and two RBW30 satellites.

Eero

Another well-reviewed company that offers mesh system is [eero](#), a startup firm. It's more than three years old, and has released generations of hardware. Still, it had layoffs in early 2018, and it's too early to tell whether it will ultimately be profitable or acquired by another firm. Its devices costs about as much as the Orbi nodes.

It's easier to pick between eero's mesh options as offers just two: the eero and Beacon (**Figure 13**).



Figure 13: Startup eero offers two models of mesh nodes, the eero (left) and the Beacon.

Here's the differences between the two models:

- The eero model is tri-band, and offers up to 240 Mbps over 2.4 GHz and 600 Mbps over 5 GHz. The company hasn't provided any details about how fast its backhaul is, which means it's likely in the 600 Mbps range. It can also use either or both of its gigabit Ethernet ports for backhaul.
- The Beacon is dual band without Ethernet, so its backhaul has to share bandwidth with Wi-Fi clients. It has an integral AC plug.

You can buy an eero plus a Beacon for \$300, an eero and two Beacons for \$400, or three eeros for \$500.

At this writing, the eeros seems slightly overpriced compared to Netgear Orbi's offerings based on range and throughput. I'd recommend reading testing-site reviews carefully to see whether the difference between the two systems is worth the additional premium.

At this writing, [Wirecutter made Orbi its top pick](#) partly because the eero has some dependency on internet connectivity.

Linksys Velop

Linksys has decades of experience selling consumer networking gear, though the company was sold to Cisco in 2003, which in turn sold it to Belkin in 2013. At this writing, the manufacturing giant Foxconn is awaiting approval to purchase Belkin, including the Linksys products.

The [Linksys Velop](#) mesh system isn't cheap, but it has received stellar marks for throughput—such as in [this TechHive review](#)—so if that's one of your primary issues, it might be your pick.

Linksys offers one model that is triband with two gigabit Ethernet ports (**Figure 14**). The Wi-Fi service is up to 400 Mbps over 2.4 GHz and 867 Mbps over 5 GHz. The wireless backhaul is 867 Mbps, but it also handles backhaul via its Ethernet ports.



<https://sanet.st/blogs/polatebooks/>

Figure 14: The Linksys Velop mesh system offers great throughput.

Velop comes as a \$300 pack of two and \$500 pack of three. You can buy additional units for \$200 each, so the three pack is no bargain.

Note: As I write this, Linksys is just about to release a dual-band Velops model that runs \$300 for a three-pack, but it's too early to know how well it performs.

TP-Link Deco M5

If throughput isn't your top criterion, the [Deco M5](#) might be the right choice: it's inexpensive for mesh, but performs well, and comes from TP-Link, a veteran tech hardware company that's been selling networking equipment in the U.S. for several years.

There's one model that has dual-band Wi-Fi and backhaul (up to 400 Mbps in 2.4 GHz and 867 Mbps in 5 GHz), as well as two gigabit Ethernet ports. It also supports backhaul over Ethernet (**Figure 15**).



Figure 15: If price matters more to you than throughput, check out the TP-Link Deco M5 mesh system.

A three pack of nodes is just \$230, making this the cheapest mesh system by far. Additional units cost \$100 for one and \$180 for two.

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.)

Choosing Between the Bands

Let's begin by comparing the two bands. The 2.4 GHz band is crowded with Wi-Fi networks, Bluetooth devices, and other uses. 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.

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 16**).

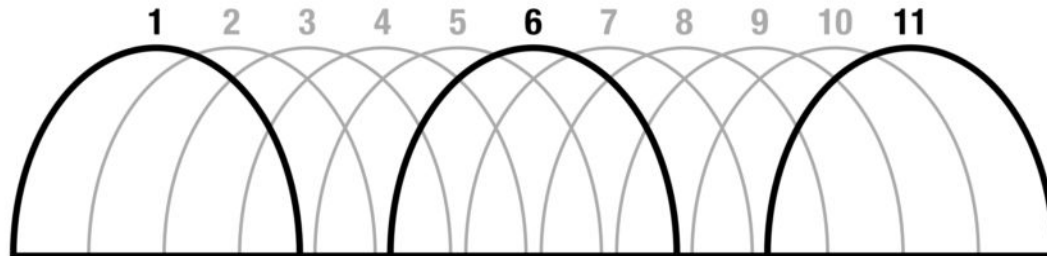


Figure 16: The 2.4 GHz band has overlapping channels, and in America, only three can be used effectively at the same time. (Channel separation exaggerated here for clarity.)

In the 5 GHz band, Wi-Fi standards only use non-overlapping channels, which makes the band easier to work with (**Figure 17**). However, the complexity of channel allocation, division into segments, and the use of wide channels (see sidebar, below) can be a little overwhelming, as you can see in that 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.

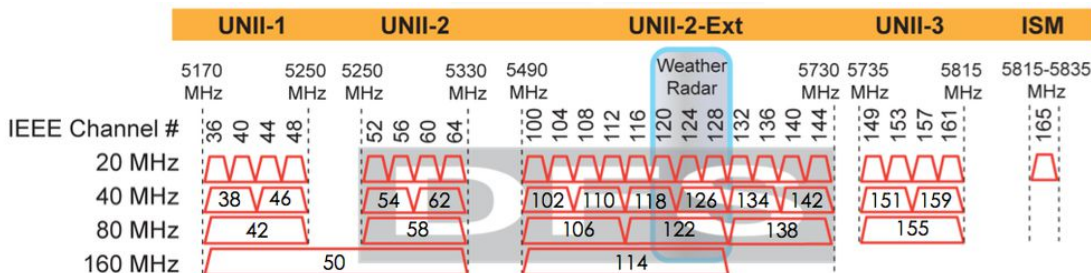


Figure 17: The 5 GHz band looks complicated, but is actually simpler to use. In the first row of the graphic, you see all the 20 MHz channels among which you can choose. The wider channels in the next row are automatically picked. (Graphic by Andrew von Nagy.)

Other Uses of the 2.4 and 5 GHz Bands

The 2.4 GHz and 5 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. (There are many other junk bands, too, most not used for networking.)

Problems with Wi-Fi networks often stem from your own or your neighbors' use of conflicting technology, including 2.4 GHz cordless phones, microwave ovens, and wireless cameras. Nearby industrial sites can send off signals that conflict, too. The 5 GHz band has many fewer approved uses; your primary enemy will be 5.8 GHz cordless phones.

What's a Wide Channel?

Starting with the 802.11n Wi-Fi standard, Wi-Fi can use *wide channels*, too. These are multiples of the existing 20 MHz channels bound together to carry greater amounts of data (see **Figure 17**, above). An access point could use double-wide 40 MHz channels in 802.11n. That expanded to 160 MHz in 802.11ac. (Nearly all 802.11n access points offered wide channels only in 5 GHz, even though 2.4 GHz could support one or two 40 MHz channel, depending on the country.)

These extra widths allow for substantial, almost linear increases in throughput: literally, two times the channel width can mean two times the throughput, and so on. Later standards can also use 20 MHz channels that aren't right next to each other, or *adjacent*, to create a wide channel.

Maximizing Throughput

The 5 GHz band offers 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 802.11n rate happens when a wireless adapter and access point use the 5 GHz band with 40 MHz, and the highest

802.11ac rate happens with 5 GHz and 160 MHz. The same will be true with 802.11ax.

Dealing with Distance

Wi-Fi performs at its highest rates the closer you are to an access point. For newer flavors of 802.11, 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, table, 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. 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 17**.) 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 802.11n, ac, and the upcoming ax can all dynamically stretch from 20 MHz to as wide as to 160 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.

Troubleshoot Your Connections

In [Make a Plan](#), I discussed how to figure out the best placement of your Wi-Fi networking 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 802.11ac. 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) 802.11 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 ratio between the two, the signal-to-noise ratio (SNR), defines the space in which information can pass.

Note: 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*.

Testing from Device to Access Point

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

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 shows you information about every access point it can detect, and visualizes channel usage as physical layout on a map you provide or using other layout options (**Figure 18**).

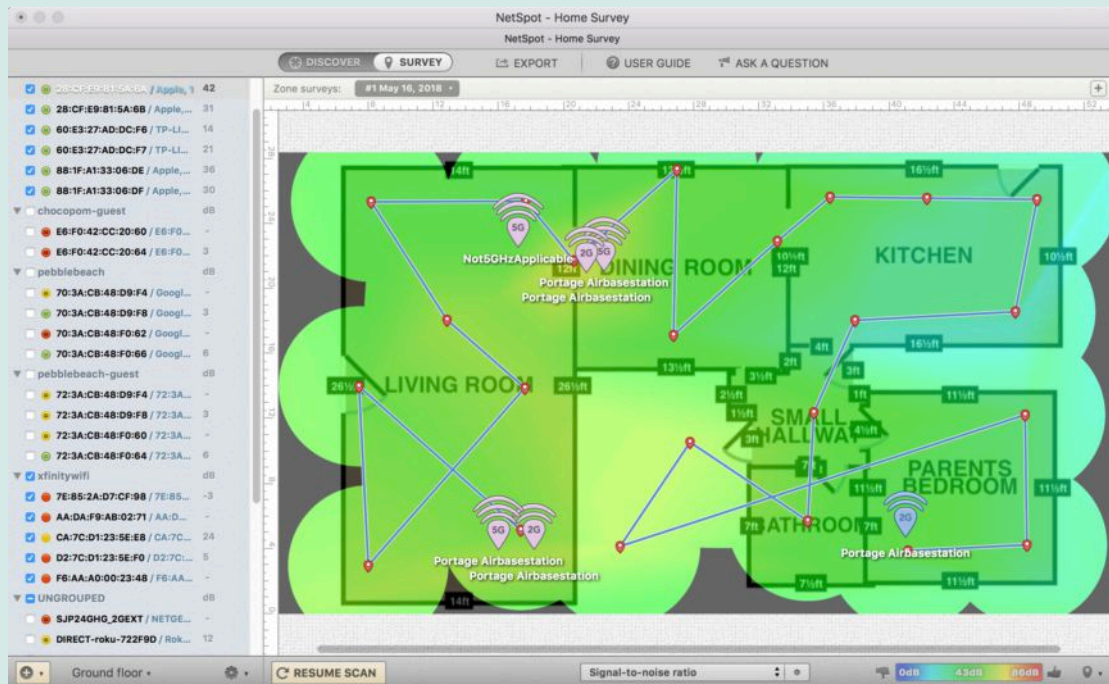



Figure 18: NetSpot lets you map out coverage areas of an existing network, and see incursions from nearby networks.

NetSpot ranges from \$49 for a home version to \$499 for an enterprise flavor.

When you want 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 Wi-Fi  menu in 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 19**).

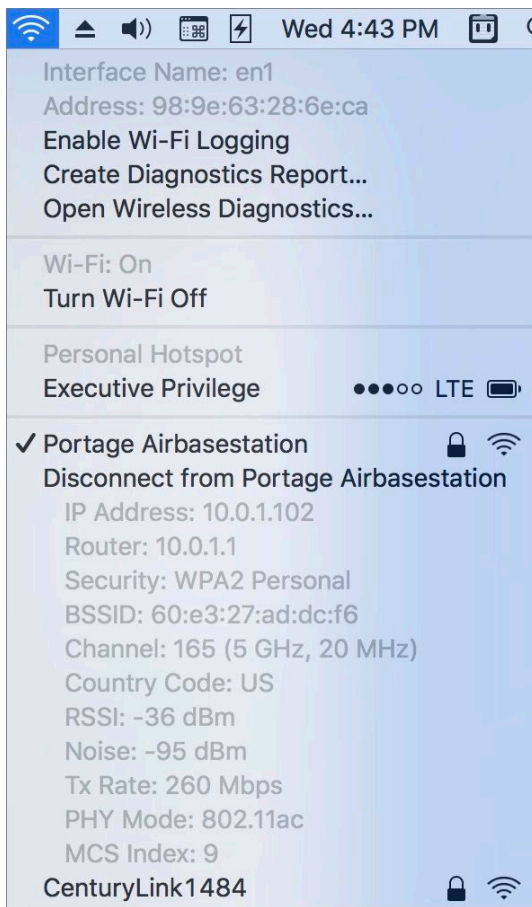




Figure 19: If you hold down Option before selecting Wi-Fi in your Mac's menubar, you'll see a lot of useful information.

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.

- **In Windows 10:** The Wi-Fi status dialog tells you the current connected data rate (**Figure 20**). To find it, click Start, and then select Settings > Network & Internet > Status > Network and Sharing Center. Next to Connections, select your Wi-Fi network's name.

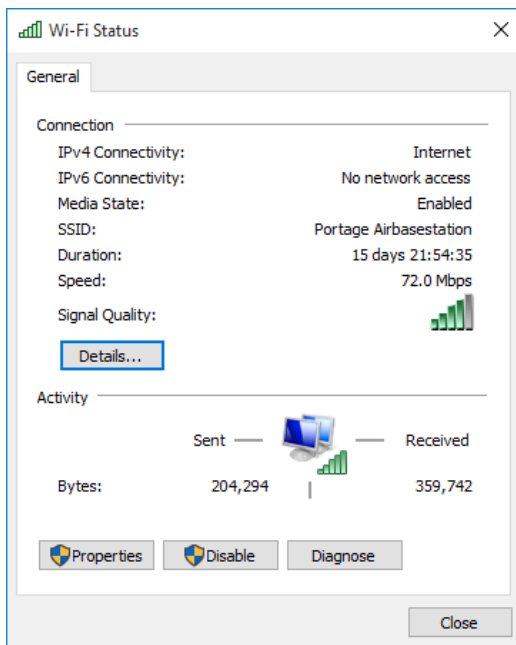


Figure 20: Open Wi-Fi Status via the Network and Sharing Center to see more detail about your Wi-Fi network.

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

- **In iOS:** When you're using an iOS device like an iPhone or iPad, third-party apps are the way to go. The folks at NetSpot [have compiled a handy list](#) of recommended Wi-Fi scanning apps that range from free to about \$6.
- **In Android:** Again, the OS offers little insight—just the connection speed if you dig down deeply—so turn to the well-reviewed [Wifi Analyzer](#) (ad supported) (**Figure 21**).

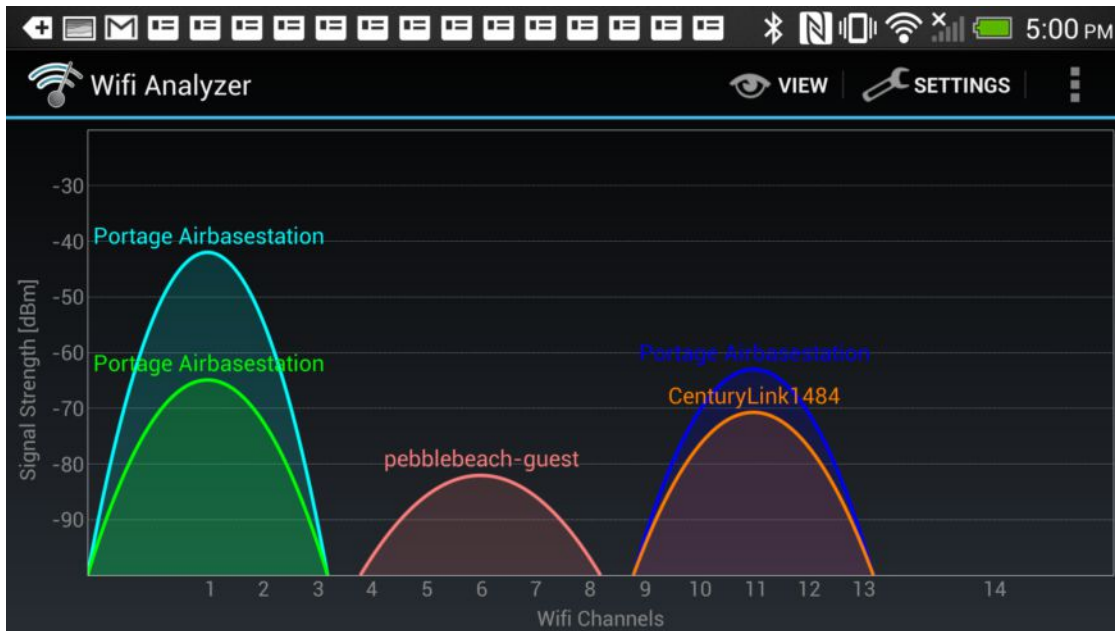


Figure 21: If you're using an Android device, the Wifi Analyzer app offers a graphical snapshot of your current Wi-Fi environment.

Testing from Network to Client

Depending on the model of gateway or other device you have, you might be able to use your network hardware's administration software to see how well clients are connecting.

Some have no information whatsoever—the TP-Link router on my network lists clients in a few ways, but offers no connection insights. When I spot-checked Linksys and Netgear routers, I got the same result.

Apple's discontinued AirPort line, on the other hand, offered extensive details. If you own AirPort gear, here's how to find that information in AirPort Utility:

- **In macOS:** Select a base station to see a list of any connected hardware beside the Wireless Clients label. Hover over, but do not click, any client name, and a floating panel appears (**Figure 22**), showing connection details: the data rate, RSSI, and PHY mode, as described earlier in this section. You can also see this information in AirPort Utility's Summary pane by Option-clicking the Edit button.

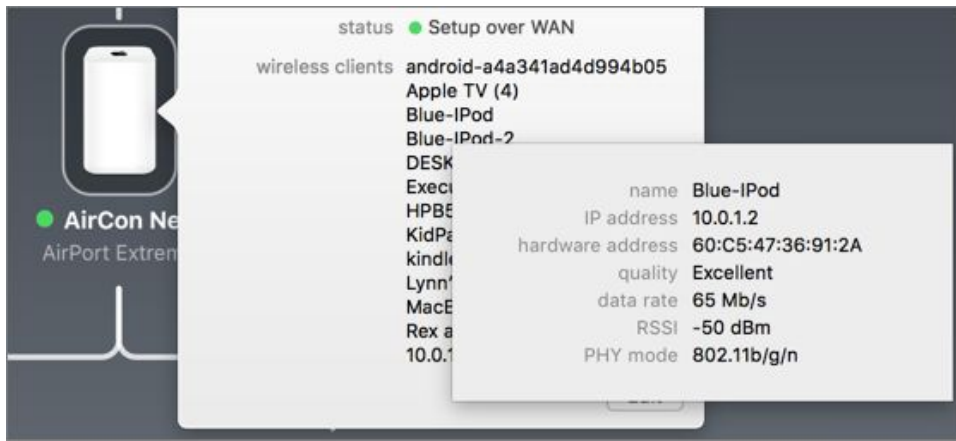


Figure 22: In AirPort Utility for Mac, the Wireless Clients entry shows connection information. Wow, that’s a lot of clients for a family of four in a small house!

- **In iOS:** Select a base station, then tap Wireless Clients (you may have to slide down), and then tap a client name. Then tap Connection to get the details on Data Rate, RSSI, and (PHY) Mode (**Figure 23**).

Blue-iPod Connection	
Data Rate	43 Mb/s
RSSI	-69 dBm
Mode	802.11b/g/n

Figure 23: AirPort Utility for iOS gives a little more information than the Mac version.

<https://sanet.st/blogs/polatebooks/>

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.)

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.

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.

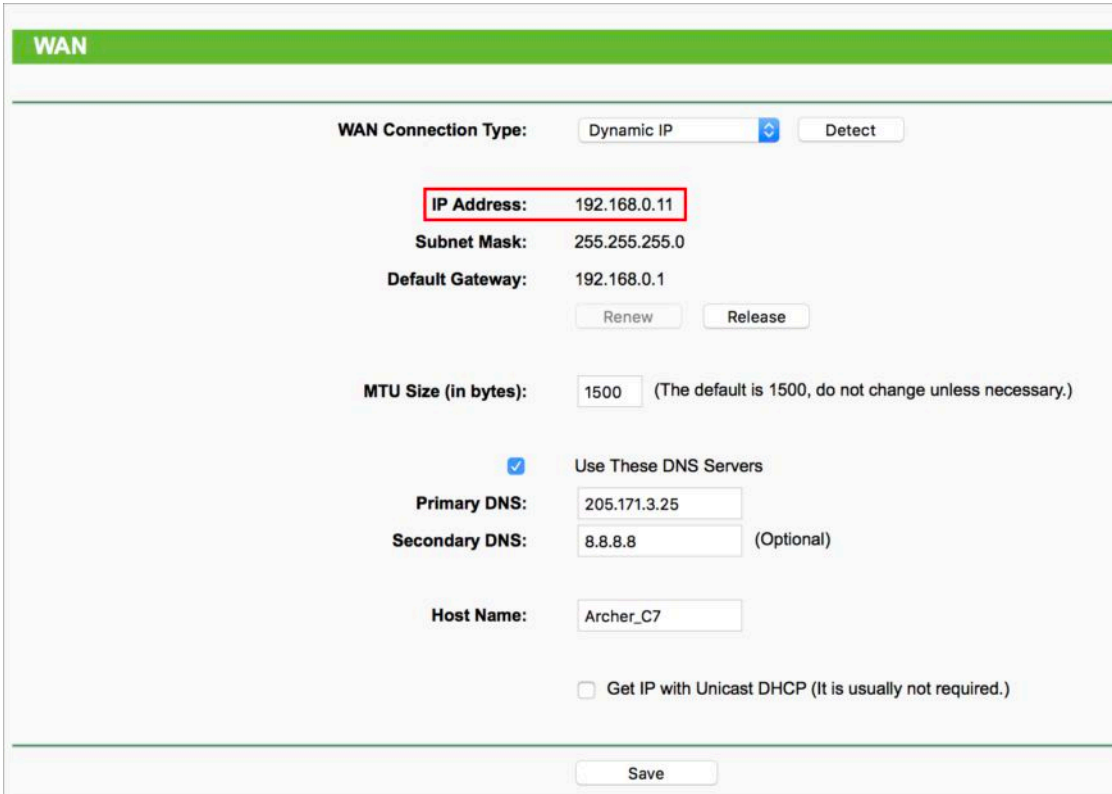
Dynamic Addressing

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 24**).

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.



The screenshot shows the WAN configuration interface. At the top, there is a green header with the text "WAN". Below this, the "WAN Connection Type" is set to "Dynamic IP" with a dropdown arrow and a "Detect" button. The "IP Address" field is highlighted with a red box and contains the value "192.168.0.11". Other fields include "Subnet Mask" (255.255.255.0), "Default Gateway" (192.168.0.1), and "MTU Size (in bytes)" (1500). There are "Renew" and "Release" buttons. The "Use These DNS Servers" checkbox is checked, with "Primary DNS" (205.171.3.25) and "Secondary DNS" (8.8.8.8) fields. The "Host Name" is "Archer_C7". At the bottom, there is a "Save" button and an unchecked checkbox for "Get IP with Unicast DHCP (It is usually not required.)".

Figure 24: 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 the underlying numeric addresses and other details required for machine-to-machine connections.

DNS software takes the name and looks up the machine-usable information, such as an IP address, used to make a connection—like a web browser needing the address to connect to a web server.

If your gateway obtains its address via DHCP, it will likely also get the ISP's default DNS values. You can find these values typically in a printed welcome packet or an email message when you start service with an ISP.

You may want to override these provided servers with other DNS servers, as your ISP's DNS servers may be slow or lack modern security options now available from so-called *public* DNS services. These include [Google Public DNS](#), [Cloudflare](#), and [Quad9](#), all of which are free and fast. (You can read more about the free offerings in an article I wrote for TidBITS in April 2018: "[Cloudflare and Quad9 Aim to Improve DNS](#).”)

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 25**).

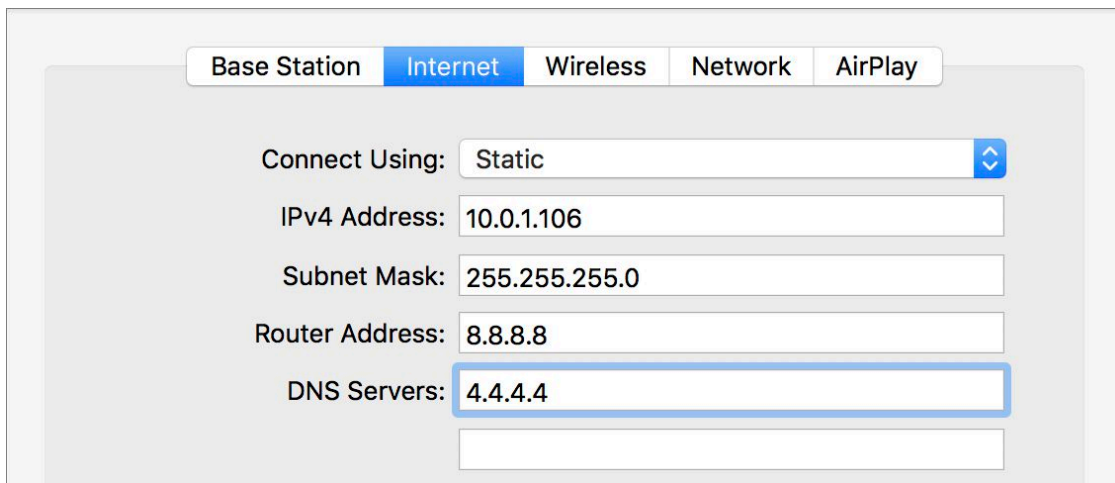


Figure 25: Setting a static address can be as simple as selecting Static from a pop-up menu and entering necessary values. (This screenshot is of AirPort Utility in macOS.)

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

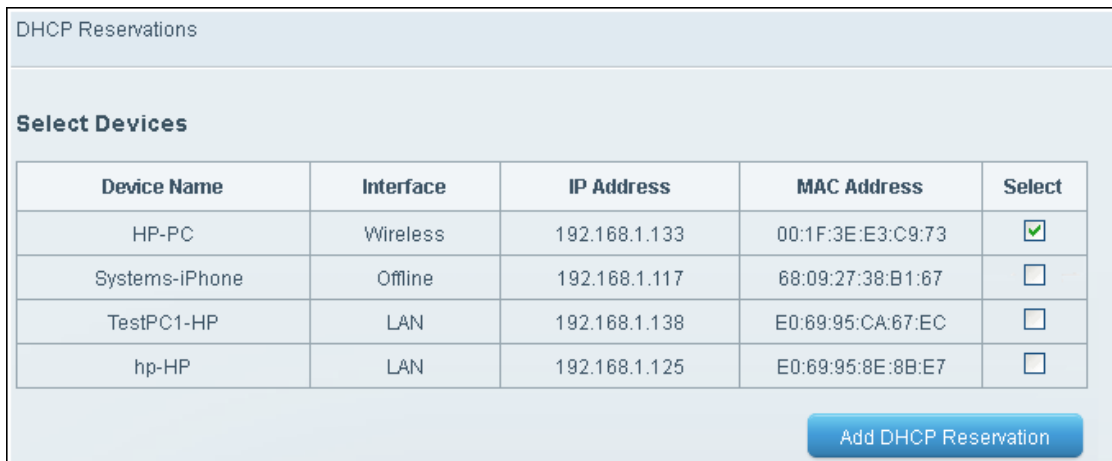
Reservation allows a given device on a network to obtain the same IP address, whether public or private, each time it joins the network. This works whether or not you share the access point's connection or distribute a range of addresses, but it does require DHCP service to be turned on.

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 26**).



Device Name	Interface	IP Address	MAC Address	Select
HP-PC	Wireless	192.168.1.133	00:1F:3E:E3:C9:73	<input checked="" type="checkbox"/>
Systems-iPhone	Offline	192.168.1.117	68:09:27:38:B1:67	<input type="checkbox"/>
TestPC1-HP	LAN	192.168.1.138	E0:69:95:CA:67:EC	<input type="checkbox"/>
hp-HP	LAN	192.168.1.125	E0:69:95:8E:8B:E7	<input type="checkbox"/>

[Add DHCP Reservation](#)

Figure 26: 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. Likewise, Apple's Wi-Fi base stations can use that DHCP ID to reserve an address.

<https://sanet.st/blogs/polatebooks/>

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](#), [Connect in Windows 10](#), [Connect in Android](#), and [Connect in Chrome OS](#).

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 choosing it from the Wi-Fi  menu on the system menu bar. Macs continuously look for networks, and a list of any yours has currently found appears in this menu when the Wi-Fi adapter is on (**Figure 27**). (If it's off, click the Wi-Fi  menu and then choose Turn Wi-Fi On.)

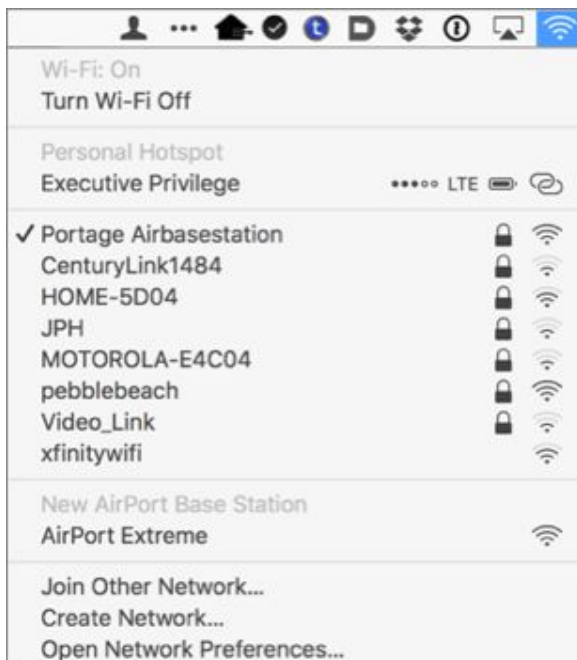





Figure 27: On a Mac, choose a network from the list or choose Join Other Network and enter a closed network’s name.

Tip: If you don’t want your Mac to show you new Wi-Fi networks whenever you’re not connected to one, go to Apple  > System Preferences > Network > Wi-Fi and uncheck “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.

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

Warning! Public Wi-Fi networks won’t appear in the Devices list. If you see a public-sounding network there, it’s likely a compromised computer, a bad configuration, or a hacker trying to get you to connect to a [honeypot](#).

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.


Store and Retrieve Your Passwords

If you don't want to type in your network password in the future, store it in your Mac's Keychain by leaving the "Remember this network" box checked.

Now, whenever you want to delete a password you don't want or retrieve one you've forgotten, you can open the Keychain Access app (found in [/Applications/Utilities/](#)) and get to work.



Keychain passwords are secured with your macOS user password, unless you set a special Keychain password, which you can do in Keychain Access by choosing Edit > Change Password for Keychain "*keychain name*".

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. You can change that via these steps:

1. Go to Apple  > System Preferences > Network.
2. Click the Wi-Fi adapter's entry in the list at left.
3. Click the Advanced button at right.
4. In the Wi-Fi tab, scroll to the network name in the Preferred Network list.
5. Select the name and then click the minus sign button to remove it.
6. Click OK and then click Apply.

You're immediately disconnected. If you use iCloud Keychain, the Wi-Fi network entry is removed from all connected devices, too.

While still in range, you may disconnect from a network in a couple of ways:

- Hold down the Option key and open the Wi-Fi  menu. The menu item *Disconnect from Current Network Name* appears. This menu item also appears without the Option key if the Mac is connected to a Personal Hotspot. Choose it, and the Mac is disconnected from the network and will not re-join it unless you select it again or the device leaves the range of the network and returns.
- Choose *Turn Wi-Fi Off* from the Wi-Fi  menu. This disables the device's network connection entirely.

Connect in iOS

iOS lets 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, iOS pops up a dialog asking if you want to join. Tap the network you want, and enter a password if one's requested.

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 28**).




Figure 28: The Wi-Fi view in iOS lets you tap a network to join.

2. Select the network from the Choose a Network list by tapping it. (If the network you're trying to find doesn't appear, tap Other—you may have to slide down to find Other.)
3. Enter a password if prompted.

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

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 in iOS, either on an iPhone 4 or later, an iPad mini, or a third-generation iPad or later. Personal Hotspot lets the iOS device 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.

Forget a Network in iOS

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

1. Tap Settings > Wi-Fi.
2. Tap the blue info ⓘ icon by the currently connected network.
3. Tap Forget This Network.

iOS 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 from a Network in iOS

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

- Swipe up 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. Starting in iOS 11, if you

press deeply or touch and hold the network card in the upper-left corner, a larger display appears showing the network symbol and the message “Not Connected” beneath it. Tap again to re-connect; it will also be re-enabled the next morning automatically.

- 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 10

To connect to a network in Windows 10 or later, follow these steps:

1. Click the Wi-Fi menu in the System Tray.
2. A Networks pane appears, showing available Wi-Fi networks (**Figure 29**).

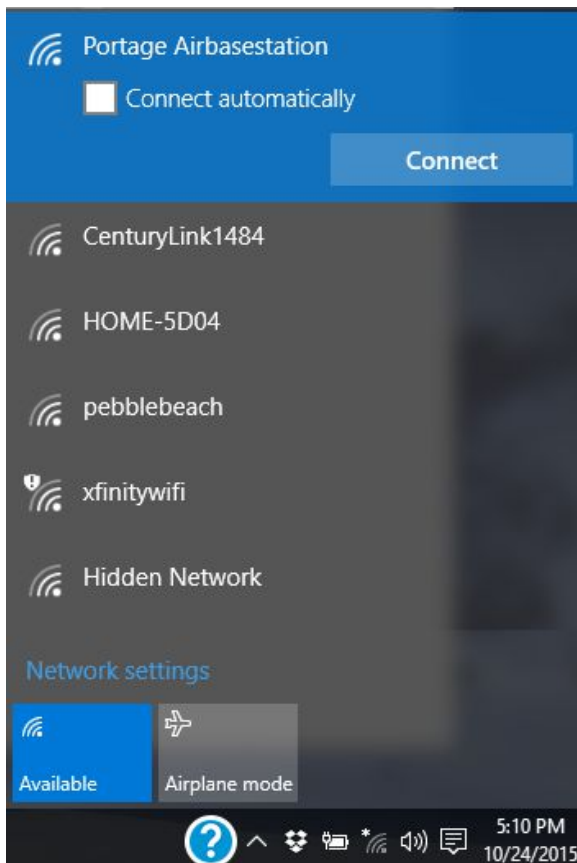


Figure 29: The Windows 10 Networks pane shows which network is connected, if any (Portage Airbasestation in this case), as well as the names of any other available networks.

3. Click the network to which you want to connect, and optionally select the “Connect automatically” checkbox. Then, click the Connect button.
4. Enter a password, if prompted, and click Next (**Figure 30**). Windows automatically figures out the right type of passphrase to send.

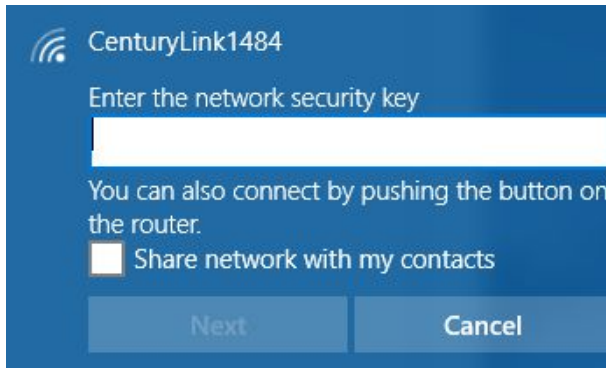


Figure 30: Enter the network’s security key and click Next.

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

Note: Microsoft added the “Share network with my contacts” option in Windows 10, as shown in the figure above. For password-protected networks, you can automatically provide access to Outlook.com contacts, Skype buddies, and Facebook friends (or any one or two of those three categories). Unless you’ve been given permission to share a network, don’t check that box.

Forget a Network in Windows 10

Windows 10 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. Click the Wi-Fi menu in the System Tray.
2. Click Network & Internet Settings.
3. Scroll down, if necessary, to find “Manage Wi-Fi settings” and click that.

4. Under “Manage known networks,” click the network name and then click Forget.

Windows immediately disconnects from the network.

Disconnect from a Network in Windows 10

To disconnect from a network in Windows 10, you can choose either of the following methods:

- Right click the connected network and click the Disconnect button.
- Click the blue box in the lower-left corner of the Wi-Fi pop-up menu, which shows the name of the network. This turns Wi-Fi off, disconnecting and disabling.

If you don’t see any Wi-Fi networks listed, make sure the button in the lower-left corner of the pop-up menu reads Available.

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 Wi-Fi. A list of networks should appear (**Figure 31**).



Figure 31: 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 32**). Tap it in, and tap Connect.

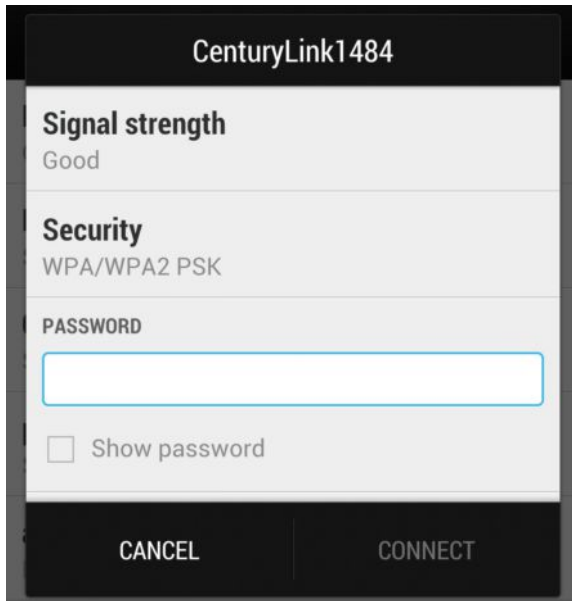


Figure 32: Enter the password and click Connect.

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. You're immediately disconnected.

Disconnect from a Network in Android

To disconnect from a network in Android, you do either of the following:

- Tap the network name and then tap Disconnect.
- Tap the switch at the top of the Wi-Fi list, which turns Wi-Fi off and thus disconnects the network.

Connect in Chrome OS

Google's Chrome OS runs the many inexpensive, powerful, cloud-connected notebook computers known collectively as Chromebooks, though they are made by many different hardware manufacturers.

You can easily connect from Chrome OS to an Apple base station, just as to any other Wi-Fi router. Follow these steps, which are quite similar to Android, but not identical:

1. In the lower-right corner of the screen, click your avatar's icon (**Figure 33**).

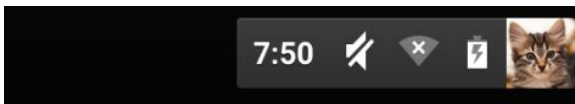


Figure 33: The status bar shows network status, including this x'd out icon if there's no currently connected network.

2. A panel appears, showing the current state of the Chromebook (**Figure 34**). Click the network area, which may show a Wi-Fi network name or say "No network."

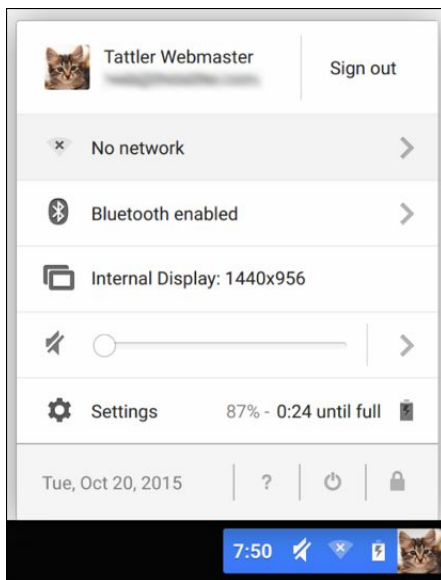



Figure 34: The Chrome OS status area includes networking information.

3. A list of available networks appears. Click the network you want to join (**Figure 35**) or tap Join other  to enter a closed network's name.

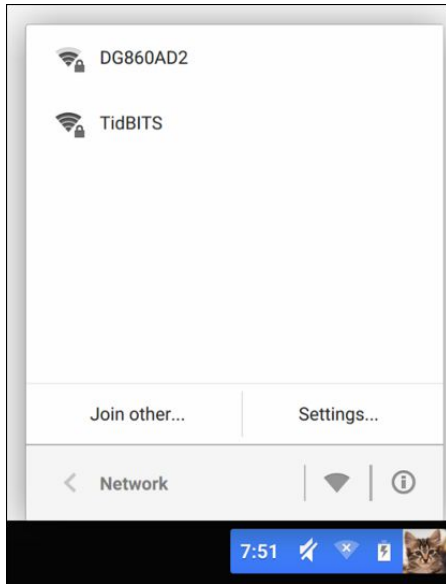


Figure 35: Chrome OS displays available networks.

4. If the network is password protected, you're prompted to enter that password (**Figure 36**). (Click the “eyeball” icon to see the password as you type.)

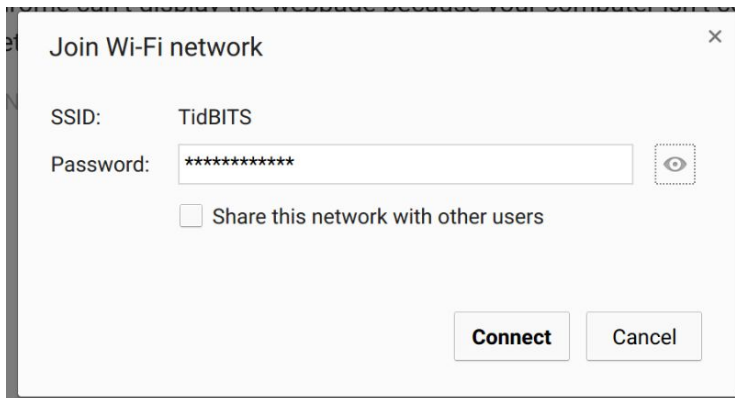


Figure 36: Enter the network password when prompted.

5. Click Connect.

If the password was entered correctly and the network is working properly, the Chromebook connects to the network. You can click the status bar to confirm the connection (**Figure 37**).

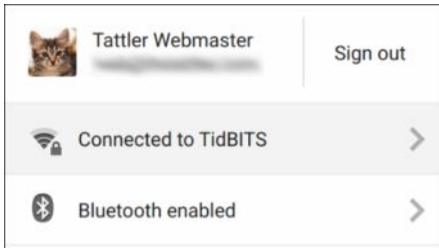


Figure 37: Now, a Connected message appears in the status panel.

You can optionally type <chrome://settings> into the browser location bar and click Add Wi-Fi to add a network.

Forget a Network in Chrome OS

In the Wi-Fi network list, click the network name, and then click Forget.

Disconnect from a Network in Chrome OS

To disconnect, click the network name and then click Disconnect.

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 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 gives you 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.

On the Mac, Go to Apple  > System Preferences > Sharing. Select the Internet Sharing checkbox. Select the network to share from (like Ethernet) in the pop-up menu, and then check the box next to Wi-Fi in the To Computers Using list. Then click Wi-Fi Options and set a password. Finally, check the box 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 10 to the latest release.)

Turn on Hotspot Sharing

Here's how to turn on the hotspot feature in iOS 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


In iOS, open Settings, tap Personal Hotspot, and tap the button to enable it. iOS sets a default password; you may want to change this to something more memorable or easy to enter. iOS always sets the name of your hotspot to the device's name (**Figure 38**).



Figure 38: iOS lets you flip on Personal Hotspot with a tap and set a password. It also has instructions (Wi-Fi shown) on how to configure different settings and use tethering.

Tethering via USB is always available and can't be disabled, but you can turn off Wi-Fi or Bluetooth (or both) to disable wireless tethering and limit it to USB.

Enable in Android

Android requires a few more steps. In Settings, under Wireless & Networks, tap More and then tap "Mobile network sharing. Tap "Portable Wi-Fi hotspot" to enable the hotspot, or tap "Portable Wi-Fi hotspot settings" to change the network name, security method and password, as well as to manage users (**Figure 39**). You can also tap the More Options  menu and tap Advanced. From here, you can modify additional items, like the Wi-Fi channel and DHCP service over the WLAN.

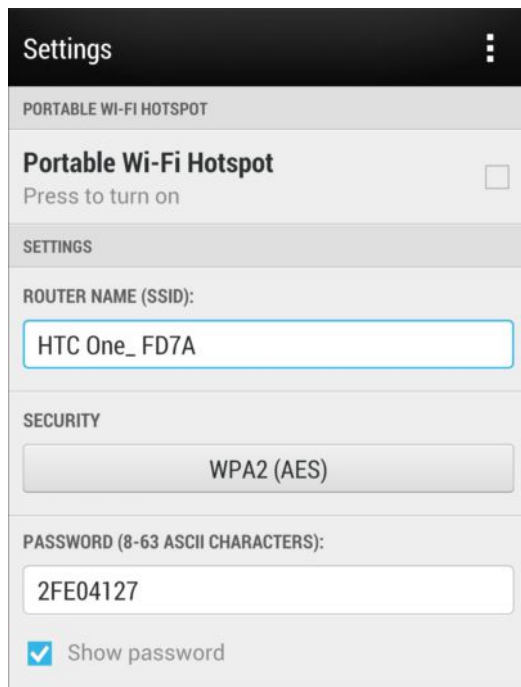


Figure 39: Android’s Portable Wi-Fi Hotspot allows more settings than iOS, including choosing a security method.

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 and macOS, an iPhone hotspot appears in the Wi-Fi list in a special place (under a Personal Hotspot label) and with a special icon (interlocked chain icon (**Figure 40**)).

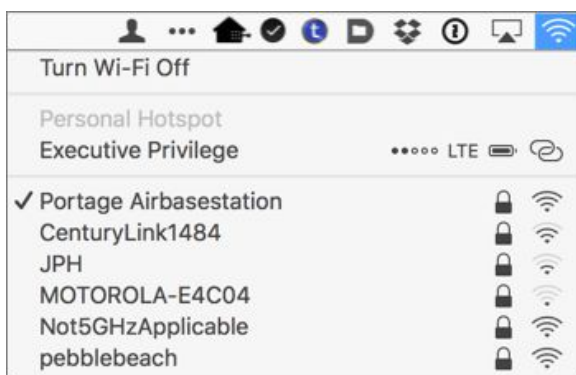


Figure 40: Select the hotspot under Personal Hotspot. In this case, you'd choose Executive Privilege.

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 and plug the device in to a Mac via USB, macOS alerts you that the interface is added and the Mac's System Preferences > Network pane adds an adapter entry to the list on the left (**Figure 41**).



Figure 41: An entry appears in the adapters list to the left.

macOS automatically activates a tethered link and turns that red dot green.

Note: If you're not seeing this, you may need to launch iTunes the first time you tether. iTunes doesn't seem to have anything to do with USB tethering except initial activation.

You can disable the iOS adapter profile to prevent a re-connection. In System Preferences > Network, select the iPhone USB or iPad USB adapter, and then from the gear ⚙️ pop-up menu, choose Make Service Inactive. Click Apply in the lower-right corner.

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

Pairing used to be incredibly frustrating and complicated, requiring as many as 15 steps on some devices! Now, it's just a matter of making sure both devices you want to pair have Bluetooth active, and confirming they want to pair.

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

- On the mobile phone, make sure Bluetooth is enabled in Settings > Bluetooth (iOS 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 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 Preferences > Bluetooth and click the Connect button next to the device.
 - ▶ In Windows, click the Action Center and then click Bluetooth. Click Connect and pick the phone's name.
 - ▶ In iOS, 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 that the pairing PIN shown on each is identical. Then tap Pair or Connect, as the case may be, on each device (**Figure 42**).

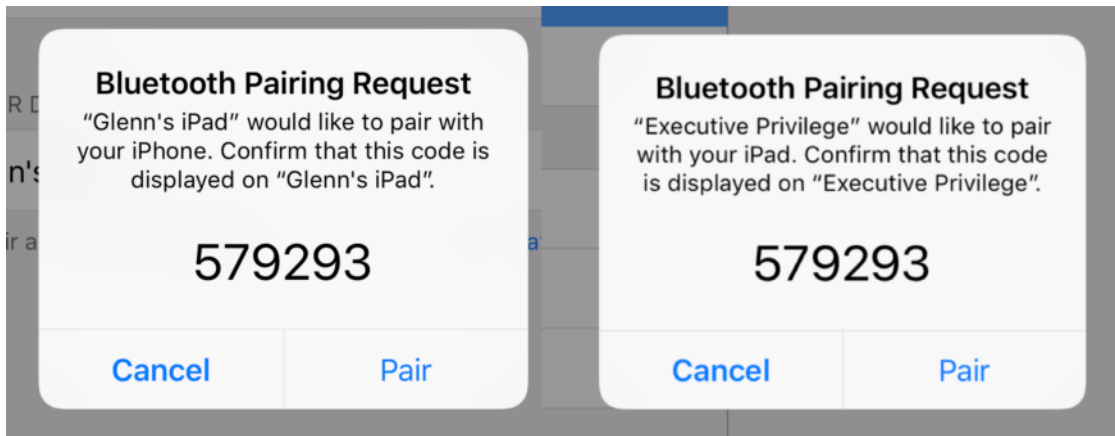


Figure 42: Two devices pairing should each display the same code and tell you the name of the other device. Confirm before pairing!

Once you're paired, you can tether to the personal hotspot by using the Bluetooth settings view (iOS 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 iOS device with the paired connection:

- In macOS right-click the device name in the Bluetooth preference pane, and select Remove and confirm.
- In Windows, open Settings > Devices > Bluetooth & Other Devices, and click the device you want to remove. Now click Remove Device and confirm.
- In iOS, tap Settings > Bluetooth, and tap the device's name under Other Devices. Tap the *i* 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](#), as well as Apple's macOS-only remote desktop and file-sharing access, Back to My Mac, as explained in [this Apple support document](#).

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 43**).

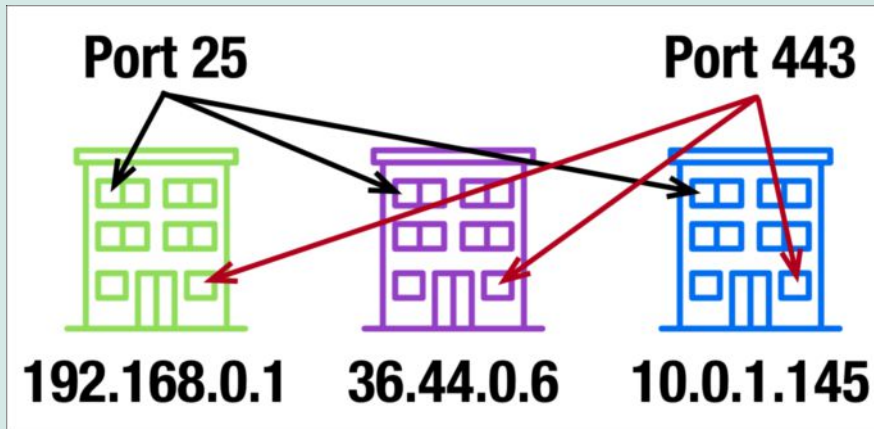


Figure 43: Ports are like apartments within a building, where the building is an operating system, and the IP address is the building address.

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 44**, 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).

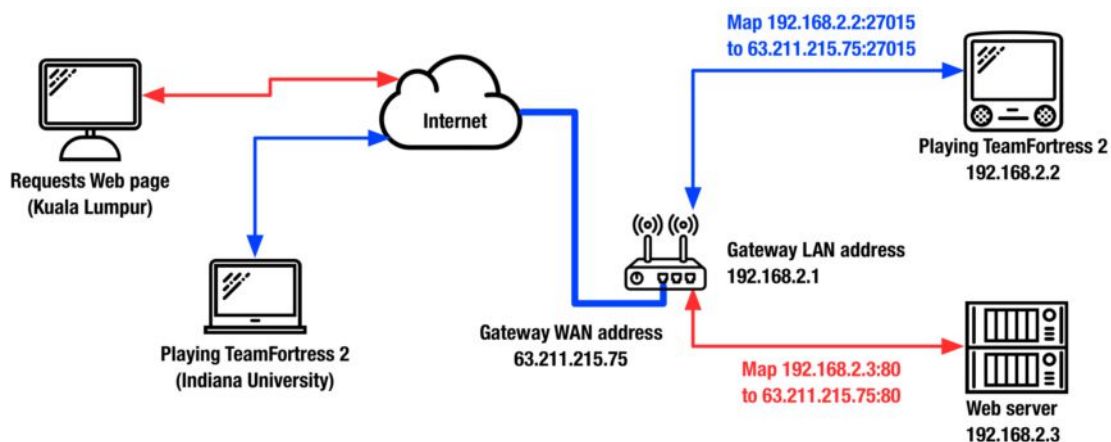


Figure 44: The gateway rewrites addresses and maps ports on the fly to connect inside and outside services and users.

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 servers. From outside the network, someone connects by using this format: <http://serveraddress.com:0>, such as <http://tidbits.com:8001>.

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 the table noted above. However, you may not be able 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.

I opened up my TP-Link router's admin utility, and it shows a list of UPnP service from several addresses on the network from ports 5353 and 4500. Searching on Google, I discovered these are the two ports used by Apple's Back to My Mac, which automatically provides remote discovery when you're logged into a Mac with the same iCloud account as the machine sharing its connection.

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.

NAT-PMP Isn't UPnP

In their retired AirPort base stations, Apple featured what they called NAT-PMP for NAT Port Mapping Protocol. They tried to make a standard back around when UPnP wasn't very robust or widespread. But NAT-PMP never became used widely, and it only included a subset of UPnP features.

At one point, some of Apple's software and some third-party hardware could make use of NAT-PMP, so you might have relied upon it. Back to My Mac, for instance, exclusively used NAT-PMP at one point but, as you can see above, it works fine with UPnP.

With the profusion of routers and competing software and OSes, nothing now requires NAT-PMP.

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 Preferences > Printers & Scanners.
2. Near the bottom-left corner, click the plus  button to open the Add window (**Figure 45**).

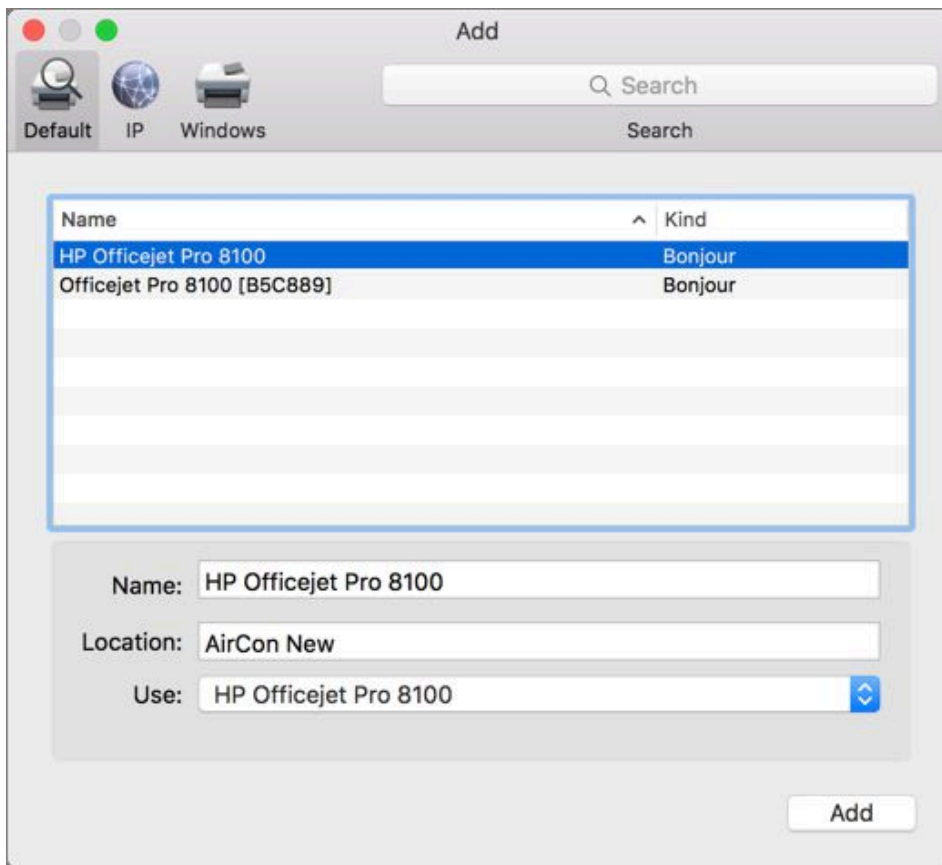


Figure 45: Choose the Bonjour-shared printer.

3. If needed, click Default at the top of the window to see the printers available over Apple's network discovery standard, Bonjour.
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, and 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: iOS devices can only use printers that support AirPrint, a special protocol. If you have an iOS device and a Mac, and your printer lacks AirPrint support, you can use the \$20 [Printopia](#), which acts like a gateway between networked or directly attached USB printers and AirPrint.

Add a Gateway Printer in Windows 10

Here's how to connect a shared printer in Windows 10:

1. Open Settings.
2. Go to Devices > Printers & scanners.
3. Click “Add a printer or scanner.”
4. At this stage, your printer may appear and you can advance to step 6. If your printer doesn't appear, click “The printer that I want isn't listed.”, and then follow the next step.
5. 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 46**).

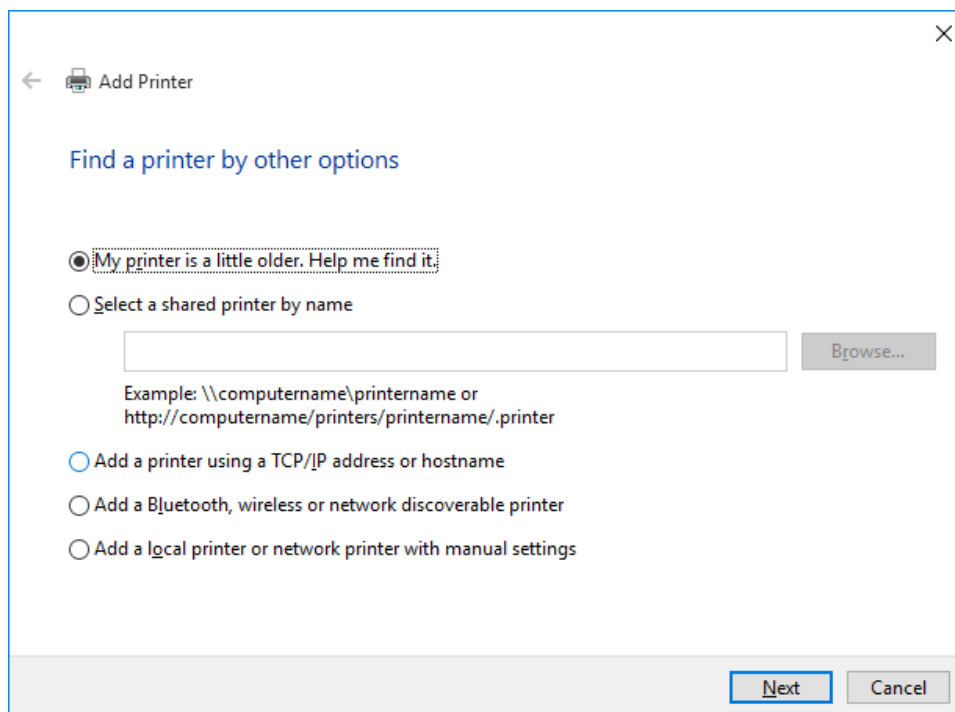


Figure 46: The Add Printer dialog lets you find “older” printers.

6. After a moment, “Choose a device or printer to add to this PC” should appear (**Figure 47**). Select your printer and click Next.

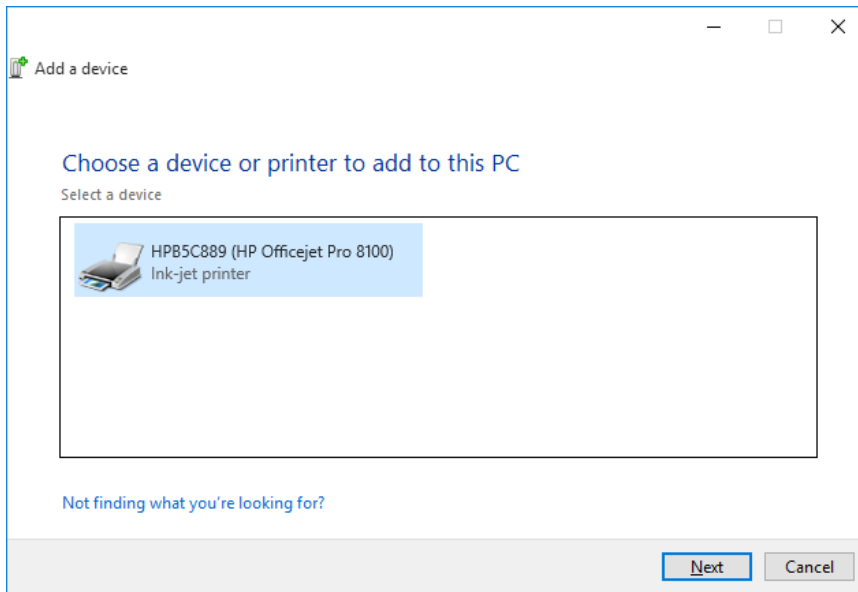


Figure 47: Your device should appear as an option.

7. 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.

<https://sanet.st/blogs/polatebooks/>

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 48**).

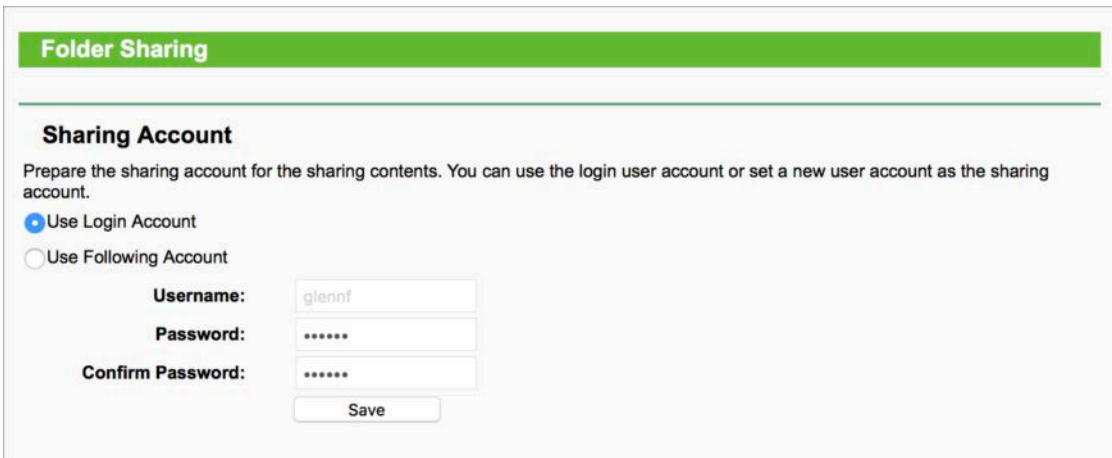


Figure 48: Some gateways can only create a single user for disk and folder sharing (here, a TP-Link model).

- 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 section of the sidebar.
2. Select the Registered User radio button in the upper-right corner, enter your credentials, and click Connect (**Figure 49**).

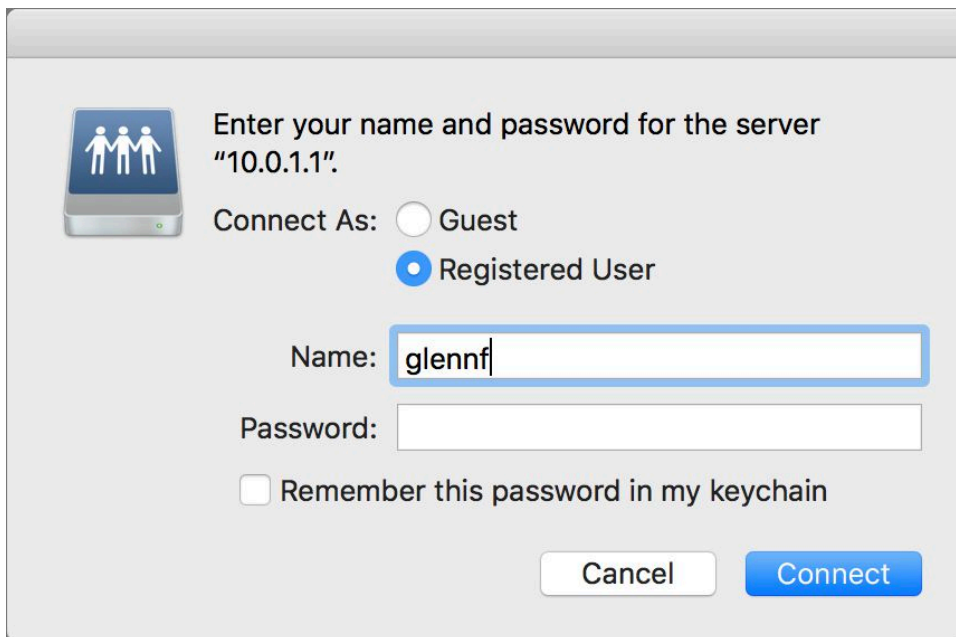


Figure 49: Enter your login credentials to proceed.

3. 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 10

In Windows 10, 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 `\\10.0.1.1`) and press Enter.
4. In the Name field (**Figure 50**):
 - ▶ 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.

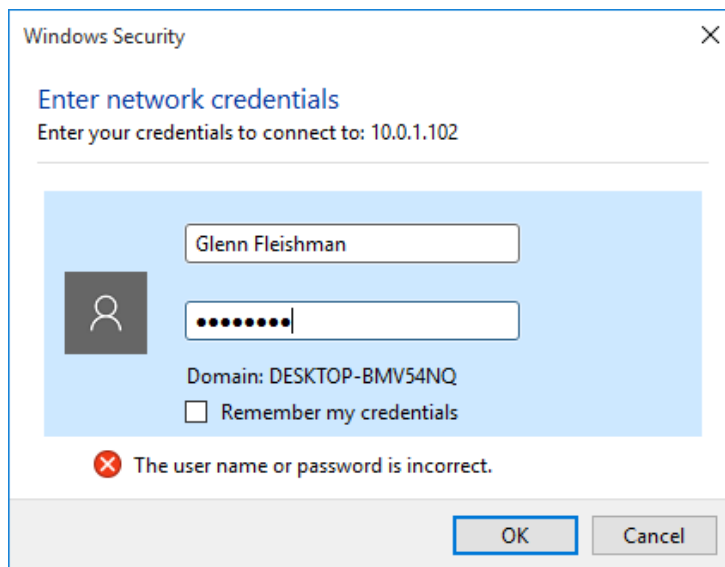


Figure 50: Enter your credentials to log in.

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.

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 programs 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. (A lot of point-of-sale systems continued to use WEP for long after that!)

WPA and WPA2 Background

The Wi-Fi Alliance released *WPA* (Wi-Fi Protected Access) in 2003. It was an interim measure because work 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. For the rest of this chapter, I'll only talk about WPA2, as WPA is effectively no longer used on modern networks, because it carried over some of WEP's weaknesses.

Note: There's work afoot on WPA3, which will eventually replace WPA2. It has a lot of neat advantages, including using encryption to protect connections made over public networks—even those that don't require a password to join.

WPA2 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 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 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.

Note: This kind of Enterprise server runs RADIUS, which expands to the hilariously old-fashioned Remote Authentication Dial-In User Service. RADIUS was developed to manage people using modems attached to phones to dial into banks of modems.

Turn on WPA2 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 even WPA2-AES-CCMP. (For some reason, gateway makers seem to include the most technical name instead of the most common name, even when they refer to the same thing.)

Depending on the age of the gateway and other factors, you might be able to select WPA/WPA2 or WPA2, or have to choose between TKIP and AES or AES-CCMP. Unless you know that you have ancient hardware on your network, always go for the strongest option, which is WPA2 or AES.

Tip: If one of your devices only supports WPA, you’ll know as soon as you change security methods, because the device will be unable to connect.

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, set the passwords to be the same, too.

A passphrase for a Wi-Fi network should be easy to enter, remember, and hand off to someone else, but it shouldn’t be easy enough to guess. The best passphrase is two or three words. Even all in lowercase and with spaces or punctuation between them, that’s about 15 characters long.

<https://sanet.st/blogs/polatebooks/>

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 latest 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 version of Android or an iPhone or iPad with iOS 11 or later can scan it and join (**Figure 51**).



Figure 51: 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 settings 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 Are TLS and SSL?

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.

TLS is a successor to SSL (Secure Sockets Layer). When both older and newer protocols were used side by side, you'd see SSL/TLS or TLS/SSL as a label. However, SSL is now definitively broken from an encryption standpoint, so it's important to look for TLS only.

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 not to employ TLS for email. If your mail host doesn't provide secured email for your incoming email (usually IMAP, but sometimes POP3) and for your outgoing email (SMTP), find a new host. Without security, email programs may send passwords in the clear or with weak encryption, and likely send all data in the clear. Most modern mail programs, especially those that ship with an operating systems, will attempt to configure your mail settings securely.
- **Secure access to websites:** A huge movement in the last couple of years has shifted a large percentage of all websites to use secured connections for all requests, not just for commerce or banking.

If you're not sure a connection is secure, navigate to the site's settings for your account and look for a section on security. There may be a setting labeled "Always use https" or "Always use secure connection" and check that box. (When you log in to a site, the connection is almost always secure, and your account name and password are rarely at risk.)

For other websites, try to always use the secured flavor by typing in or bookmarking [https](#) instead of [http](#) as the start of the URL. Many sites offer TLS sessions as an option reachable by entering the URL in this fashion.

- **Transfer files to a server securely:** When making an FTP connection, use only a secured alternative to plain FTP, such as the SSH-based SFTP or one of several TLS-protected methods. FTP programs otherwise send passwords and data in the clear.

Tip: On a Mac, enable Remote Login and File Sharing in the Sharing preference pane to allow SFTP over a local network or via the remote Back to My Mac service.

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.
- **Skype, sort of:** Microsoft’s Skype was the earliest message, voice, and video service to use end-to-end encryption. Still, some aspects of how it keeps your conversations private have received criticism. Microsoft has never improved on this or fully responded.
- **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.
- **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.

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.

Still, that's not always what you want and it's not always convenient. There are file- and folder-encryption packages for Windows, Linux, and macOS, but these aren't helpful with Android and iOS because of how the built-in email program and file management work—you need apps instead.

That leaves me with one recommendation: public-key (PK) cryptography as implemented in several compatible PGP (Pretty Good Privacy) tools and apps. PK dates back decades, and relies on algorithms that allow the creation of an intertwined public key and private key for encryption and validation.

The public key may be freely distributed and, in fact, must be for other people to encrypt messages sent to you. You have to keep the private key in the pair strictly secure to decrypt messages. The public key offers no utility at all to deriving the private key, which solves the problem of exchanging keys. (I recommend using [Keybase](#) to verify and distribute your public key.)

The pair of keys may also be used to “sign” a document, creating a cryptographic message that lets a recipient check whether a file or text has been modified.

PGP was the first widespread, usable implementation of PK, because it simplified the process of exchanging keys and encryption and signing. In PGP, each recipient of a document's public key is used to encrypt a strong “session key,” or an encryption key used for the file to which the key is attached. That session key works very well for encrypting data, but is hard to protect. The public-key encrypted portion provides exceedingly strong protection, so the session key can't be extracted by any but a recipient.

Several different projects implement PGP using OpenPGP, an updated protocol, which leads to people often calling it GPG as a result.

In order to use PGP/GPG, you need all the other parties to have compatible software installed, generate their own public/private key pairs, and distribute the public key to you. With standalone software and extensions, you can encrypt, decrypt, sign, and validate files and archives, as well as manage all that inside of many email programs.

This is relatively easy to set up on the desktop, where you can rely on [GNU Privacy Guard \(GnuPG\)](#) for several platforms and [GPGTools](#) specifically for macOS. For iOS, file encryption seems problematic, but several PGP/GPG-email programs can do the trick, such as [iPGMail](#) (\$2). For Android, [OpenKeychain](#) (free) offers email integration and some assistance with files.

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 [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.

Country-Hopping with a VPN

There's a trick up the sleeve of VPNs: they can let you seem to be accessing a service from a country other than the one that you currently occupy. This can be handy when you want to access a service as if you are in the same country as the one in which the service operates, or when you might distrust the internet infrastructure of an ISP, cellular network, or entire country that you're in. (This isn't a joke: many countries routinely monitor and suck down data that's sent, in the clear and otherwise.)

It used to be useful as well to evade certain per-country licensing limitations on free and subscription online video streaming and other services. These services started tightening requirements in 2016, and it's now very difficult to bypass them with these workarounds. Further, BBC iPlayer, free to those paying a television license in the United Kingdom, requires a login in addition to a UK network address.

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. 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, often without requiring direct entry.

Warning! Some operating systems allow their network adapters to change their MAC address in a process called *MAC cloning* or *spoofing*. That's sometimes useful when you have to register a computer's MAC address, but then want to use a router in its place. However, because it's trivial to do so, it also means you can't rely on a MAC address as a true method of 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 Preferences > Network.
2. Click Wi-Fi in the adapter list
3. Click the Advanced button in the main window.
4. In the Wi-Fi view, the MAC number is described as the Wi-Fi Address at the bottom.

Find the MAC Address in iOS

Take a three-step jaunt to locate an iOS device'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 10

Windows 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 in ChromeOS

Find the MAC address in ChromeOS with these steps:

1. Click your account photo.
2. Click the Wi-Fi icon.
3. At the top of the box, click Information. The ChromeOS MAC address appears next to Wi-Fi in the resulting window.

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. However, if you bought this ebook elsewhere, you can add it to your account manually:

- If you already have a Take Control account, log in to your account, and then click the “access extras...” link above.
- If you don't have a Take Control account, first make one by following the directions that appear when you click the “access extras...” link above. Then, once you are logged in to your new account, add your ebook by clicking the “access extras...” link a second time.

Note: If you try these directions and find that your device is incompatible with the Take Control website, [contact us](#).

About the Author



Photo by Jeff Carlson

Glenn Fleishman is a veteran technology, business, and science reporter, who has contributed over his career to the *New York Times*, the *Economist*, *Fast Company*, *Wired*, *American History*, *Macworld*, and many other publications. In 2017, Glenn was the inaugural Designer in Residence at Seattle's School of Visual Concepts, where he spent the year relearning letterpress and culminated with printing a book of his typographic and language reporting. You can find (and purchase) his books and read his work at [his blog, called Glog](#).

Shameless Plug

Glenn is also the author of *A Practical Guide to Networking, Privacy & Security in iOS 11*, which you can [purchase from him directly](#) or through [Take Control Books](#). His most recent title about typography and printing is *London Kerning*, a jaunt around that city and its deep history that can still be found in archives and letterpress studios.

About the Publisher

alt concepts inc., 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 May 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 San Diego with their two children and their cat.

Credits

- Publisher: Joe Kissell
- Editor: Scholle Sawyer McFarland
- 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.

More Take Control Books

This is but one of many Take Control titles! Most of our books focus on the Mac, but we also publish titles that cover other Apple devices, along with general technology topics.

You can buy Take Control books from the [Take Control online catalog](#) as well as from venues such as Amazon and the iBooks 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.

Copyright and Fine Print

Take Control of Wi-Fi Networking and Security

ISBN: 978-1-947282-24-7

Copyright © 2018, Glenn Fleishman. All rights reserved.

[alt concepts inc.](#) 4142 Adams Ave. #103-619, San Diego CA 92116, USA

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 inc. 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 inc. 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.