Saturday Safaris
Exploring Technology In-Depth

Modems, Routers, and Wi-Fi

Presented by
Bill James, Region 8 Advisor
APCUG Speakers Bureau Member

The Early Days

- In the early days of networking, the term modem was used to describe a device that transformed speech into analog signals (and vice versa) to be transmitted over telephone lines.
- Modems have been in use for teletype services since the 1920s.
- To send telegrams and cablegrams via teletype, the serial RS-232 standard was developed and used for teletype machines which could communicate with each other over phone lines.
- Each teletype would be physically connected to its modem (working on 110 bps) via an RS-232 connection and the modems could call each other to establish a remote connection between the teletypes.

The Early Days

- What one typed at a teletype (or had saved on punched paper tape) could be printed on a remote teletype located far away.
- No computer was involved.

Teletype teleprinters in use in England during World War II Wikipedia Public Domain .jpg

The Early Days

- In the late 1950s, AT&T developed the first commercial, mass-produced computer modems, then called a “digital subset” to link Semi-Automatic Ground Environment (SAGE) computers across the United States.
- They communicated at 110 bits per second.
- Since then, this term has been broadened to describe a variety of devices that to perform modulation-demodulation (or encoding-decoding) in its most fundamental sense.

prrrrr krrrrrrgggg rrrrrrch

- The most iconic aspect of the early days of the internet is probably a series of sounds - a dial-up modem seeking connection!
- It sounds something like prrrrr krrrrrgggg rrrrrrch.
- There's a brilliant joke about this in the movie The Muppets (2012) when a character named '80s Robot tries to connect to the Internet and all other Muppets can't stand the sound.

The Muppets: "Modem" Film Clip - Bing video

- Internet worked over phone lines, however, when using the Internet, it wasn’t possible to call or receive calls.
- My mother would shout: 'Are you done internetting? I would like to make a call.’

The Hayes Smartmodem

- Early modems were clunky affairs, with the acoustic coupler and the need to dial the phone numbers yourself.
- The Hayes 300 baud Smartmodem, introduced in 1981, changed the market forever.
- It had the ability to plug directly into the phone system and could dial numbers directly, as well as answer calls automatically.
- Despite its price, these features made the Smartmodem attractive to BBS operators, known as "sysops.“

The Hayes Smartmodem

- Unfortunately for Hayes, a lot of other manufacturers liked the Smartmodem’s features and duplicated them on devices that sold for a fraction of the cost.
- Soon, a number of "Hayes-compatible" modems popped up, eroding Hayes’ original market.
- Hayes managed to hang on until the 90s, when it filed for Chapter 11.
- The name is still in use.

Need for Speed

- The speed of modems continued to get faster and faster. The first modems as analog devices were 300 bits per second, then
- 1200 bps
- 9600 bps
- 14.4k
- 28.8k
- 56k
- Advances in echo cancellation and noise-reduction technology helped make these possible.

Need for Speed

- At the start of the 90s, the Internet was making its way from universities and research labs into public consciousness, which also provided demand for more, better and faster modems. Instead of an add-on, they became standard equipment on new PCs. But the fastest dial-up modems were still not fast enough.
- With the explosion of the World Wide Web, users wanted to surf even faster.
- They turned to services like cable and DSL, which provided faster broadband access.
- However, DSL and cable modems weren’t strictly modems in the traditional sense, as they had a completely digital signal path.

The Growth of the Internet

- The popularity of mobile computing led to the growth of wireless technology, including Wi-Fi.
- Of the modern devices, Wi-Fi might be the closest to the traditional modem, as it encodes data into radio waves and turns radio waves back into data.
- Most people in North America use broadband these days, while only three percent still use dial-up.
- The way we access the Internet has also changed, as more people log on with smartphones or other mobile devices, often bypassing the traditional PC.

The Growth of the Internet

- Even with all the changes we've seen, it's always important to remember that we didn't just wake up one day and have the Internet.
- Looking back to see where we've been is a way to appreciate how far we've come...and perhaps how far we still have to go.

Bulletin Boards

- For many people in the 80s and early 90s, the primary reason to get a modem was to access Bulletin Board Systems (BBS).
- While it's fashionable these days to describe past online media as the precursor to social networking services like Facebook, there are definite similarities.
- They offered users a forum for posting and replying to public messages, a kind of email, and often games.
- In contrast to modern social networking services, BBSes were almost exclusively local.
- Many computer clubs had BBSes.

Bulletin Boards

- In 1978, Ward Christensen and Randy Suess created the first public BBS, taking advantage of a blizzard in their hometown of Chicago to build it.
- The idea quickly spread across the country and around the world.
- For an entertaining look at BBS culture through the eyes of the people who lived through its heyday, check out Jason Scott's excellent "BBS: The Documentary." It's Creative Commons-licensed, so you can watch it guilt-free on YouTube. You can get to the videos from here: http://www.bbsdocumentary.com/

Point-to-Point Protocol (PPP)

- Today, no one uses dumb terminals or terminal emulators to connect to an individual computer.
- The Internet lets us connect to any machine in the world via an Internet Service Provider (ISP) with your modem routing TCP/IP packets between you and your ISP via PPP (Point-to-Point Protocol).
- TCP/IP dictates how information should be packaged (turned into bundles of information called packets), sent, and received, and how to get to its destination.
- The same process occurs to get data from the ISP to your computer.

Types of Modems

- **DSL Modem**
  - When you connect to the Internet, you might connect through a regular modem, through a local-area network connection in your office, through a cable modem or through a digital subscriber line (DSL) connection.
  - DSL is a high-speed connection that uses the same wires as a regular telephone line.
  - You can leave your Internet connection open and still use the phone line for voice calls.

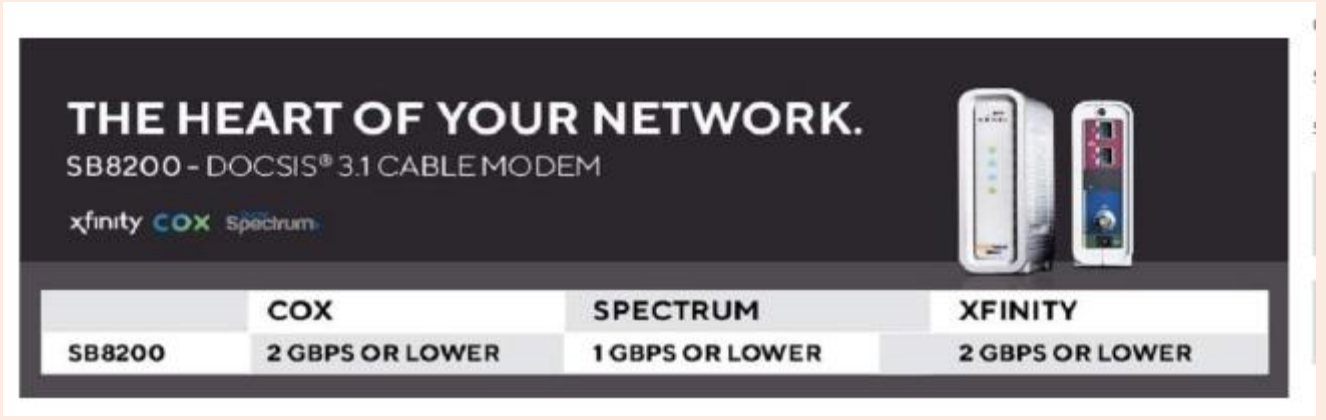
Types of Modems

- **Cable Modem**
  - A cable modem uses your TV cable to get a high-speed connection to the Internet.
  - It operates over coax cable TV lines and provides high-speed Internet access.
  - Since cable modems offer an always-on connection and fast data transfer rates, they are considered broadband devices.

Cable Modem


ARRIS
SURFboard
SB8200


1
2


THE HEART OF YOUR NETWORK.
SB8200 - DOCSIS® 3.1 CABLE MODEM
xfinity COX Spectrum
COX
SPECTRUM
XFINITY
SB8200
2 GBPS OR LOWER
1 GBPS OR LOWER
2 GBPS OR LOWER

Setting Up a Cable Internet Connection

- Plug the cable modem into your computer.
- Make sure your computer is near a wall cable socket.

Setting Up a Cable Internet Connection

- Plug the cable modem into the wall cable socket.

Setting Up a Cable Internet Connection

- Plug in the cable modems' power cord.
- Most modems don't have an On/Off switch.
- Plugging and unplugging them is how you turn them on and off.

Setting Up a Cable Internet Connection

- When the cable modem is turned on, it has to go through a boot up process.
- You can tell this process is done when most of the lights have turned on and stopped blinking.
- There's usually one light that will keep blinking.

Setting Up a Cable Internet Connection

- It usually takes about 30-60 seconds for a modem to finish turning on.

Setting Up a Cable Internet Connection

- If you've purchased a new modem, you'll need to call your cable ISP and give them information about your new modem, otherwise they won't recognize it as being associated with your account.

Setting Up a Cable Internet Connection

- You'll need your modem's serial number and its MAC address, both of which should be printed on the bottom or side of the modem.

Setting Up a Cable Internet Connection

- Test your Internet connection.
- Open a web browser and go to a website that you haven't been to before.
- If you go to a website, you've been to recently, your browser may load it from its cache.

Setting Up a Cable Internet Connection

- If the website loads, then you're connected to the Internet.
- If not, complete the rest of the steps.

Setting Up a Cable Internet Connection

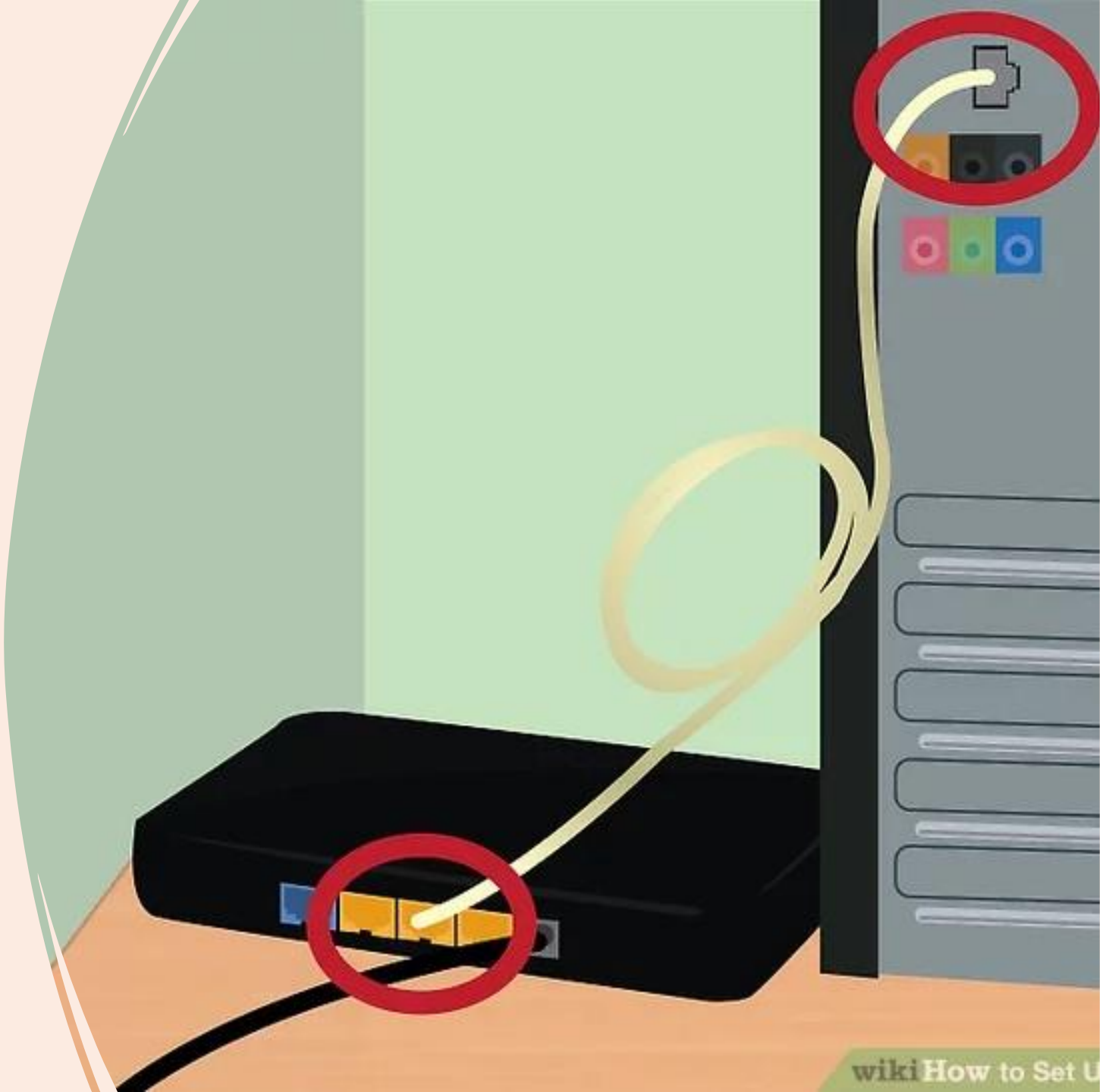
- Testing your connection is not limited to web browsers; you can use any other program that requires Internet.
- Searching for something using a search engine is a good way to do this.

DSL Modem

Comcast Xfinity	Time Warner Cable	Charter	Cox	Cablevision
—	—	—	—	—
Verizon FIOS	**AT&T U-verse**	**Century Link**	***Other***	
—	—	✓	***If not listed, contact your service provider for compatibility information***	

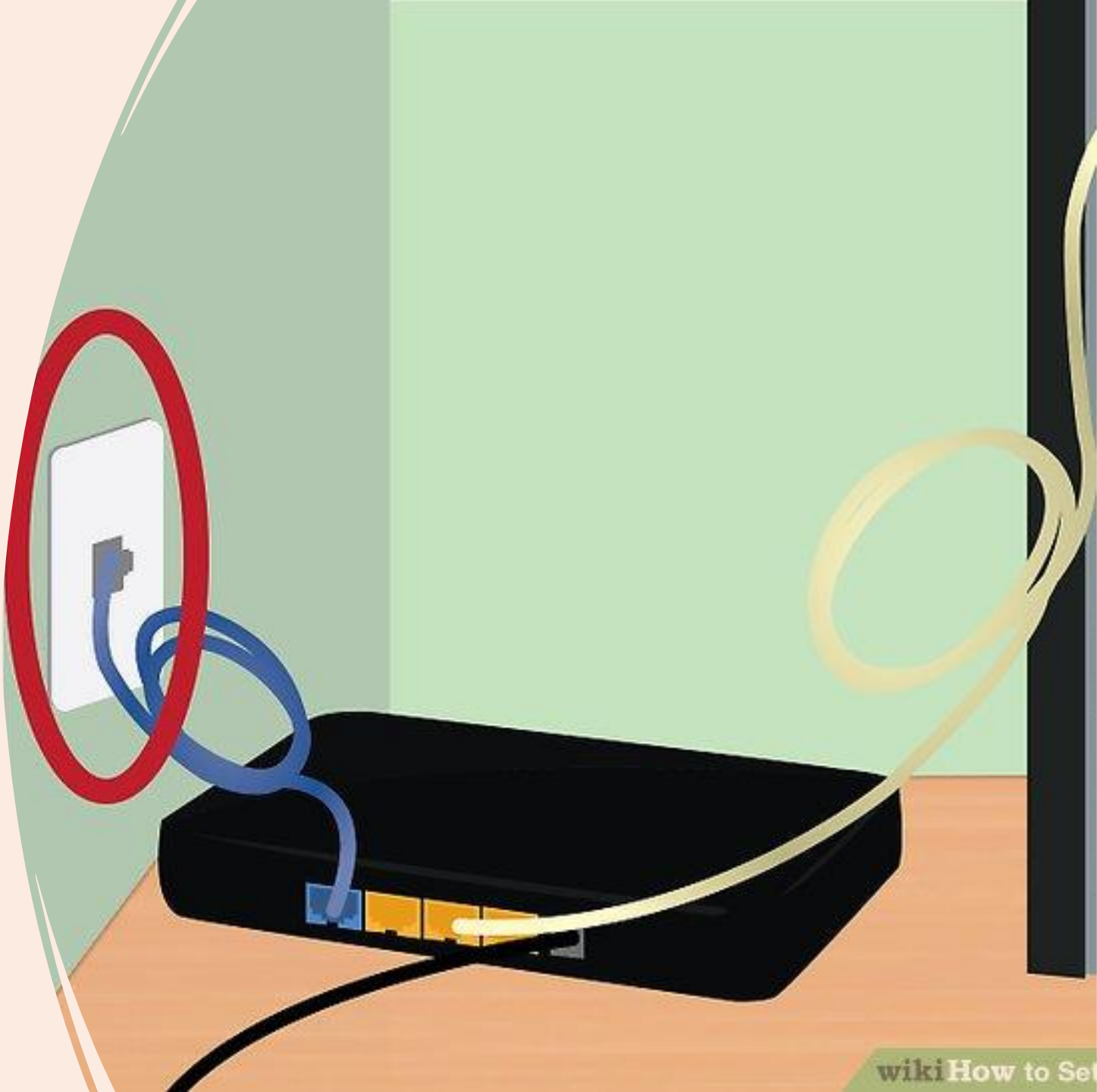
Setting Up a DSL Internet Connection

- Plug the DSL modem into your computer.
- Make sure your computer is near a wall cable socket.



Setting Up a DSL Internet Connection

- Plug the DSL modem into the wall cable socket.



Setting Up a DSL Internet Connection

- Plug in the DSL modem's power cord.
- Most modems don't have an On/Off switch.
- Plugging and unplugging them is how you turn them on and off.

Setting Up a DSL Internet Connection

- When the DSL modem is turned on, it has to go through a boot up process.
- You can tell this process is done when most of the lights have turned on and stopped blinking.
- There's usually one light that will keep blinking.

Setting Up a DSL Internet Connection

- It usually takes about 30-60 seconds for a modem to finish turning on.
- If you've purchased a new modem, you'll need to call your DSL ISP to associate your modem with your ISP account username and password.

Setting Up a DSL Internet Connection

- If you don't know what these are, you'll need to call your ISP to get them.

Setting Up a DSL Internet Connection

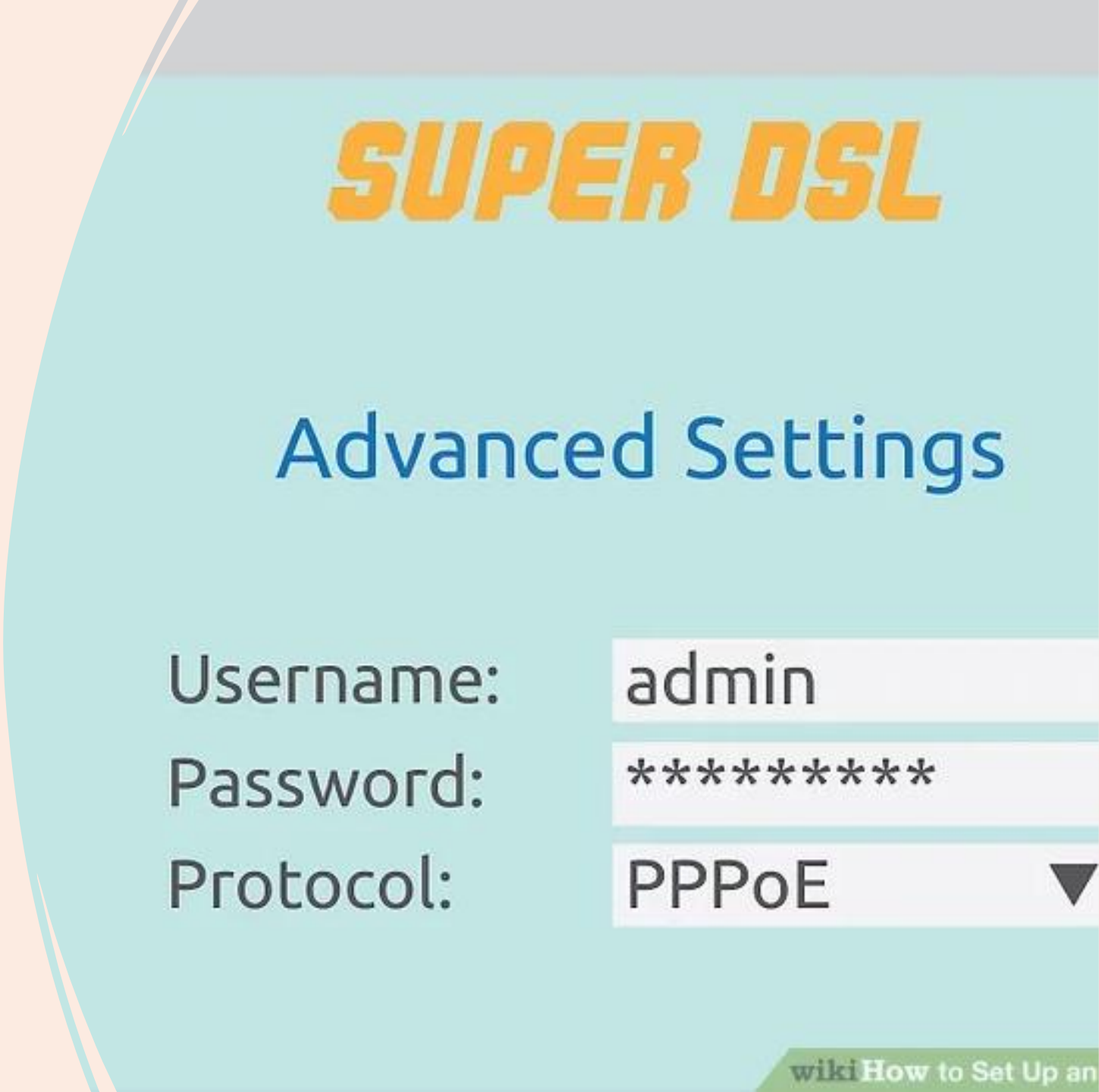
- Log in to the modem's administrative screen.
- Open a web browser.
- In the address field, type the modem's IP address.
- It's often printed on the modem itself.
- If not, it will be in the modem's manual.

Setting Up a DSL Internet Connection

- Common modem IP addresses are 192.168.0.1 and 192.168.1.1.

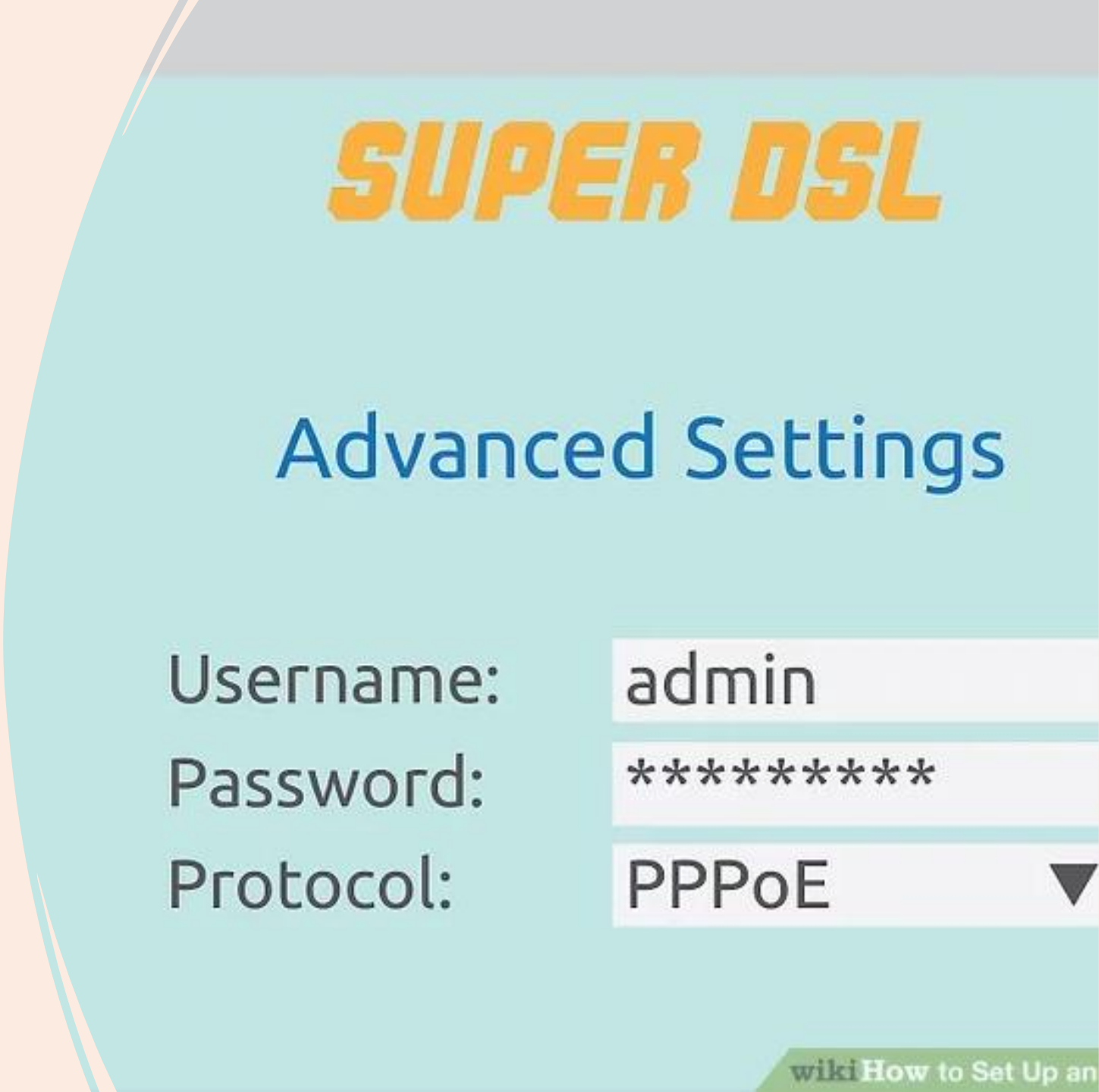
Setting Up a DSL Internet Connection

- Enter your DSL account username and password.
- Once you've connected to the modem's administrative screen, look for PPPoE.
- Enter your DSL account username and password into the PPPoE fields.



Setting Up a DSL Internet Connection

- The username is usually an email address.
- If you don't know your account username and password, contact your DSL ISP.



Setting Up a DSL Internet Connection

- When the setup is complete, save the settings.
- The Internet light on your modem should turn green to indicate you are online.

Setting Up a DSL Internet Connection

- Test your internet connection.
- Open a web browser and go to a website that you haven't been to before.
- If you go to a website you've been to recently, your browser may load it from its memory.

Setting Up a DSL Internet Connection

- If the website loads, then you're connected to the internet.
- If not, complete the rest of the steps.
- Searching for something using a search engine is a good way to do this.

Modems and DOCSIS

- All modems are generally very simple devices and work the same.
- The biggest difference between them is the standard they support, which determines the internet speed capacity they are capable of delivering.
- This standard is called "data over cable service interface specification," or DOCSIS, and currently they all use DOCSIS version 3.0/3.1
- Data Over Cable Service Interface Specification (DOCSIS) is an international telecommunications standard that permits the addition of high-bandwidth data transfer to an existing cable television (CATV) system

Modems and DOCSIS

- It is used by many cable television operators to provide Internet access (see cable Internet) over their existing hybrid fiber coaxial (HFC) infrastructure. The version numbers are sometimes prefixed with simply "D" instead of "DOCSIS" (e.g., D3 for DOCSIS 3).
- Data Over Cable Service Interface Specification, or DOCSIS, is an international telecommunications standard that allows for the addition of high-bandwidth data transfer to an existing coaxial cable TV system.
- DOCSIS is important for Internet users and Internet providers because it allows Internet speeds to increase without having to completely replace coaxial cable networks.

Modems and DOCSIS

- In an ideal world, everyone would have Fiber to the Home service. In reality, it would cost billions of dollars to make happen.
- On a practical level, DOCSIS matters for consumers because you'll have to decide which DOCSIS standard you need when purchasing a modem for your cable Internet connection.
- Depending on the quality of your connection, the answer isn't necessarily just "the newest one."
- You can generally still use your older equipment for most providers, but you'll be limiting yourself in terms of what top speeds you can achieve, especially during hours of peak activity in your area.
-

Routers

- Computer routers have existed since the early days of the Internet, even though many people think it’s a newer technology.
- Without a router, the Internet couldn’t exist.
- Traditional routers are devices that connect different computer networks together.
- A router is also capable of connecting a computer to multiple networks referred as ‘bridging’.

Routers

- Wireless routers are hardware devices that internet service providers (ISP) use to connect you to their cable or xDSL Internet network.
- They are sometimes referred to as a wireless local area network (WLAN) device and can function as a wireless access point and a traditional router.




Routers

- Gaming routers are Wi-Fi devices that give priority to multiplayer online games when given a list of gaming sites' URLs.
- The router then provides a higher quality of service for transmissions to and from those URLs.
- Mesh routers are Whole Home Wi-Fi systems consisting of a main router that connects directly to your modem, and a series of satellite modules, or nodes, placed around your house for full Wi-Fi coverage.
- They are all part of a single wireless network and share the same SSID and password, unlike traditional Wi-Fi routers.

Wi-Fi Routers

- With almost every house now having a broadband connection, evolution of Wi-Fi routers are more popular than ever.
- Most devices on the market such as smartphones, computers, lights, doorbells, locks and some home appliances are equipped to use Wi-Fi.
- Though Wi-Fi has become an integral part of our routine, most of us do not know much about the Wi-Fi technology.

Wi-Fi Routers

- The history of evolution of Wi-Fi routers is fascinating and an earlier form of Wi-Fi was in existence since 1971.
- Apparently, “ALOHA Net” accounted for connecting the Hawaiian Islands with aid from a wireless network asset.
- ALOHA Net and ALOHA protocol are the early forerunners to the concept of Ethernet which later transcends to the IEEE 802.11 internet protocols.

AC(X)1200, AC(X)1750, AC(X)1900, What does it Mean?

- When you buy a wireless router, you will notice the term AC followed by a number somewhere in the name. Newer models may include the letters AX followed by a larger number.
- The AC suffix indicates that the router supports the 802.11ac (or Wi-Fi 5) wireless networking standard, which provides fast Wi-Fi network connections at 5 GHz.
- The suffix AX indicates that the router supports the 802.11ax (or Wi-Fi 6) wireless networking standard.

AC(X)1200, AC(X)1750, AC(X)1900 What does it Mean?

- The number following AC or AX represents the router's maximum THEORETICAL bandwidth. 1200 Mbps equals 1200 Mbps, 1900 Mbps equals 1900 Mbps, 3200 Mbps equals 3200 Mbps, and so on.
- When you see AC2300 in a router's name, it means you're dealing with a Wi-Fi router that offers a wireless network based on the 802.11ac (Wi-Fi 5) standard, with a total theoretical bandwidth of 2300 Mbps.

AC(X)1200, AC(X)1750, AC(X)1900, What does it Mean?

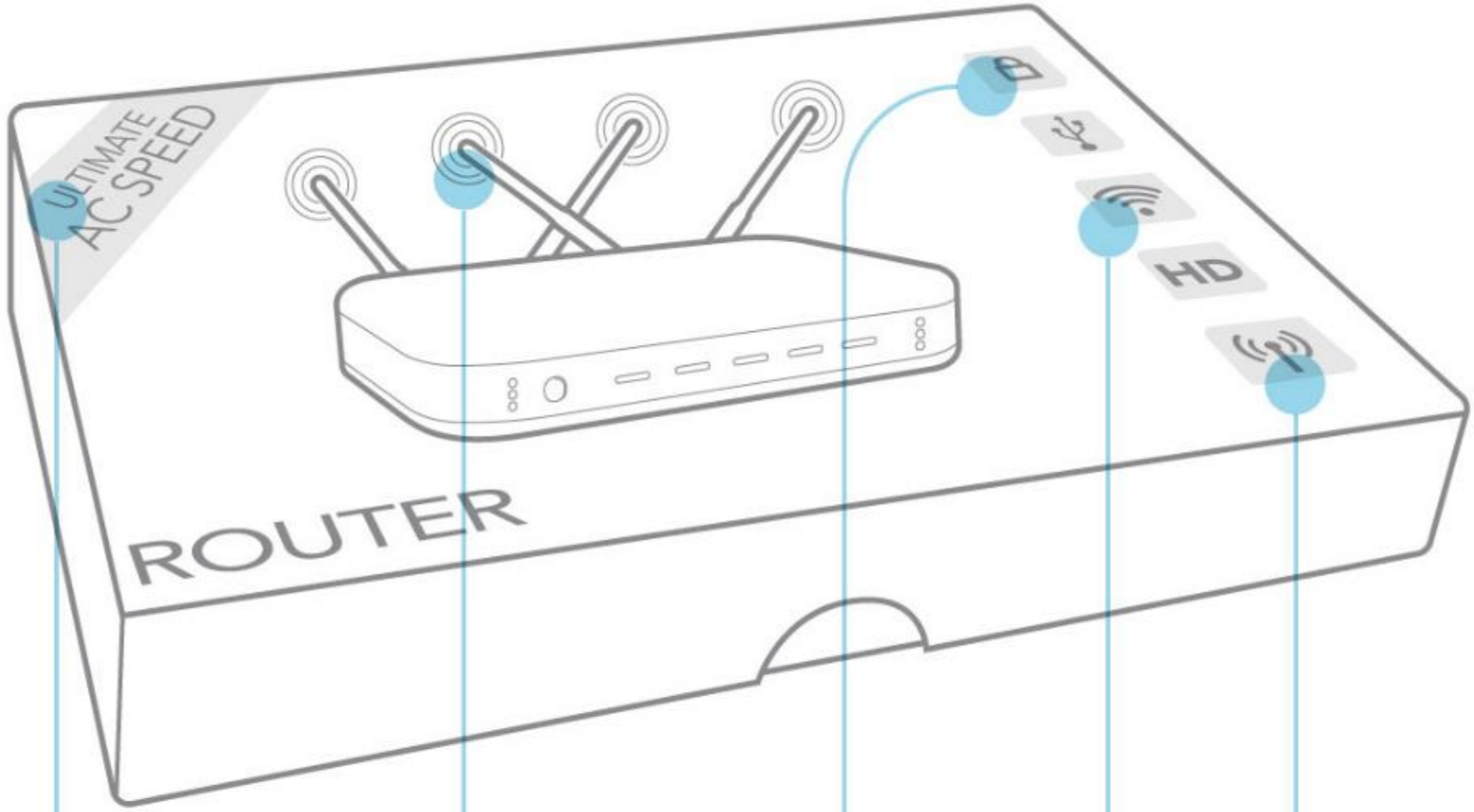
- You might be tempted to believe that an AC3200 router provides a 3200 Mbps wireless network.
- That would be incredible, but it is, unfortunately, false. The truth is that this naming convention is ineffective when making a purchasing decision.
- It's just a marketing ploy to trick you into thinking a router is faster than it actually is.

Antennas

- Most current Wi-Fi routers, such as the NETGEAR Nighthawk and TP-Link AC 1750 SMART Wi-Fi routers, include 3-6 antennae, compared to older routers that only had 1 or 2 antennas.
- Wi-Fi routers use several antennas to help increase data transfer speed and reliability. A router with multiple antennas may broadcast multiple streams of data at the same time (MIMO (multiple Input/Multiple Output)), resulting in increased speed.
- Additionally, they make it easier to use the beamforming technique, which helps focus signals on the target device.

Antennas

- It's crucial to remember, too, that in order to fully benefit from MIMO routers' higher transfer rates, your receiving devices must likewise handle multiple streams of data via multiple antennas.
- A Wi-Fi router can have six to eight antennas but only support three data streams. The remaining antennas are usually utilized for beamforming and antenna diversity.
- External antenna wireless routers are not inherently superior than those with inside antennae, but they do provide better directional control. This means that, if the external antennas are properly positioned, they can send a stronger signal in the direction of the target.
- Routers with inbuilt antennae, on the other hand, are better at uniformly spreading signals.



Wireless standard

Look for routers that support the newest standard, 802.11ac, for maximum speed and coverage.

Antennas

When it comes to antennas, quality is better than quantity.

Security

WPA2 is the most secure networking protocol.

Speed

Advertised speeds are usually theoretical maximums — actual speeds depend on a variety of factors in your home.

Frequency channels

Dual band routers support more devices and activities (like Netflix bingeing).

Setting up Routers

- Placement and setup should consider where you'll place your router.
- Finding an open space toward the center of your residence is the best way to ensure optimal coverage.
- Be aware that walls and floors will impede Wi-Fi signals, so the more obstructions you have between your devices and your router, the weaker (and potentially slower) the signal will be.
- Try to avoid proximity with large metal, glass, brick, or concrete objects.
- Wi-Fi mesh systems get around this problem by letting you place an attractively designed node wherever coverage is weakest.
- But for those working with standard routers or even wireless range extenders, this will require some patience and testing to see where your optimal placement areas are.

Setting up Routers

- Start this process by connecting your router to your modem.
- For this you'll need an Ethernet cable, which you'll want to plug into the WAN (wide-area network) port on your router's rear face.
- This port might look slightly different from router to router, but it will usually have a distinct color from the other ports and be labeled "WAN," "Internet," or something similar.

Setting up Routers

- Before we go any further, let’s discuss WAN vs. LAN: What Is the Difference?
- Quick exercise. Connect your phone to Wi-Fi and then browse over to your favorite website. How did everything go?
- Congratulations! You just used a LAN and WAN network and perhaps did not even realize it. How did that happen? You connected first to a LAN and were then forwarded to and from a WAN, which in this example was the Internet.

Setting up Routers

- LAN and WAN Defined
- Local Area Network (LAN) is an acronym for local area network. The term "wide area network" refers to a network that spans a large area.
- Let's start with something that almost everyone has heard of: the Internet.
- The Internet is the world's largest WAN. It's a great example of Wide Area Networking because it allows you to leave your Local Area Network and view websites that aren't on your local network. They may not even be in your country, which is why the Internet is such a wonderful thing.

Setting up Routers

- Most routers come with some kind of administrative website you access by typing their IP address into your favorite web browser and entering your login and password—which you changed from admin/admin or admin/password, right?
- If you are lucky, you have a “smarter” router that’s a bit easier to configure via an app, but most people (and their older, non-mesh Wi-Fi gear) are probably stuck with a website.

Setting up Routers

- Unless the manufacturer has built an “easy mode” into the experience, a router’s admin page can feel overwhelming at first glance, especially if you’re not used to much of the terminology you’ll find.
- Our goal today is to help you get your router’s most important features set up and explain all the other details you ought to know about.

Username and Password

- The first step to get your network up and running will be to set up a username and password.
- If you happen to have a pre-owned router, the username and password can be reset to factory defaults by holding a recessed button somewhere on the router (usually the back).
- Often, these defaults are something like "admin" and “password," which every would-be hacker knows, so make sure to change these right away.
- Be sure to use a secure password that includes a mix of uppercase and lowercase letters, numbers, and symbols.

Username and Password

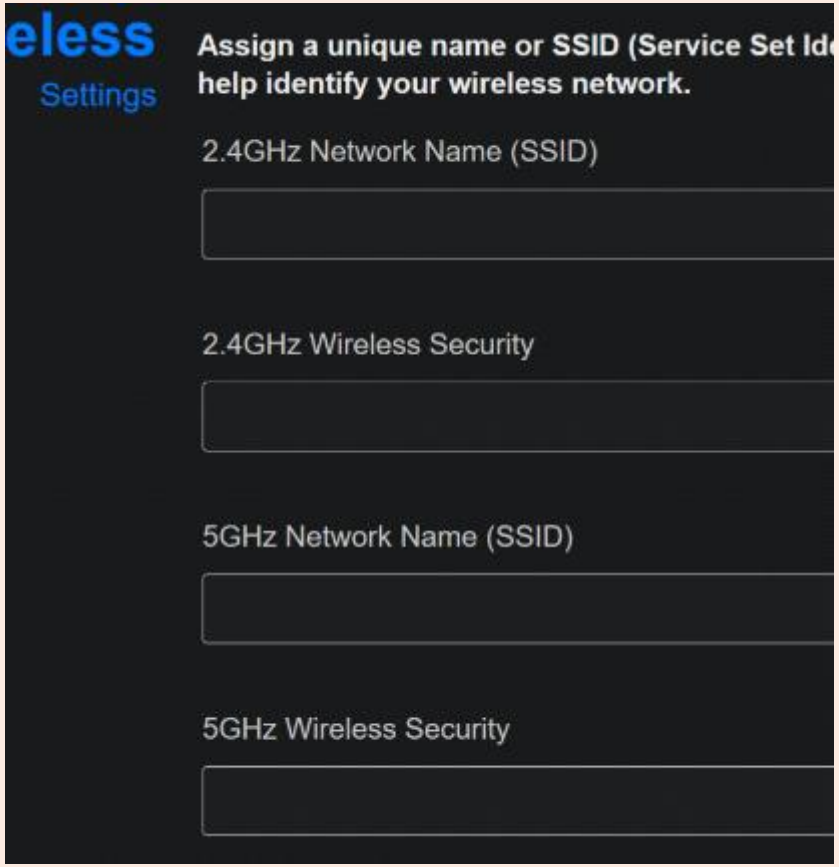
- Once you're there, the first thing you want to do is select an SSID.
- If you are upgrading a wireless router and want to save yourself sometime, I recommend you use the same SSID.
- Choose whatever name you want; it's your wireless network.
- You'll either be asked to use one SSID that will cover all of your wireless networks—and your router will decide whether devices connect on 2.4 GHz or 5 GHz—or you'll be able to set separate names for each wireless network you run on each band.
- The latter is better because it's good to know what you're connecting to, but plenty of people go with the former for the extra convenience.

Username and Password

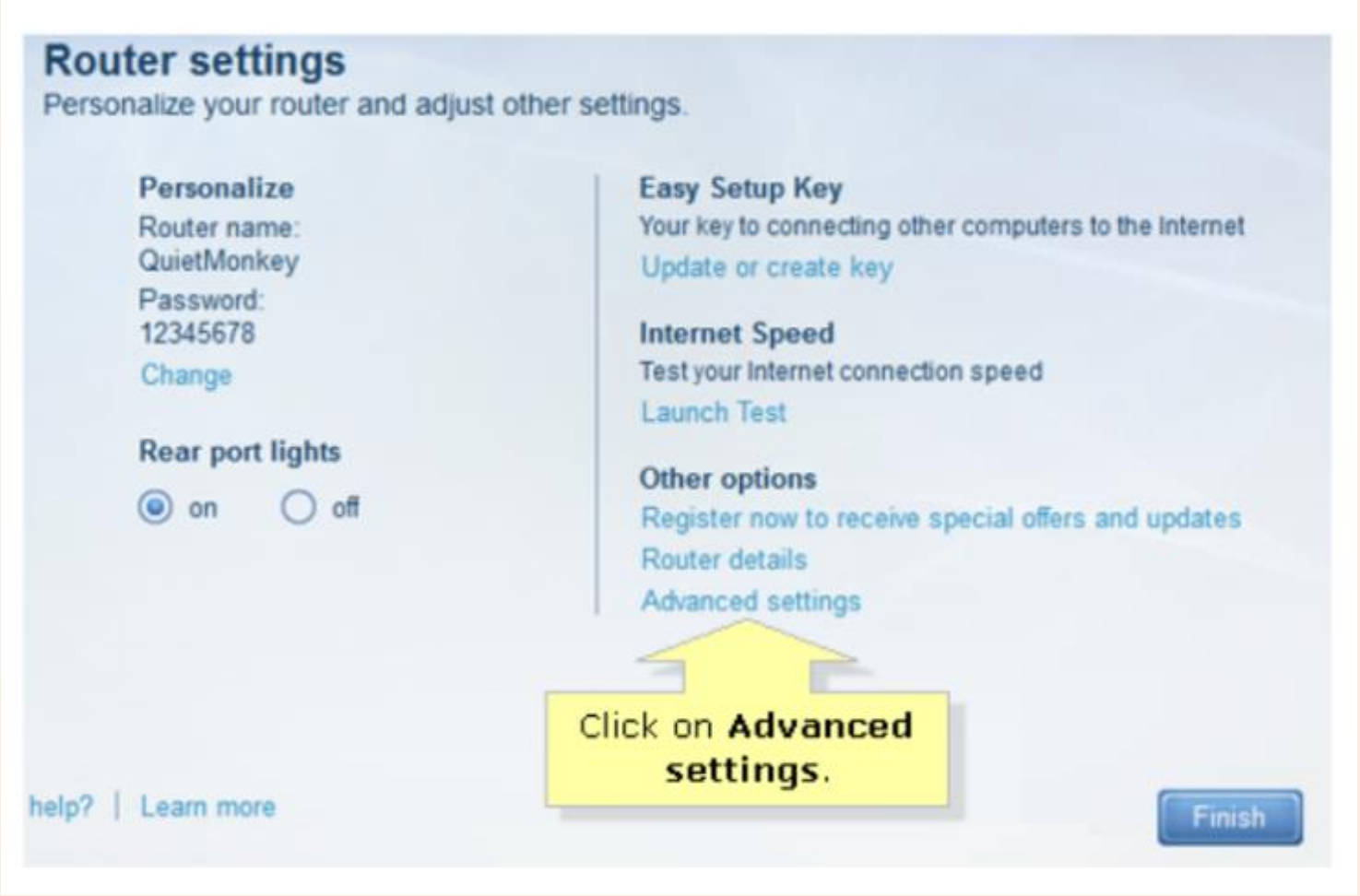
- While it may seem trivial, there are actually a few things you need to know about naming your router.
- To start, the name of your router and wireless network are different.
- Naming your wireless network is really naming the service set identifier (SSID) that the router broadcasts—what you select on your computer when you want to connect to your Wi-Fi network and get online.
- If you are upgrading a wireless router and want to save yourself sometime, I recommend you use the same SSID.

Username and Password

- SSIDs? Super-important.
- Router name? Not important.
- Give each network a solid password and that’s all you need to do to get the Wi-Fi working.
- However, it’s possible your router might have a few more options to pick from (or an “Advanced” mode.



Advanced Settings



How Do I Configure My Router?

- With the username and password set, you can proceed to configure your router's settings.
- As with cooking a dinner, there's no "right" way to install a router, and every model is likely to have its own unique steps, depending on its features.
- Because of this, trying to describe every possible configuration path here would be exhausting and pointless.
- We recommend consulting your router's manual for specifics.
- Visit few YouTube videos on the subject for further recommendations and advice.

How Do I Configure My Router?

- That said, we do have a few points of advice:
- Use the easy setup wizard.
- Most routers provide some form of brief setup routine that asks for little more than the SSID and password. If in doubt, start with this.
- (The SSID is your router's Wi-Fi name.
- It might be something like "asus" or "netgear" out of the box, but feel free to change this to something creative, like "FBI-surveillance-van.")
- Yes, this utility only gets you as far as the set of blinking green lights, but even for those looking to go beyond that stage, you need to get there first.

“Auto” Configuration

- Following the router's documentation and using its own setup utility is always the shortest path to that destination.
- When in doubt, let the router do it.
- "Auto" configuration tools are your friend.
- For example, while you can certainly go to the trouble of building your own internal IP address range and assigning static addresses to all your devices by hand.
- By simply checking the Dynamic Host Configuration Protocol (DHCP) box in your router's settings will take care of that immediately since this is a protocol that automatically assigns IP addresses to devices.

Connect to the 2.4 GHz or 5 GHz Band?

- The lesson here is that just because you can change something doesn't mean you should.
- At least during the setup and early-use stages, go with the auto settings as much as possible.
- On the client device side, all other things being equal, 5GHz connections will provide better performance at short ranges than 2.4 GHz.
- This is because 5 GHz, while somewhat faster, can't travel as far or transmit through some objects due to that band's shorter wavelengths.

Connect to the 2.4 GHz or 5 GHz Band?

- The 2.4 GHz band tends to have more congestion and fewer channel options.
- That said, if you want to keep using 2.4 GHz, consider experimenting with the channel selection.
- "Auto" usually does a decent job of hopping around the channel options and finding the best one, but if you're struggling with client connections, try manually setting the channel to 1 or 11.
- The 2.4 GHz band has a total of 11 channels you can switch between to avoid interference, with channel 6 usually being the default.

Connect to the 2.4GHz or 5GHz Band?

- When you select a given channel, there's usually some signal spillover.
- So, selecting channel 2, for example, will often spill traffic onto channels 1 and 3.
- Thus, switching to the extremes of 1 or 11, the farthest points from the default of 6, can sometimes ensure the best-performing connections.

Wi-Fi Protected Set-up (WPS)

- Use the WPS button to connect Wi-Fi devices.
- If you've ever paired two Bluetooth devices, such as a smartphone with headphones, then you already have the basic understanding of how this works.
- Let's say you want to connect a Windows 10 laptop to your router.
- On your laptop, you'll see your router's SSID pop up on the list of visible wireless networks in Windows.
- When you select the SSID and attempt to connect, Windows will prompt you to enter the network security key, which is a needlessly technical way of saying password.

Wi-Fi Protected Set-up (WPS)

- If you've done a proper job with your security and created a password with randomized uppercase and lowercase letters, numbers, and symbols, you might have forgotten it and not want to mess with typing it in ever again.
- Instead, press the WPS button on your router.
- You should allow at least a minute for the router and laptop to find each other and successfully pair.
- Keep in mind that WPS only works with Windows and Android devices.

A Few Extra Steps

- After the "easy" setup, some routers will walk you through a few extra steps, such as establishing parental controls (features that allow you to filter certain types of content) and automatically updating the router firmware.
- After these preliminaries, proceed to "wireless setup," or a similarly named tab/screen to activate your Wi-Fi network.
- Once your network is activated, you can connect any device to it and start browsing the web.

A Few Extra Steps

- Taking It To The Next Level With most routers, simply activating your network and connecting to the internet is only scratching the surface of what you can do.
- While a tab name like "advanced settings" may seem a bit intimidating, the menus contained here often allow you to control some of your router's most helpful features.
- We'll cover some of the most compelling items.

Quality of Service (QoS)

- QoS is one of the most useful features for online entertainment.
- It allows you to select and prioritize the upstream and downstream traffic on your network, which can provide a performance boost for your favorite streaming service or online game.
- Most routers will have a tab in their app/configuration page dedicated to traffic monitoring.
- Navigate to this and find the QoS tab.
- Turn QoS on, and then you can prioritize certain services, such as online games or video streaming. You can also prioritize devices on the network.

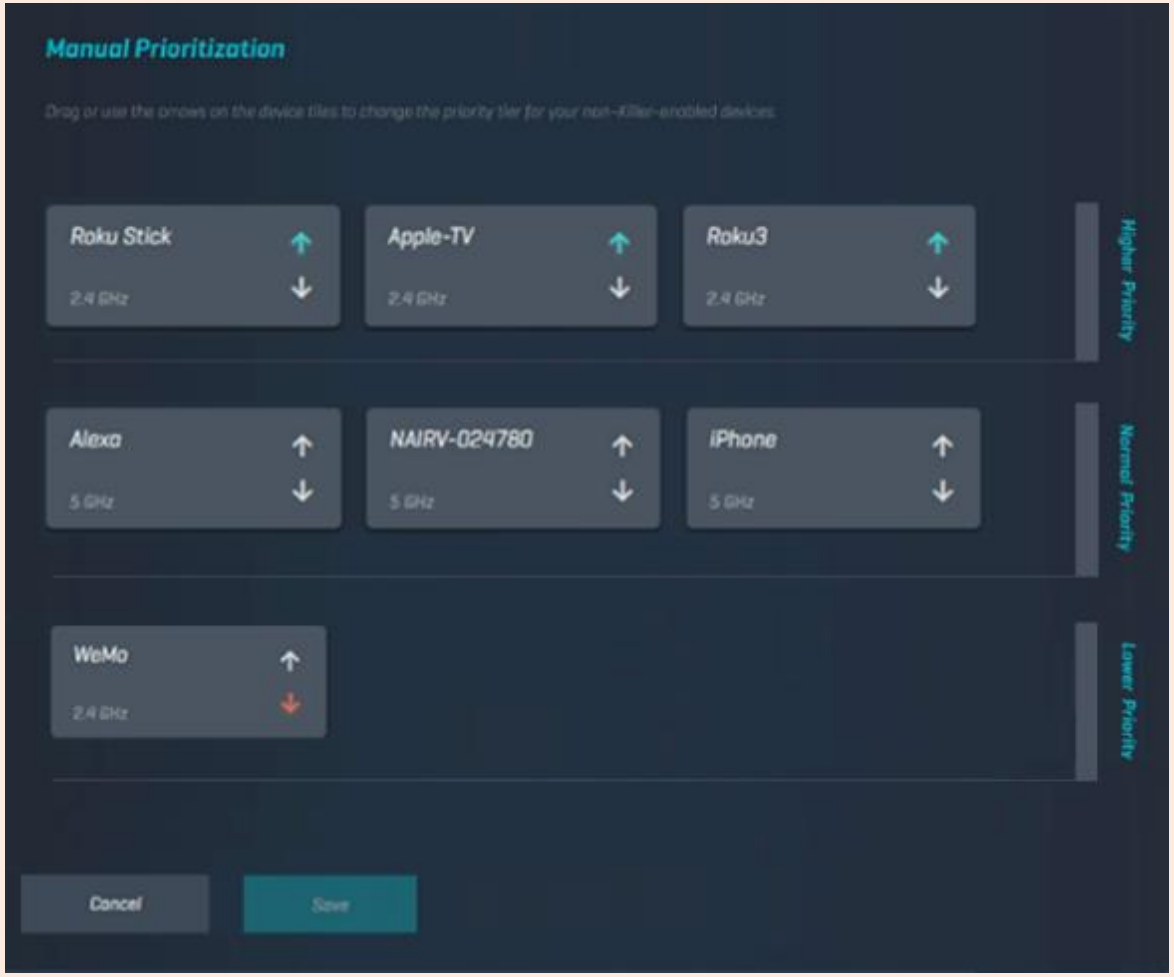
Quality of Service (QoS)

- Years ago, this was usually done by supplying the device's unique MAC address and setting a priority level for that device.
- These days, vendors are increasingly supplying more intuitive, graphical approaches to the same idea, as in the Manual Prioritization screenshot.

Quality of Service (QoS)

Setting up Manual Prioritization

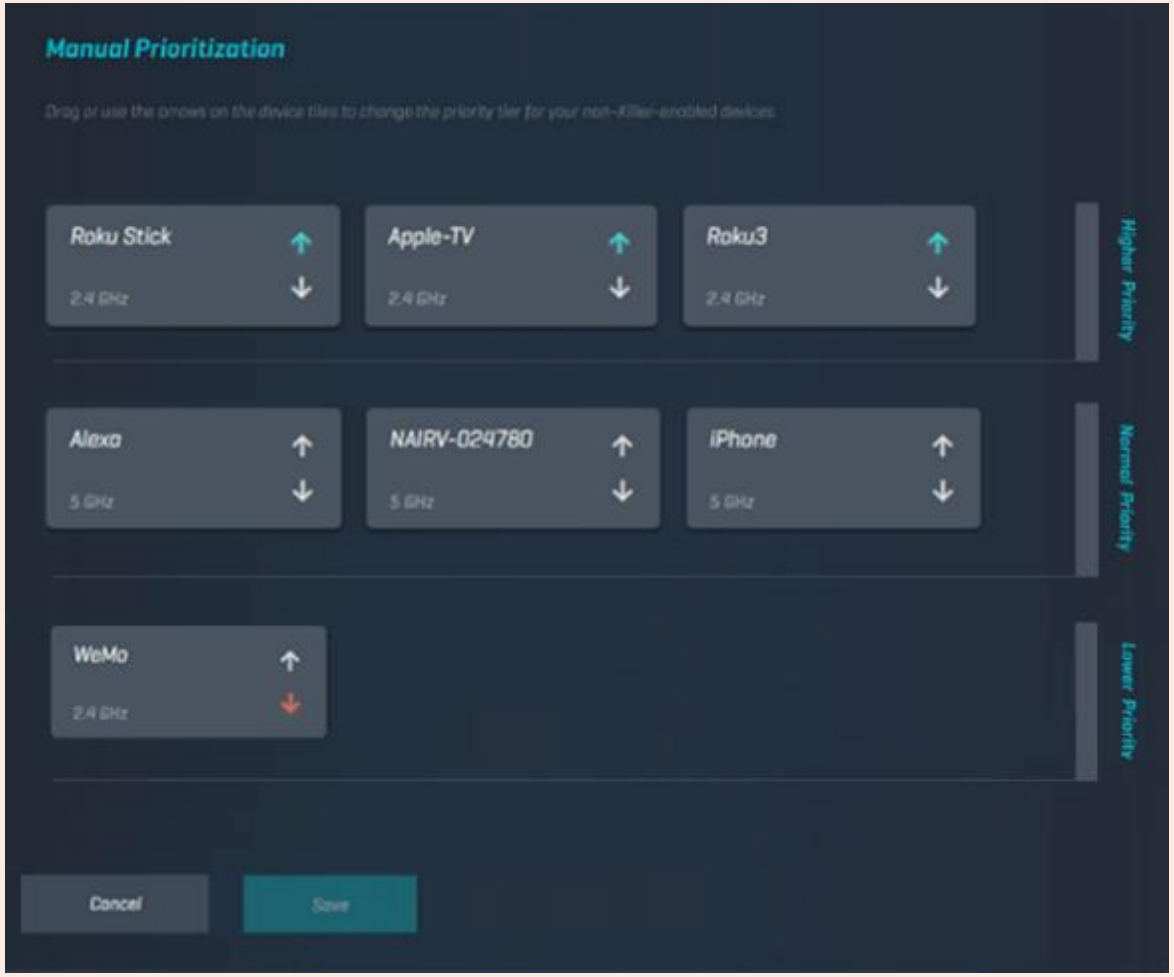
All your devices will be displayed in the Manual Prioritization section.
By default, all devices fall in the Normal Priority queue.



Quality of Service (QoS)

Setting up Manual Prioritization

Use the up and down arrows if you want to set a Higher Priority or Lower Priority to a device.
Make sure to click or tap the Save button to apply any changes made.



Guest Network Configuration

- A guest network is handy to have if you'd prefer to keep all the data and files on your personal network out of unapproved hands.
- To set one up, go to your router's app/configuration page and navigate to the wireless settings.
- Most routers have guest networks disabled by default, so there will usually be a page to set one up here.
- Confirm the network's name and password and the network will be set up.
- It is recommended to apply at least WPA2 encryption to your regular Wi-Fi network, but you may want to leave your guest network "open" for easier access.

Guest Network Configuration

- While convenient, this might also encourage connections from neighbors and stray people parking on your curb.
- Limit guest network access privileges, such as which band they can use or what hours the network is active.
- You may also want to limit the guest network to either the 2.4 GHz or the 5 GHz band, but not both.

File Transfer Protocol (FTP)

- Internet oldsters might remember the days before Dropbox, when transferring large files between systems required jumping through several hoops with dedicated file-transfer protocol applications.
- FTP apps may have fallen out of common use, but the technology can still be a handy way to transfer lots of files without dealing with cloud services.
- FTP servers are only available to routers that have at least one USB port.
- The first thing you'll need is a USB storage device, such as an external hard drive, plugged into your router.

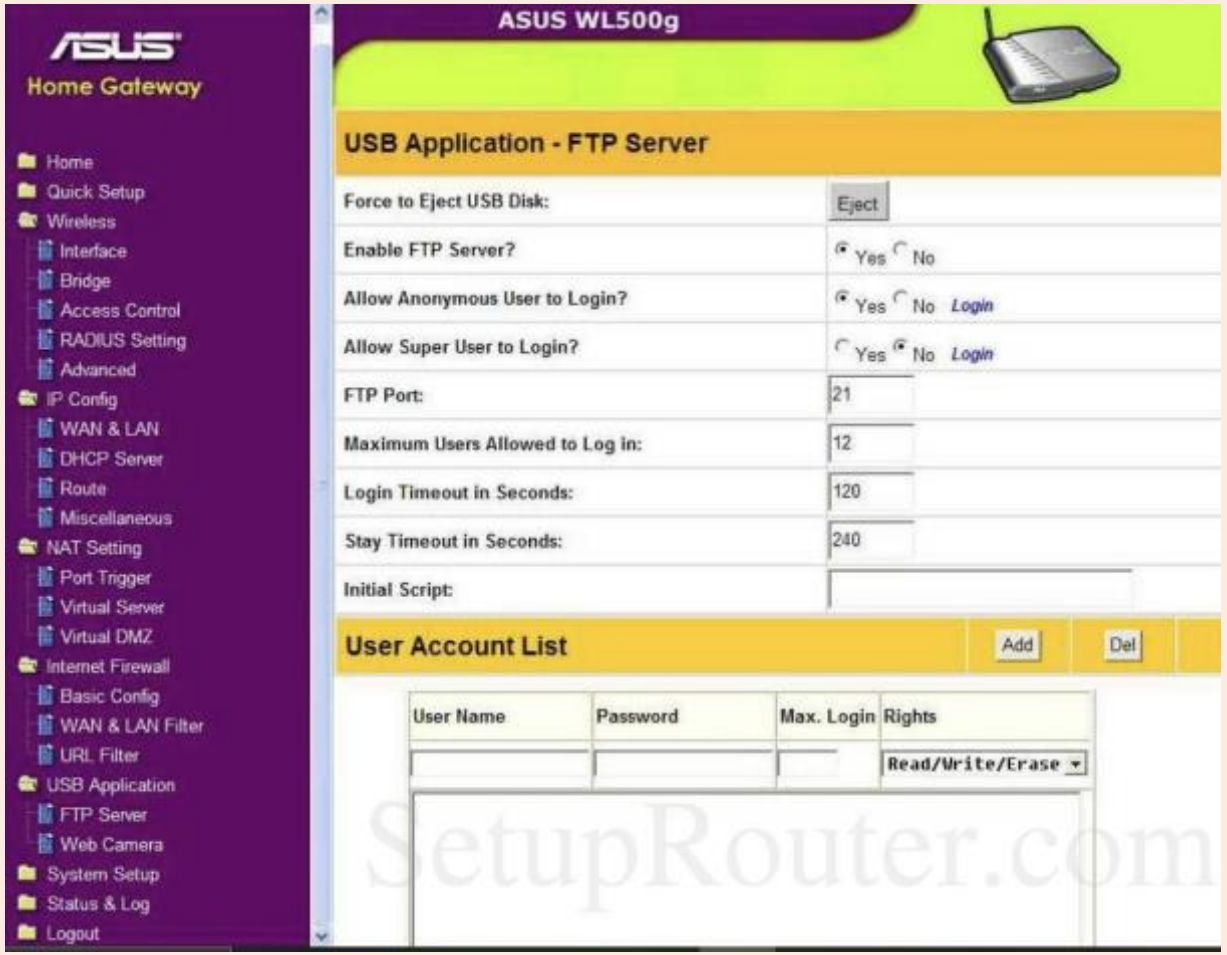
File Transfer Protocol (FTP)

- Next, make your way to the advanced settings on the app/configuration page and find a tab called USB Storage, USB Settings, or something similar.
- Once in that tab, click the checkbox for "FTP via internet" or similar.
- Your USB device will now be available to users on your network.
- If you would like to be the only one to access the USB device, you can modify the read and write access to be admin-only.

File Transfer Protocol (FTP)

- Some routers will have you configure read and write access for specific folders.
- Simply click "new folder," "select folder," or something similar, and navigate to the desired folder on your USB device.
- Select the folder and click apply changes.

File Transfer Protocol (FTP)



MAC Address Filtering

- Think of a MAC (media access control) address as a universally unique name for any network device.
- The address is tied to the device hardware.
- Some routers allow you to set a list of specific MAC addresses that can (or can't) access your network.
- It's like blacklisting or whitelisting what devices can access your LAN.
- Netgear device settings configuration
- To do this, find the MAC filter under the advanced settings tab.

MAC Address Filtering

- Dual- or tri-band routers will typically have you select which band the filter will apply to, and some routers will have you select whether the entered MAC address will be the only one accepted onto the network or the only address rejected from it.
- Once you've set your preferences for those options, the last step is to find the MAC addresses on the devices you'd like to filter and type them in.

Parental Controls

- Parental control, at a minimum, lets you establish time limits for when each allowed device (identified by MAC address) can be on the network.
- So, if your grandkids have a bad habit of using devices long after bedtime, but you don't want to constantly play the bad cop who has to police where and when devices get turned in every night, no problem.
- First use MAC address filtering to make sure that only approved devices can connect to your router.

Parental Controls

- Then use parental controls to make sure those allowed devices can only connect within approved hours.
- It only takes a few minutes to set up and, like having a well-configured router in general, will cure innumerable headaches and make sure your household runs much more smoothly.

What is Wi-Fi?

- Wi-Fi is a wireless networking technology that allows devices such as computers (laptops and desktops), mobile devices (smart phones and wearables), and other equipment (printers and video cameras) to interface with the Internet.
- It allows these devices – and many more IoT devices – to exchange information with one another, creating a network.
- When you access Wi-Fi, you are connecting to a wireless router that allows your Wi-Fi compatible devices to interface with the Internet.

What does Wi-Fi Mean?

- Wi-Fi is not an acronym.
- This term was coined by a branding company, and it only caught on in its abbreviated form.

How does Wi-Fi Work?

- On the technical side, 802.11 is a set of IEEE standards that govern wireless networking transmission methods.
- Each standard is an amendment that was ratified over time.
- The standards operate on varying frequencies, deliver different bandwidth, and support different numbers of channels.

Wi-Fi 802.11 Subcategories

- 802.11a and 802.11b were developed at about the same time – 1999.
- 802.11b enjoyed faster acceptance because its implementation was more affordable.
  - They use different frequencies, so are incompatible.
- 802.11a found a niche in businesses, while the less expensive 802.11b became standard in homes.
- 802.11g emerged as a hybrid standard that contained the top-rated features of a and b.
  - Despite a large bandwidth and good speed, it still faced interference from other appliances.

Wi-Fi 802.11 Subcategories

- 802.11n is presently used around the world, it evolved in terms of wireless antennas and signals.
  - It has a capacity of transferring data at speeds of maximum 450 Mbps.
  - It even has a better bandwidth (2.4 Ghz and 5 Ghz) and limited interferences.
- 802.11ac has High Frequency, better speed, but short range.
  - It is capable of providing speeds within the range of 7Gbps as well as higher internet speeds.

Wi-Fi 802.11 Subcategories

- 802.11ax: High Connectivity through MU-MIMO Technology.
  - It is a variant, which mainly focuses on the advanced features including MU-MIMO and enhanced life sustainability.
  - MIMO is a set of multiple-input and multiple-output technologies for wireless communication, in which a set of users or wireless terminals, each with one or more antennas, communicate with each other.
  - It also highlights advancements such as Bluetooth 5.0 technology and infrared connectivity.
  - The dominant feature that is lacking in this variant is the improved speed.
  - However, it was later noted for its top speed of 11Gbps at CES 2018.

Game Changer 802.11ax

- 802.11ax isn’t capable of the massive speed generated by the 802.11ad but is capable of providing much better Internet connectivity and speed when compared to the 802.11ac variant.
  - This Wi-Fi technology was built to suit smart devices which are being used by the conventional people on a regular basis.
  - This standard made its market appearance in 2019.
- The Wi-Fi Alliance bowed to the call for an easier nomenclature for the technology that had followed the 802.11 brand moniker, with the latest version designated as 802.11ax.

Wi-Fi Alliance

- In 1999, several visionary companies came together to form a global non-profit association with the goal of driving the best user experience, regardless of brand, and using a new wireless networking technology.
- In 2000, the group adopted the term “Wi-Fi®” as the proper name for its technical work and announced its official name: Wi-Fi Alliance®.

Wi-Fi 6

- The Wi-Fi Alliance® introduced Wi-Fi 6 as the industry designation for products and networks that support the next generation of Wi-Fi®, based on 802.11ax technology.
- Wi-Fi 6 is part of a new naming approach by the Wi-Fi Alliance that provides users with an easy-to-understand designation for both the Wi-Fi technology supported by their device and used in a connection the device makes with a Wi-Fi network.
- The new naming system identifies Wi-Fi generations by a numerical sequence which correspond to major advancements in Wi-Fi.

Wi-Fi 6

- The generation names can be used by product vendors to identify the latest Wi-Fi technology a device supports, by OS vendors to identify the generation of Wi-Fi connection between a device and network, and by service providers to identify the capabilities of a Wi-Fi network to their customers.
- The new numerical sequence are:

  Wi-Fi 4 to identify devices that support 802.11n technology

  Wi-Fi 5 to identify devices that support 802.11ac technology

  Wi-Fi 6 to identify devices that support 802.11ax technology

  Wi-Fi 6e to identify devices that support 802.11ax extended technology

Wi-Fi 6e

- Simply put, Wi-Fi 6E means Wi-Fi 6 extended to the 6 GHz band.
- Wi-Fi 6E works with the same standard as Wi-Fi 6 but with an extended spectrum.
- The 6 GHz band is the new frequency band ranging from 5.925 GHz to 7.125 GHz, allowing up to 1,200 MHz of additional spectrum. Unlike the existing bands on which channels are currently crammed into the limited spectrum, 6 GHz band exists without overlap or interference.
- Access to the 6 GHz frequency brings more bandwidth, faster speeds, and lower latency, opening up resources for future innovations like in Augmented Reality/Virtual Reality (AR/VR), 8K streaming, and more.

What is a Wireless Access Point?

- A wireless access point (AP) allows wireless devices to connect to the wireless network.
- What a wireless access point does for your network is like what an amplifier does for your home stereo.
- A wireless access point takes the bandwidth coming from a router and stretches it so many devices can go on the network from farther distances.
- A wireless access point does more than simply extend Wi-Fi.
- It also gives useful data about the devices on the network, provides proactive security, and serves many other practical purposes.

What are Hotspots?

- **Mobile Hotpot**
  - A mobile hotspot is a common feature on smartphones with both tethered and untethered connections.
  - When you turn on your phone’s mobile hotspot, you share your wireless network connection with other devices that can then access the Internet.

Benefits of Wi-Fi

- **Convenience**
  - Wireless networks allow multiple users to connect through the same network.
  - In a fraction of seconds without any configurations, connections can be made through the router or hotspot technology.
  - This ease of use and convenience is not present in the wired networks.
  - In a wired network, it takes more time to configure and allow access to multiple users.

Benefits of Wi-Fi

- **Mobility**
  - As long as you are in the range of a Wi-Fi Access Point, with Wi-Fi you can access the Internet from anywhere you want especially with the mobile devices.
  - You don't have to always sit right in front of your computer to get Internet access.
  - You can pay your bills, send email, search the Internet….

Benefits of Wi-Fi

- **Productivity**
  - Users who connect to a Wi-Fi network can experience different ranges of speed as they move from one location to another.
  - There are also less chances of experiencing technical glitches with the Wireless LAN.
  - As a result, users can be more engaged, complete tasks, and enhance their overall productivity.

Benefits of Wi-Fi

- **Deployment**
  - The installation of a Wi-Fi access point is relatively easy compared to a Wired network connection.
  - There are no complex cables being run in different locations and operating switches.
  - Think of setting up a desktop with the network connection in your home office?
  - Installing a new Wi-Fi router is easy rather than fitting a complex cable network.

Benefits of Wi-Fi

- **Expandability**
  - Adding new users to a Wi-Fi network is an easy task.
  - With the proper Wireless LAN credentials, more users can access the Wi-Fi network.
  - Additionally, there is no need to install any new type of equipment, all can be done with existing equipment.
  - This significantly saves your time and effort.

Benefits of Wi-Fi

- **Cost**
  - Compared to a Wired network connection, Wireless networks offer significant advantages in terms of cost and labor.
  - Especially when installing a new Wi-Fi network, you can cut down the expenses in wiring and maintenance.
  - Out of these the bigger expense comes under the wiring part.
  - Since very a smaller number of wires are used here, it can save you money.

Disadvantages of Wi-Fi

- **Security**
  - Even though many encryption techniques are taken by the wireless networks, still the Wi-Fi is vulnerable to hacking.
  - Due to its wireless nature, it has high chances of being hacked especially Public Wi-Fi networks.
  - Since Public Wi-Fi networks are open for anyone, hackers can impose their fake networking ID.
  - Without consent users may connect to this fake ID and fall into the category of cyber-attack victims.

Disadvantages of Wi-Fi

- **Range**
  - Range offered by a Wi-Fi network is limited, typically around 100-150 feet.
  - While it is sufficient for a normal home, it can actually be a problem for building structures.
  - The strength of a Wi-Fi network will be reducing as you move away from the access point.
  - Since building can be multistoried, the strength of the Wi-Fi network can be varying at different floors.
  - The cloud weakens workflow.
  - The only way to overcome this is by purchasing additional access points.

Disadvantages of Wi-Fi

- **Speed**
  - The speed of a Wi-Fi connection is far slower than a wired connection (around 1-54 Mbps).
  - This may look fine if there are few devices connected to the network.
  - The moment there are more devices connected, you could experience a drastic reduction in speed.

Disadvantages of Wi-Fi

- **Reliability**
  - A Wi-Fi network works in the frequency of 2.4 Ghz.
  - This frequency has high chances of getting hindered due to the electromagnetic waves and other forms of obstacles.
  - As a result, you may frequently experience connectivity issues and weak signal strengths.
  - Especially during large file transfers, the signal can get interfered.

Disadvantages of Wi-Fi

- **Bandwidth**
  - Many routers only allow 30 maximum devices to be connected.
  - The bandwidth of the Wi-Fi network gets weaker as you add more devices.
  - It is solely reserved for a single user.
  - Most often when the bandwidth gets limited users can experience slow speeds.

Disadvantages of Wi-Fi

- **Health issues**
  - There are certain conspiracy theories about Wi-Fi that it causes health issues in humans.
  - Some of them are cancer, insomnia, and apoptosis.
  - Same as the effects caused from the Microwave frequencies (EMF).
  - It is also a phony notion about the effects caused from the Microwave frequencies (EMF) and advising pregnant women not to get exposed to the Wi-Fi signals as it releases Electromagnetic radiation.

Disadvantages of Wi-Fi

- **Power Outage**
  - Temporary loss of connectivity.
  - Once power is restored, most devices will reconnect.

Mesh Wi-Fi Routers

- Mesh Wi-Fi or Whole Home Wi-Fi systems consist of a main router that connects directly to your modem, and a series of satellite modules, or nodes, placed around your house for full Wi-Fi coverage.
- They are all part of a single wireless network and share the same SSID and password, unlike traditional Wi-Fi routers.
- Picture this: You've just set up your home network with the latest Wi-Fi hardware and a 100 Mbps Internet connection.
- But for some reason, you still encounter buffering when you try to stream video in the bedroom.

Mesh Wi-Fi Routers

- You called your ISP and everything checks out, so what's the deal?
- Chances are, your Wi-Fi isn't set up efficiently for a mesh Wi-Fi system.

What's Slowing Down Your Network?

- The weakened signal or Wi-Fi dead spots could be the result of physical obstructions.
- Simple things like the floor, doors, and walls of your home can come between you and your router, especially if they're made of metal, brick, or concrete.
- Or perhaps the distance is simply too great in a large home, and your traditional router is only capable of reaching as far as the kitchen, but not to the backyard, the garage, or a distant bedroom.

What's Slowing Down Your Network?

- Interference from other devices could also be the culprit, whether it's your microwave, cordless phone, or baby monitor.
- If you live in close quarters with other Wi-Fi networks and devices—such as in an apartment complex—this problem increases tenfold.
- Think of it like a room full of people who are all speaking at once—nobody's going to be heard very well.

Blanketing Your Home with Wi-Fi

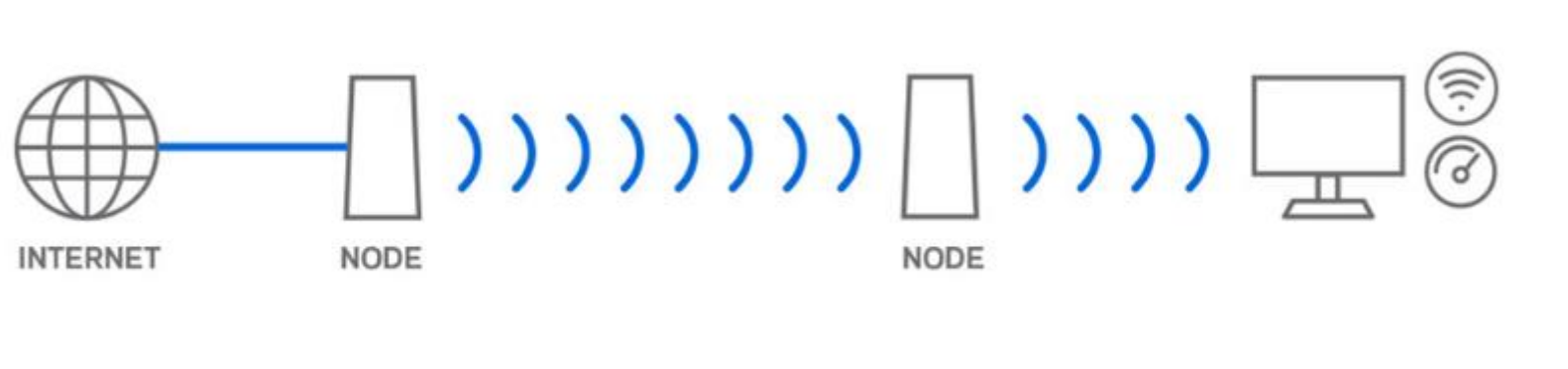
- A better solution is Wi-Fi that works with your home design, instead of against it.
- Think of a standard router like a speaker.
- You could be playing music loudly in the front of your home, but the office in the back will only hear a faint echo.
- A standard router works the same way—you can only move so far from it before the signal starts to wane, and eventually it’s going to cut out altogether.

Blanketing Your Home with Wi-Fi

- Instead, why not install a “speaker” in each room of the house?
- That’s how whole home Wi-Fi or mesh networks work, with multiple nodes installed around your home so you’ve got solid Wi-Fi coverage from one end to the other, even the backyard.

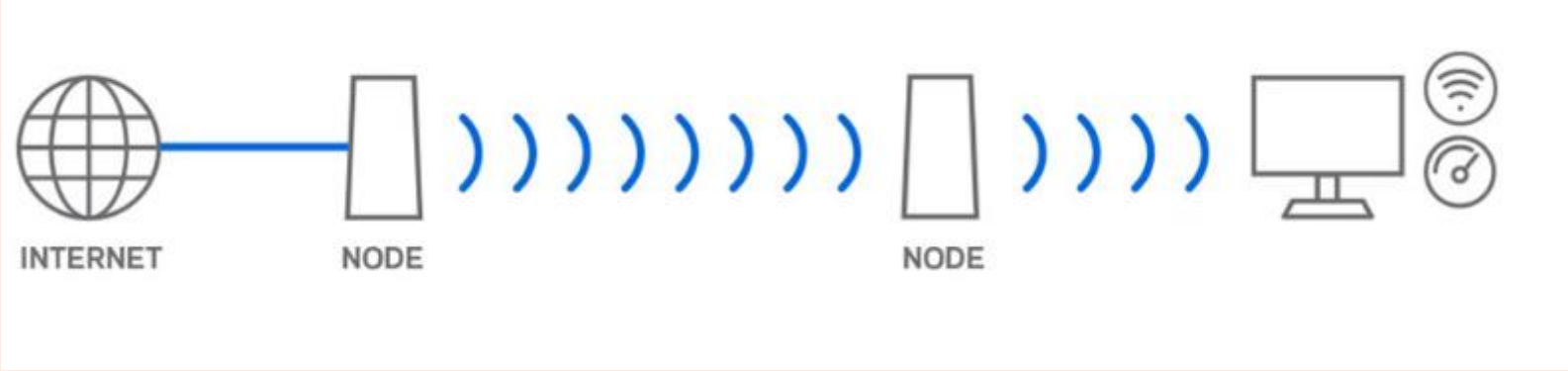
Blanketing Your Home with Wi-Fi

- **Wired and Wireless Expansion**
  - In a modular system, there's one node connected to your modem that acts as a router.
  - Each additional node finds the best channel and path to wirelessly connect to the previous one, creating a seamless and reliable Wi-Fi connection throughout your entire home.



Blanketing Your Home with Wi-Fi

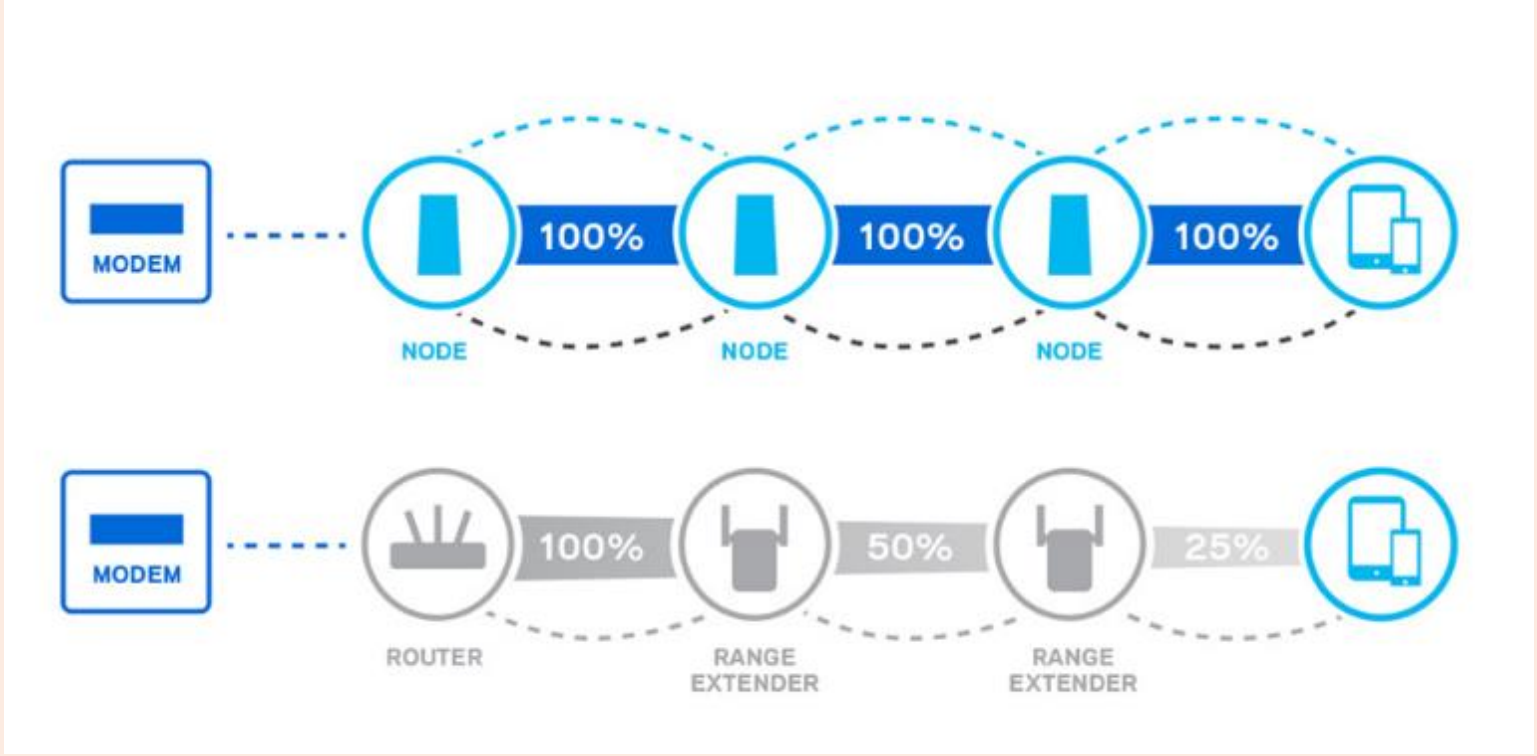
- **Wired and Wireless Expansion**
  - However, if your home is already wired with Ethernet cables in every room, some mesh systems can still connect the nodes together using an Ethernet cable to create a whole-home Wi-Fi system.
  - Even using the wired option, you'll still be able to expand your signal to hard-to-reach areas such as the garage or basement.



One Network and Seamless Roaming

- The name “mesh network” itself implies that every component of your Wi-Fi system is working together, and seamless roaming is a perfect example of that.
- When you use a router and range extender combination, you have to switch between the networks manually as you move from one coverage zone to the other.
- But with seamless roaming, you only have one network with one name and password—that means that as you move about your home, you’ll never have to manually switch from one network to the other.
- So, go ahead, stream video in the living, kitchen, or bedroom without worrying about buffering or a dropped connection.

One Network and Seamless Roaming



Mesh Vs. Traditional Router with Range Extenders

Why Not Use a Range Extender?

- Comparing range extenders to whole home Wi-Fi is like comparing apples to oranges.
- Range extenders are certainly effective when it comes to increasing the range of your router, but they do so at the expense of Wi-Fi performance, which gets cut in half.
- In a large space where Wi-Fi struggles to reach every corner, a range extender can diminish the overall performance of your network, creating a bottlenecking effect.
- You might also experience connection issues when jumping from the router to the extender, because you'll need to switch networks manually.

Why Not Use a Range Extender?

- For example, even when standing next to the range extender, you can still experience dead zones or slowdowns if you haven’t manually changed your device over from the router’s signal.
- These two separate networks also have different names and interfaces, which can be a serious hassle.

Wi-Fi Security – WEP/WPA

- Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b. That standard is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.
- WPA2 has been the recommended way to secure your wireless network since 2004 because it is more secure than WEP and WPA.

Wi-Fi Security - WEP/WPA

- WPA3 makes further security improvements that make it harder to break into networks by guessing passwords; it also makes it impossible to decrypt data captured in the past i.e., before the key (password) was cracked.
  - stronger encryption in both enterprise and personal modes
  - improved authentication for personal mode
  - perfect forward secrecy for personal mode communications
  - not compatible with some legacy devices

Wi-Fi Security - WEP/WPA

Wireless security cheat sheet

ENCRYPTION STANDARD	FAST FACTS	HOW IT WORKS	SHOULD YOU USE IT?
Wired Equivalent Privacy (WEP)	First 802.11 security standard. Easily hacked due to its 24-bit initialization vector (IV) and weak authentication.	Uses RC4 stream cipher and 64- or 128-bit keys. Static master key must be manually entered into each device.	No
Wi-Fi Protected Access (WPA)	An interim standard to address major WEP flaws. Backward-compatible with WEP devices.	Retains use of RC4 but adds longer IVs and 256-bit keys. Each client gets new keys with TKIP. Enterprise mode: Stronger authentication via 802.1x and EAP.	No
WPA2	Upgraded hardware ensured advanced encryption didn't affect performance.	Replaces RC4 and TKIP with CCMP and AES algorithm for stronger authentication and encryption.	If WPA3 is not available
WPA3	Current standard. New authentication method helps thwart KRACK and offline dictionary attacks.	Replaces PSK four-way handshake with SAE. Enterprise mode has optional 192-bit encryption and a 48-bit IV.	Yes

IPv4 vs IPv6 — What's the Difference Between the Two Protocols?

- IP, an abbreviation for Internet Protocol, is a protocol that helps computers/devices communicate with one another over a network.
- As the "v" in the name suggests, there are different versions of Internet Protocol: IPv4 and IPv6. What Is the Internet Protocol (IP)?
- Internet Protocol (IP) is a set of rules that help with routing packets of data so the data can move across networks and make it to the right destination.
- The Internet Protocol (IP) helps route data around networks. To accomplish this, each device is assigned an IP address.

IPv4 vs IPv6 — What's the Difference Between the Two Protocols?

- IPv4 is the original version that was launched back in 1983.
- However, its 32-bit format only allows for ~4.3 billion unique addresses, which can't serve the needs of the modern world.
- To address the lack of unique IPv4 addresses (and make some other technical changes), IPv6 was created. IPv6 uses a 128-bit address format that offers 1,028 times as many unique addresses as IPv4.
- For most people, that's all you need to know – IPv6 uses a different format and offers far more unique addresses than IPv4.

Getting the Most Out of Your Router

- Anybody can get an Internet connection up and running in a few minutes by using your router's quick start guide, but most models hide lesser-known treasures in their setup menus.
- If you want to get the most value possible out of your router investment, take the extra time to explore these advanced options.
- If you're still in the market for a new router, consider going beyond the box's features list and the product's spec sheet.

Getting the Most Out of Your Router

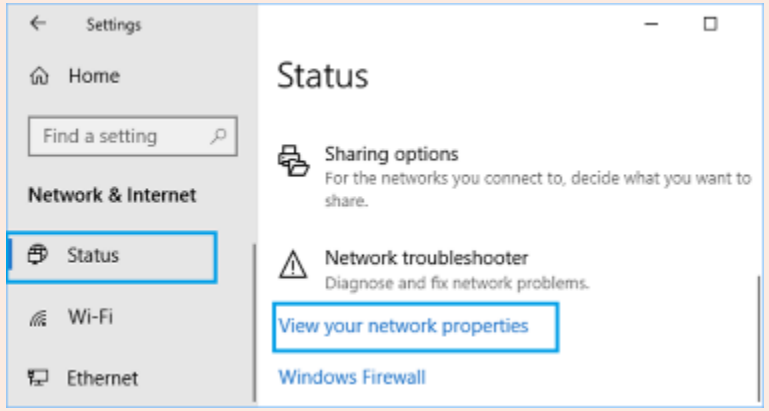
- Download the manual, dig into the advanced options, and see which features will deliver the most value in your environment.
- Once you're up and running, test your Internet speed.
- If you need more guidance, Google: 10 Tips to Speed up Your Wi-Fi and 12 Tips to Troubleshoot Your Internet Connection.
- Again, YouTube videos will give you a wealth of information and recommendations.

How to Find a Router IP Address in Windows 10

- As, the router has its own unique IP address you need to know it in order to log in to the router.
- In general, people want to log in to their router to update the software, change security settings, set up parental controls and set up IP address filtering.
- Router manufacturers like D-link and LinkSys use 192.168.0.1 and 192.168.1.1 as the Default Router IP Address and make this information available on their websites.
- The default router IP address should also be available in the instruction manual that came with your router.

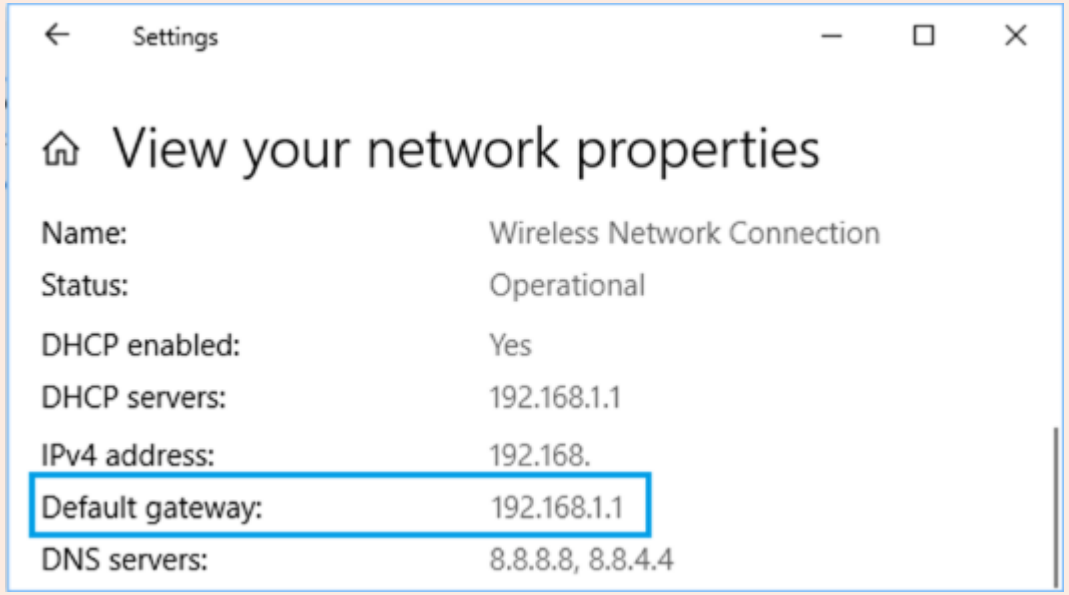
How to Find a Router IP Address in Windows 10

- You should also find the default router IP address printed on a sticker/label attached to the bottom of the router.
- If the default router IP address has been changed by your ISP, you will have to find it on your computer using the below method.
- If you are using a Windows laptop or desktop computer, you can follow the steps below to find Router IP address in Windows 10.
- Go to Settings > Network and Internet > click on Status in the left pane.
- In the right-pane, scroll down and click on View Your Network Properties link.



How to Find a Router IP Address in Windows 10

- On this screen, scroll down to the details of your active network (Ethernet or Wireless) and you will see the IP Address of your router listed next to “Default gateway.”



The Internet Doesn't Have to be Scary

- The best way to protect yourself online is to know what to expect.
- Take the time to understand some popular threats and learn how to avoid them.
- Think of your antivirus program as a safety net that will catch you if your safe browsing habits aren't enough.
- Remember these tips:
  - Don't visit unsafe websites.
  - Ignore any emails from unknown senders.
  - Protect your private information.
  - Keep your email address out of the hands of predatory marketing companies.

The Internet Doesn't Have to Be Scary

- Keep your antivirus up to date.
- Perform routine virus scans.
- Don't keep your passwords saved in a document on your computer and change them regularly – use a password manager.
- Reboot your modem and router at least twice a month.

- It's always easier to avoid danger when you know what to look for.
- With good habits and strong security software, you'll be able to browse safely, check in on your loved ones, and enjoy all the benefits of being connected.

Resources

- https://www.wikihow.com/Install-a-Modem
- https://www.wikihow.com/Connect-a-Router-to-a-Modem
- https://www.lifewire.com/what-is-wi-fi-2377430
- The Muppets: "Modem" Film Clip - Bing video
- BBS: The Documentary (bbsdocumentary.com)
- WPA 3 https://tinyurl.com/yuj7ny4j
- https://www.digitalcitizen.life/what-does-ac1200-ac1900-ac3200-mean/
- https://techusersguide.com/why-do-wifi-routers-have-multiple-antennas/
- https://www.tp-link.com/us/wifi-6e/

An International Association of Technology & Computer User Groups

- APCUG Saturday Safari
- Modems, Routers, and Wi-Fi

Wjames(at)apcug.org

Questions?