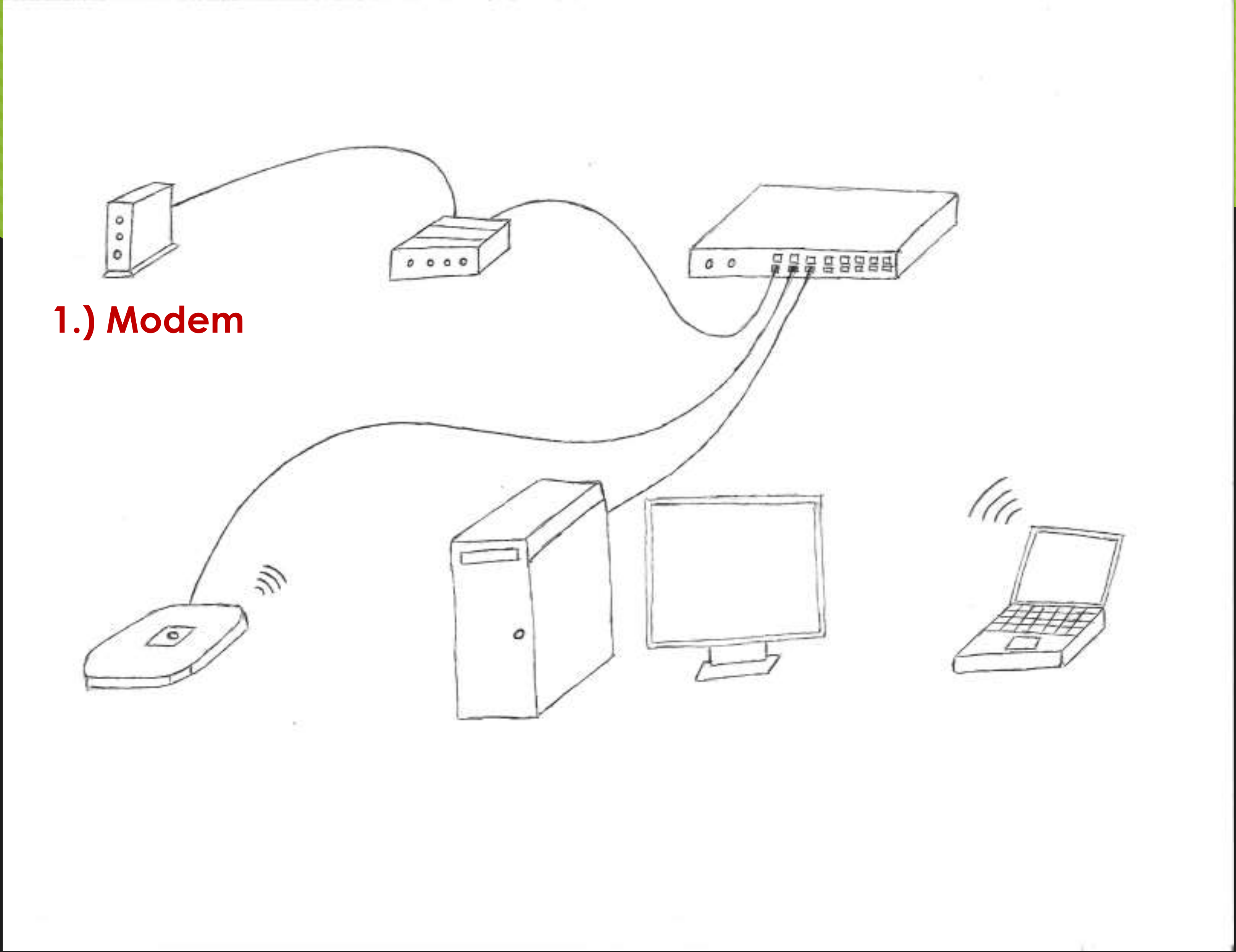
Basics of Computer Networking

Wednesday, January 31, 2024
Virtual

What is a Computer Network?

- For our purposes, a computer network is the equipment that allows computers and other devices to reach the internet and each other, whether wired or wireless.
- Basic Categories:
  - Wired Devices – Modem, Router, Switch, Cabling
  - Wireless Devices – Wireless Access Point



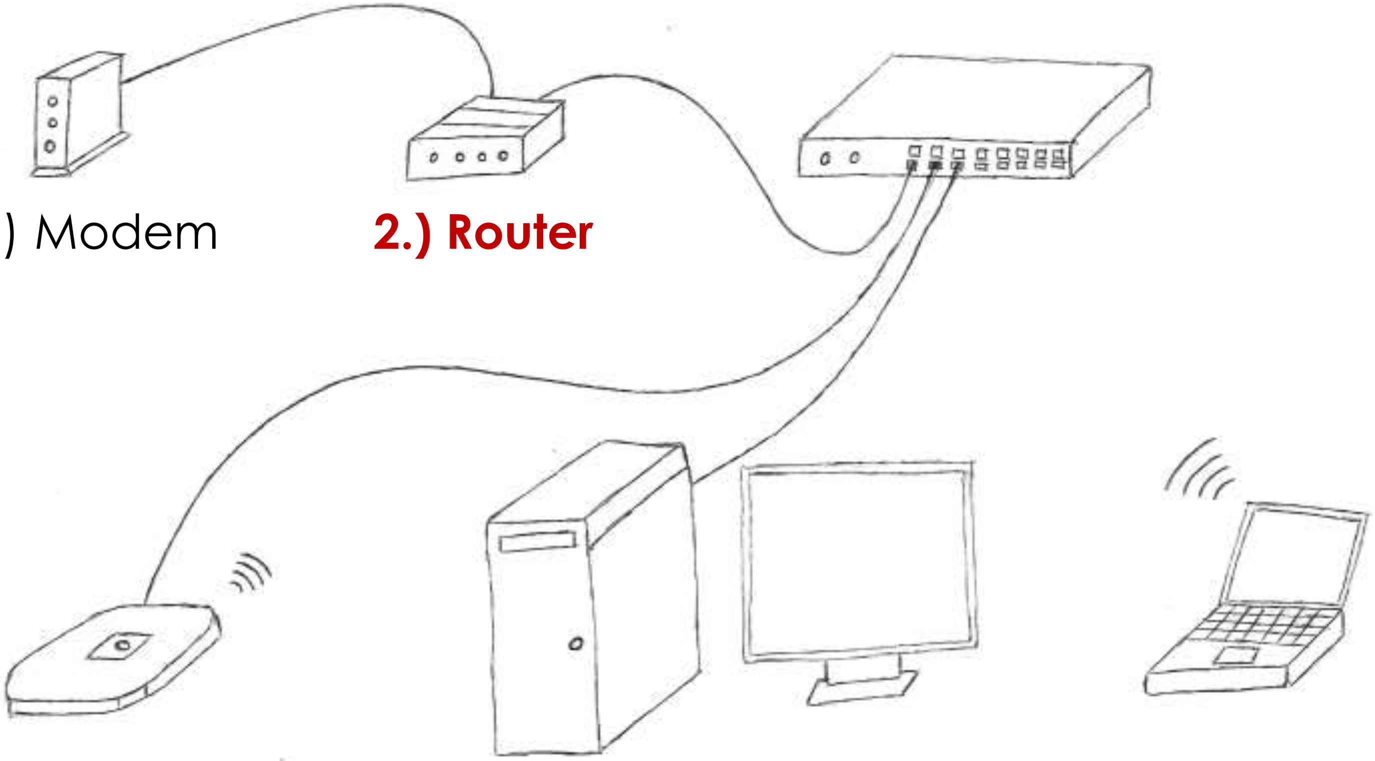
1.) Modem

1.) Modem

- Differs based on technology (cable, fiber, satellite), but basically does the same thing.
- Connects your network to the provider’s network (and thus, the internet).
- Internet Provider may give you one for free, may charge you for one, or you may be able to buy your own.
- A modem has very little configuration. It has some lights and a web interface that might help if it’s not working.

Aside – Combination Devices

- Internet providers (especially residential ones) increasingly provide devices that combine functions – a modem/router/firewall/wireless access point.
- You can also just ignore their added functionality, and use something separate but better. This is especially true for WiFi.



1.) Modem

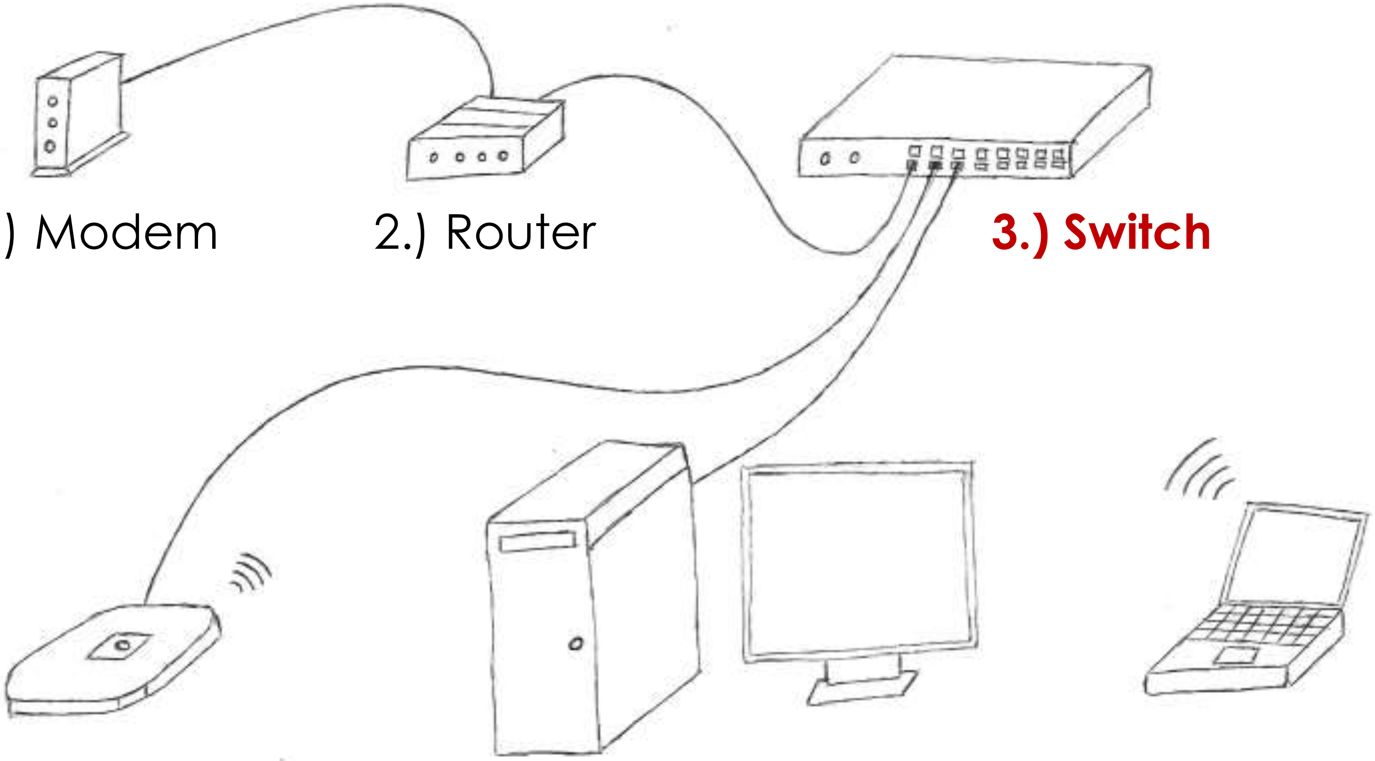
2.) Router

2.) Router/Firewall

- Connects the modem to the rest of your network and keeps track of what needs to go where.
- A firewall can be a separate device but is often combined. Basically, it allows connections you want and prevents ones you don’t.
- Routers and firewalls have a lot of configuration options for customizing your network.

Aside – Device Security

- Passwords - If networking devices have a default password, you should definitely change it, unless it’s a long random string of characters (some internet provider devices may have this). And then write it down somewhere safe. This is most relevant for routers and wireless access points, which face the outside world.
- Updates – If your networking devices don’t auto update, you should occasionally check for security updates. Again, this is most relevant for routers and wireless access points.



1.) Modem

2.) Router

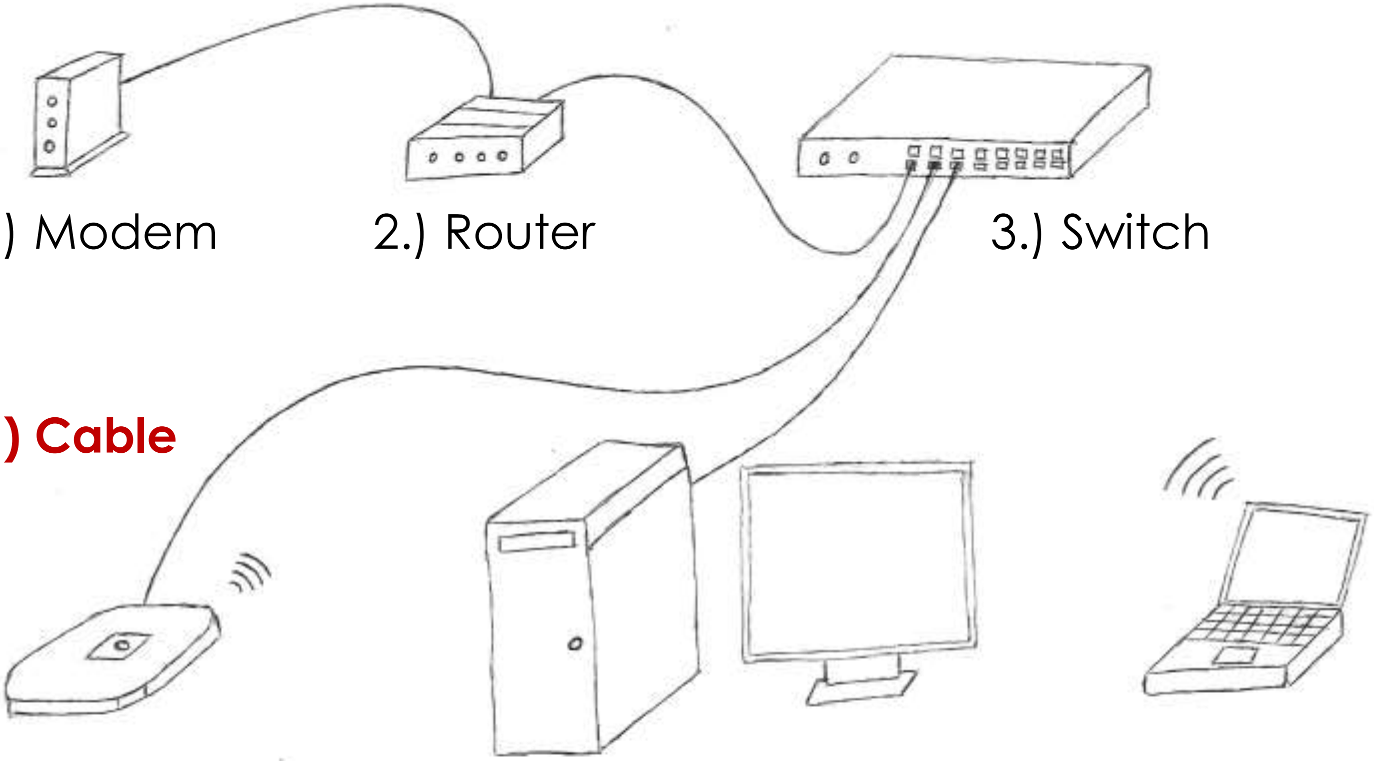
3.) Switch

3.) Switch

- Allows you to connect more devices to the network by cable. Can have 5, 10, 24, or even 48 ports.
- Managed switches allow you to configure how your network is structured, but cost more. Unmanaged switches have no configuration options, while managed ones do.
- Power Over Ethernet (POE) switches carry electrical power in the network cable, making it simpler to hook up devices like wireless access points and IP cameras (but cost more).

Aside – Battery Backup

- Though not technically part of a network, you might use an uninterruptible power supply for your networking equipment. This battery backup gives you power for a certain amount of time during an outage, but also protects your equipment from power surges/fluctuations.



1.) Modem

2.) Router

3.) Switch

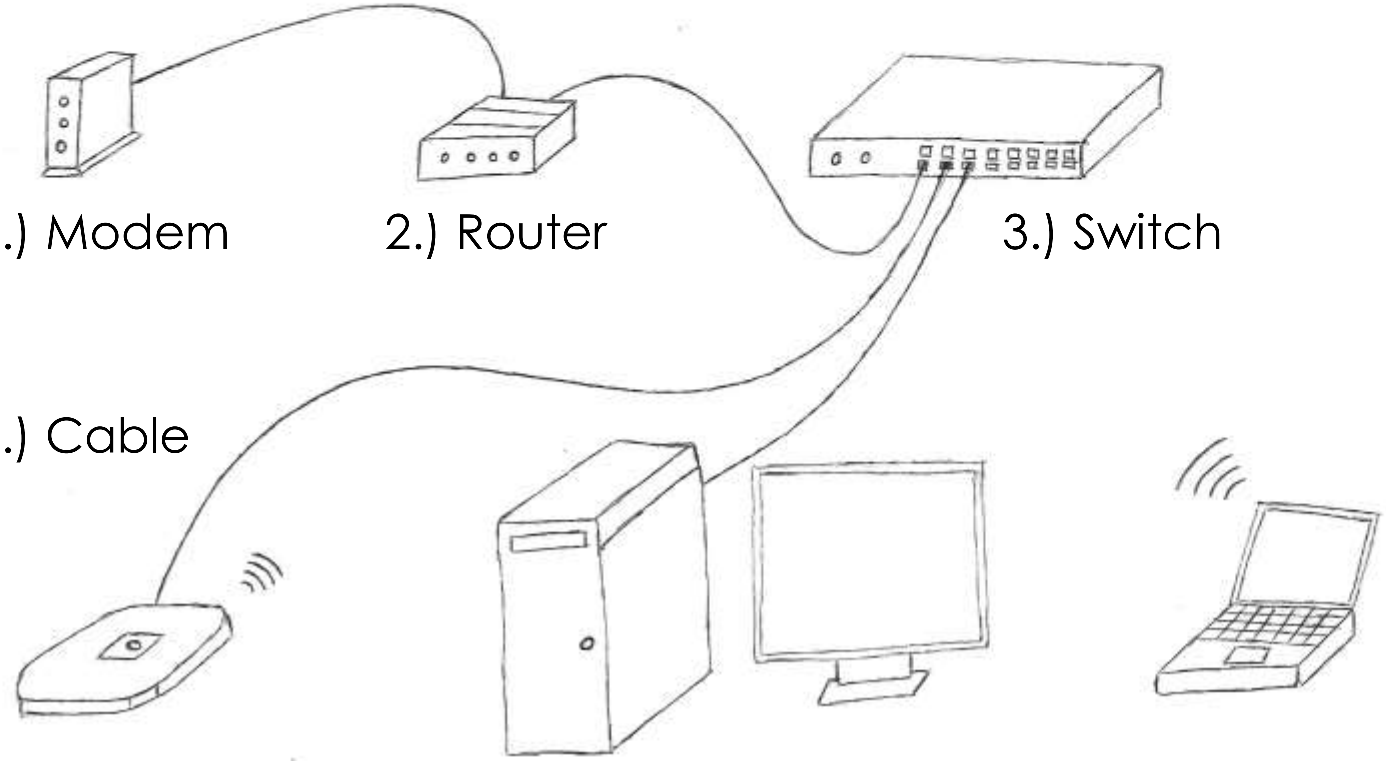
4.) Cable

4.) Network Cable

- Not a device, but connects all of your wired network.
- Includes the cable on the floor or in the wall/ceiling, as well as the network jacks in the wall.
- Patch bays look like a switch, but are really a way to organize/extend cables. They don’t have any lights and don’t plug in to an electrical outlet.

Aside – Wired Connection Speeds

- Every device with an ethernet jack has a maximum speed – 10 Mbps (outdated), 100 Mbps, 1000 Mbps (Gigabit).
- Today, you should opt for Gigabit or faster if at all possible, so it doesn’t become a bottleneck when/if you get faster internet.
- Ethernet cable also has a speed associated, so it’s possible you might eventually have to replace some old cable to get Gigabit speeds.
- Be aware, switches and potentially some routers might have 1-2 fast ports, with the rest slower.



1.) Modem

2.) Router

3.) Switch

4.) Cable

5.) Wireless Access Point

5.) Wireless Access Point

- Provide a WiFi signal to users. You might need anywhere from one to many, spread around the building.
- Can be sitting on a shelf, mounted on the wall or ceiling, or even on the exterior of the building or in the middle of a garden.
- In a mesh network, the Access Points are connected to each other wirelessly, they don't all have to be on cables (which is a bit slower, but could be easier).
- Access Points have considerable configuration options, depending on how you want your WiFi to be setup.

Aside – WiFi Standards & Speeds

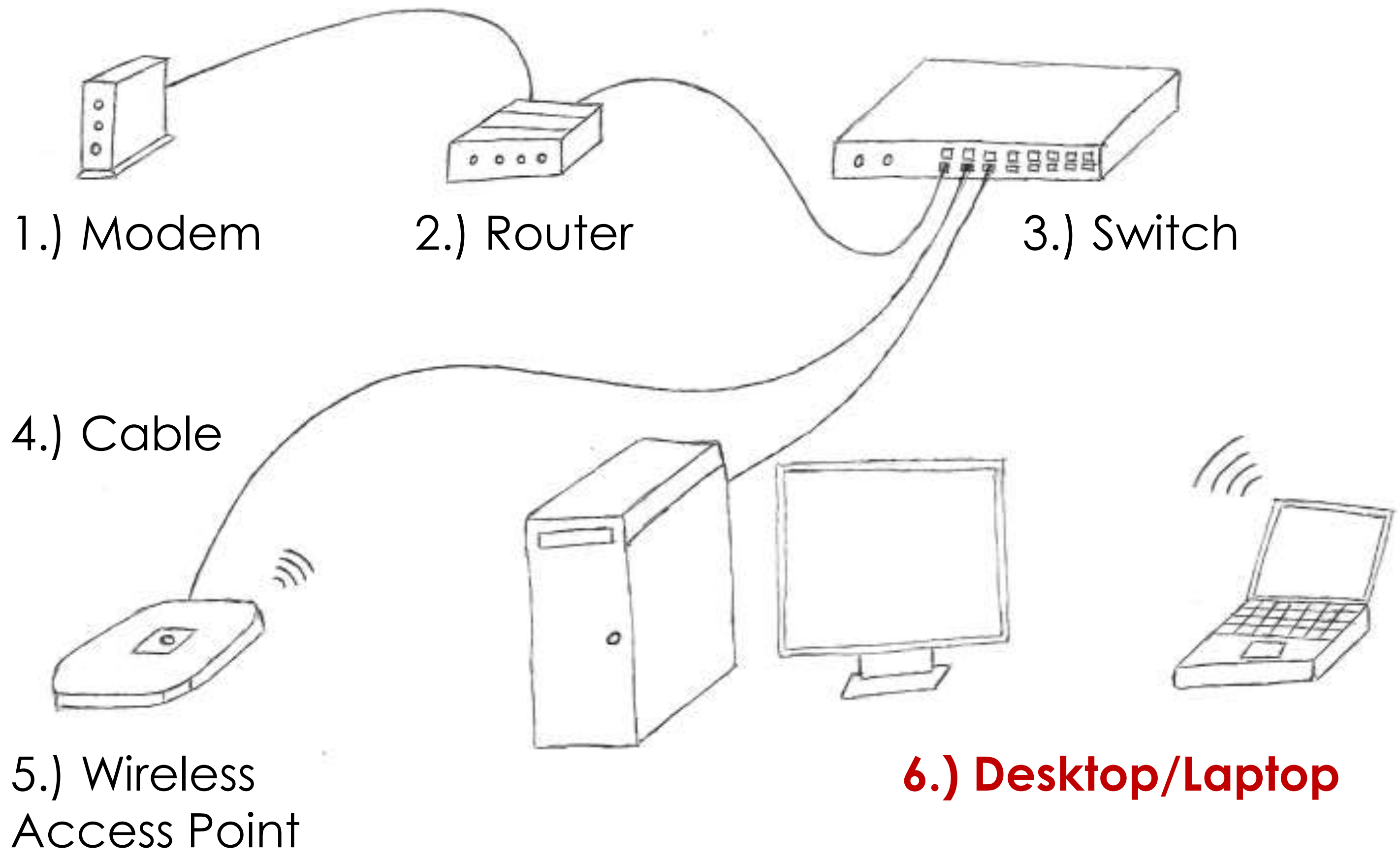
- WiFi generations are a bit gibberishy, with names like 802.11ax or be, or Wi-Fi 6 or 7 (which are among the current offerings).
- But you might also see other complicated info about bands, beam forming, MU-MIMO and the like.
- To really get a handle on a specific model, you may need to check out reviews or talk to an expert.

Aside - WiFi Terms

- SSID – The name that identifies your WiFi (“JoshHouse”). You can have multiple SSID’s for different uses (like a staff-only one).
- Band – Devices offer 2 (or even 3) different frequency bands: 2.4, 5 and 6 Ghz, but things are mostly automatic for users at this point.
- Should I Use a Password? – There is some disagreement on this for public WiFi. A password means that data is encrypted while it is being transmitted, though with WPA2 it is not wildly difficult to crack with a known password.
- Security – WPA3 is more modern and secure than WPA2.

Aside - WiFi Statistics

- The options for WiFi statistics vary dramatically by wireless access point:
  - For some (like Meraki), there are easily accessible stats.
  - Other devices will give you a log of devices connected over the last 24 (for example) hours. By checking this once a day for a week, you can get a solid estimate for usage.
  - Still other devices have incredibly basic logging, which can make it nearly impossible to get useful numbers.



1.) Modem

2.) Router

3.) Switch

4.) Cable

5.) Wireless Access Point

6.) Desktop/Laptop

6.) Desktops, Laptops, Tablets, Phones

- Your network ultimately reaches a device being operated by a patron or staff member, whether wired or wireless.
- Before the internet, networks were primarily intended to allow devices to reach one another within a network. But now, with the exception of printers and the few local servers, most of the time we’re just trying to reach the internet.

Aside – Servers and Storage

- There was a time when servers were common in libraries. But with the move to web-based ILS's, and to cloud-based storage, they've become much less frequent. Servers can offer a range of functionality – domain controller, file server, web server, applications (such as an ILS). Servers bring a dramatic increase in administrative complexity and security concerns, and may not be necessary in many situations.
- Network Attached Storage (NAS) is like a simplified server, that just functions as a file server.

Aside – VoIP Phone Service

- Voice Over IP (VoIP) phone service runs as part of your network, rather than using traditional phone lines. Typically, the devices look just like normal phones, rather than calling through a computer.
- It often requires a specific switch, router, or other device which connects to the phones.

Aside – Addressing

- Almost every device on a network has some basic info that allows it to be found, and to find other devices:
  - IP Address – Functions a bit like a phone number. Ranges from 0.0.0.0 to 255.255.255.255. With the numbers going from broad to narrow left to right (sort of like an area code). This is for IPv4 – the newer approach (IPv6) is similar, but has much larger numbers.
  - IP addresses are usually assigned automatically by your router (DHCP), based on the settings you assign. These addresses tend to stay the same on a regular network, but can change. Alternately, you can use a reservation or static IP to make sure a devices address doesn’t change.
  - Subnet Mask – This is a bit complicated. It looks like an IP address, but basically tells your computer how “big” the network you’re attached to is.
  - Gateway – This is the address for the network device that can reach other networks, typically a router.
  - MAC Address – Less important, but you might need to know it, for example to reserve an IP address. Every interface on a device has a unique MAC address that identifies it. For example, 00:1b:63:84:45:e6 .

Aside – Diagnostics

- Here are a few tricks you might be able to use for diagnosing:
  - On a Windows computer, if you open up a command prompt (cmd), you can enter the command ipconfig and it will list your IP address, subnet mask, and gateway. Other OS's will have a similar equivalent.
  - You can also run the ping command, to see if one device is visible to another on the network. Note, some devices are configured not to respond even if everything is working.
  - A speed test can be a good diagnostic to see if there are slowdowns in some portion of the network (bad cabling, poor WiFi signal, or a bottleneck somewhere).