Internet - The Internet is a network of computers. It can travel by radio waves, phone line, cable networks, and even the electrical wiring in your house. For the most part, data travels between computers using physical wires. Because wires are so efficient (and widely available), most Internet connections come via some sort of cable. The prevalent options are:

Landline telephone lines (DSL) - Download 5-35 Mbps, Upload 1-10 Mbps. Provided by phone companies like AT&T & CenturyLink. Cheaper but slower than cable & fiber optic options. Often your only wired option when you live in rural areas. Slower than Cable, but not affected by other peoples' usage.

Dial-up - This is the ancient stuff. Through phone lines but not the same thing as DSL. DSL is much, much faster.

Cable TV lines (cable) - Download 10-500 Mbps, Upload 5-50 Mbps. Slows does when everyone around you is using the internet at the same time.

Fiber-optic lines (fiber) - 250-1,000 Mbs wither direction. Verizon Fiios and Google Fiber.

The backbone of the internet is built on fibreoptic cables. It's only the last couple miles between your home and your ISP where the connection slows down because data switches over to older, copper cables. Fiber just isn't available everywhere.

Internet of Things - the next phase. 5G is supposed to be a key part in enabling such technologies, like driverless cars and smart homes, etc.

Web Server - The primary function of a web server is to store, process, and "serve" web pages to clients. Web servers typically operate on Linux, and most websites are hosted on Linux servers, though some use Microsoft Windows or other OS's. Servers also run key software programs in the background, these are called daemons. Confusingly "server" also refers to the software run on physical servers, the daemons. Examples of these servers include the HTTP server, FTP server, Database server, Email server. So you have to distinguish which server you're talking about. It can either refer to a sort of company computer connected directly to the internet, or a long running process (also called a daemon) which listens on a pre-specified port and responds to a request, which is sent using a protocol called HTTP, or one of the others listed. Every server has a unique IP address.

Daemon - a computer program that runs as a background process, rather than being under the direct control of an interactive user.

Operating System (OS) - Basically the bit that communicates between the hardware and software of your computer. People generally don't know how to address a CPU in assembler, or how to communicate with a graphics card. An OS such as Linux or Windows acts as a middleman. The dominant desktop operating system is Microsoft Windows with a market share of around 82.74%. macOS by Apple Inc. is in second place (13.23%), and the varieties of Linux are collectively in third place (1.57%). In the mobile (smartphone and tablet combined) sector, use in 2017 is up to 70% of Google's Android and according to third quarter 2016 data, Android on smartphones is dominant with 87.5 percent and a growth rate 10.3 percent per year, followed by Apple's iOS with 12.1 percent and a per year decrease in market share of 5.2 percent, while other operating systems amount to just 0.3 percent. Linux distributions are dominant in the server and supercomputing sectors.

Unix - A family of operating systems. Led to the Berkeley Software Distribution which in turn led to a bunch of other Operating systems, notably, **MacOS and Linux**. Originally developed at Bell Labs.

Linux - Linux is the leading operating system on servers and other big iron systems such as mainframe computers, and the only OS used on TOP500 supercomputers (since November 2017, having gradually eliminated all competitors). It is used by around 2.3 percent of desktop computers. The Chromebook (Google), which runs the Linux kernel-based Chrome OS, dominates the US K–12 education market and represents nearly 20 percent of sub-$300 notebook sales in the US. Linux also runs on embedded systems, i.e. devices whose operating system is typically built into the firmware and is highly tailored to the system. This includes routers, automation controls, televisions, digital video recorders, video game consoles, and smartwatches. Many smartphones and tablet computers run Android and other Linux derivatives. Because of the dominance of Android on smartphones, Linux has the largest installed base of all general-purpose operating systems. Although Android is based off Linux, it is not “Unix-like” in the sense of experience or command prompt. Linux is based off Unix. So really, among Windows, Mac, & Linux... Windows is the odd one out.

Distro - Different distributions of the linux OS. Ubuntu, Fedora, etc. are different flavours of the OS which you can use. Some distros are more for the server side, but some are for desktop, with varying learning curves.

Mainframe Computers - or mainframes (colloquially referred to as "big iron") are computers used primarily by large organizations for critical applications; bulk data processing, such as census, industry and consumer statistics, enterprise resource planning; and transaction processing. They are larger and have more processing power than some other classes of computers: minicomputers, servers, workstations, and personal computers. Mainframe computers are often used as servers.

Browser - The purpose of a web browser is to fetch information resources from the Web and display them on a user's device.

URL - Uniform Resource Locator. Whoever has this value will end up at the same address. Like 25 Arrowhead Cove, Gadsden, AL, 35901, USA, they'll end up at the same place. google.com is an abbreviation of https://www.google.com

HTTP - HyperText Transfer Protocol. The https:// protocol defines how your browser should connect to the website. Like you could take an X or a Black Uber to get to 25 Arrowhead Cove. On the internet either you use http:// or https:// - https is just a more secure version of http. It's encrypted. HTTP is essentially how you initiate your request for a website.

www - World Wide Web. This bit is kind of optional. It's like including the +1 in your phone number. But usually the browser includes it in the URL for completeness.

Domain Name - This is the actual name of the site: google.com, whitehouse.gov, wikipedia.org, etc.

DNS - Domain Name Service. This converts a domain name to an IP address so your computer knows where to go. Your computer keeps a list of recent domain-IP pairs on the hard-drive, but if it doesn't know the pair, it will ask your ISP.

IP Address - Internet Protocol Address. Everything that connects to the internet has a unique IP address, a letter-number combination. Websites have IPs. It's how computers locate websites.

TCP - Transmission Control Protocol. TCP essentially breaks up the website you're requesting into smaller packages. Then IP transmits them to your computer, and then TCP reassembles the packages and checks if anything is missing on your computer.

ISP - Internet Service Provider. These are the people who connect your home etc. to the internet via cable, dial-up, DSL, fiber, etc.

Common HTTP Status Codes: 200 = OK. 404 = Not Found. 500 = Internal Server Error.

Hub - A hub connects computers into a network via ethernet cables. It is not “smart” in the sense of distinguishing devices. So any information sent through a hub is broadcasted to all other MAC addresses on the network.

Switch - Similar to a HUB except it can distinguish devices so only the intended devices receive the broadcast.

Router- Routes data from one network to another via IP addresses. It connects the network to the rest of the public internet via IP addresses. Anywhere two or more parts of the internet intersect, there is a router. HUBs and Switches create networks, while routers connect networks. No need to have a switch if your router has a switch built into it. Routers also send out connection via radio waves (wifi).

Modem - Brings the Internet into your home. Demodulates the analog signals of the web into digital for the computer to understand. It also modulates the digital signals of the computer into analog to send out to the web. That’s why it’s called a modulator/demodulator = modem. If you only have one computer, you could just plug in the ethernet cable directly into the modem, but if you have multiple devices, you'd need a router. No need to have a router if your modem already has a router built into it.

Antenna - From the Latin for pole? An antenna takes in electrical impulses and spits out radio waves.

Text Messages - Essentially when you click send on a text, your phone sends commands through the processors to the circuit board which then sends the appropriate electric commands to the antenna. To create radio waves you need to make fluctuations in the electromagnetic field in the range of 30 Hz to 300 GHz. To create those fluctuations you need electrons moving around in a conductor. The antenna broadcasts your (encrypted) message to the radio tower of your service provider. Then that tower uses high speed cables to send your message to the appropriate tower at a point around the world. That tower then broadcasts your message as radio waves to the receiving telephone, which translates it back into message format.

Phone calls - Essentially, your voice is translated into 0s and 1s and then sent out as electromagnetic waves via the antenna to the tower which then sends it via cables to the appropriate tower and is then broadcast cak out to the receiver as electromagnetic waves, and reverse translated on the receiving phone. Your service, in both calls and messages can depend on how difficult it is for your waves to get to the tower. You can't just send the waves directly to the other phone because electromagnetic waves can't travel that far or something like that, also because the Earth curves away from you, so.

SIM Card - from my understanding, the primary utility of these is just to help the cell tower know which other cell tower to send the message to. And to store your actual phone number.

Wifi - A wireless network uses radio waves, just like cell phones, televisions and radios do. In fact, communication across a wireless network is a lot like two-way radio communication. Here's what happens: 1. A computer's wireless adapter translates data into a radio signal and transmits it using an antenna. 2. A wireless router receives the signal and decodes it. The router sends the information to the Internet using a physical, wired Ethernet connection. The process also works in reverse, with the router receiving information from the Internet, translating it into a radio signal and sending it to the computer's wireless adapter.

IDE - Integrated Development Environment. Essentially it's a text editor, debugger, and compiler all in one. It makes writing code easier. Sublime is a text editor, but you can't actually compile the code in it, you have to use the command line via terminal.

MAC Address - Every node on a network has a MAC address. These are hardware addresses, and different from IP addresses.

Cloud - The term can actually refer to several different types of cloud services, including software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS). Microsoft's Office 365 is one of the best examples of SaaS, while PaaS includes things like

Google's App Engine tools, which allow developers to build their own products and services. Meanwhile, IaaS involves things like networking features, virtual machines, and actual data storage -- which Amazon, Microsoft, and Google all offer.

SaaS - Essentially another name for apps that run in the cloud. You can access all these apps through a web browser, and all your data is stored on other companies' servers. Google Docs, etc.

IaaS - Infrastructure as a service. AWS, Azure, Google Cloud, etc.

PaaS - Platform as a service. Somewhere in-between the above two. Heroku, etc.

Using the restaurant analogy, Saas is you ordering your food from a restaurant. Iaas is renting out a kitchen so that you can cook your own food. Paas is you bringing your own ingredients but letting the restaurant cook them for you.

AWS is Iaas. It's a tool that lets you rent space on Amazon's servers, making it much faster, cheaper, and easier to launch an app than if you had to set up your own servers.

P2P - "Peer to Peer." In a P2P network, the "peers" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client. SKype was P2P for a while but has recently started moving to the classic client-server model. So essentially, SKype was decentralized, and is now centralizing. This is because P2P led to some inefficiencies in terms of battery life, data, etc. Once you’re in a network via P2P software you can browse the files in a “shared” folder from the other computer. This is how LimeWire & Napster used to help you get copyrighted music downloads from other computers. They were both PTP based systems.

Tor - The Onion Router. This is a specialized encrypting and anonymizing software. Tor wraps your communication in several layers of encryption and bounces it around many intermediary “relay” computers, each of which only knows the previous and next computers in the chain. So it’s nearly impossible to trace communication over it. Your IP is effectively hidden. The physical location of the servers also is not known because we don’t know their IPs. There are other such softwares, Tor is just the most popular. Now when you use Tor, your wifi provider/ISP will know that you are using Tor but not what exactly you are doing on Tor. Also there will be metadata that can be collected such as bandwidth, time of access, size of traffic (Mbs), etc. In other words, using Tor protects you from content inspection by the Wifi provider. However, it does NOT protect you from traffic correlation attacks (e.g. the Wifi provider can usually find out that you're using Tor and they’ll know at exactly what times you use Tor and how much data you exchange with the network - this is important information to have if they can also observe the target you visit over Tor - in that case, they'll be able to prove that you're communicating, even if they doesn't know the content of the communication). Using a bridge can help with hiding Tor from your Wifi provider, but correlation attacks are still possible even when you connect over bridge.

.onion - the domain of sites on the dark web. They reject any visitor that isn't using Tor.

Deep web - Everything on the internet that can't be accessed via the Google Search bar. Every page that isn't indexed by search engines.

Dark web - Subset of the deep web that you can't access without specialized software that encrypts all communications and anonymizes your IP address, like Tor. All of the .onion domains.

Silk Road - An illegal marketplace that used to be pretty big on the dark web. Basically Amazon. You paid via Bitcoin, which was stored in a central repository. Eventually the silk road was busted. Now, the marketplaces exist but transactions are decentralized and payment is handled by third-party services. OpenBazaar is a good example of this.

HTTPS - This is essentially the same thing as HTTP, except HTTPS protocols use an SSL (secure sockets layer) certificate, which helps create a secure encrypted connection between the server and the browser, thereby protecting potentially sensitive information, like bank usernames and passwords, from being stolen as its transferred between the server and the browser.

Robots.txt - The robots.txt file, also known as the robots exclusion protocol or standard, is a text file that tells web robots (most often search engines) which pages on your site to crawl.
It also tells web robots which pages not to crawl. Let's say a search engine is about to visit a site. Before it visits the target page, it will check the robots.txt for instructions.

Web Crawler - sometimes called a spider or spiderbot and often shortened to crawler, is an Internet bot that systematically browses the World Wide Web, typically for the purpose of Web indexing (web spidering). Web search engines and some other sites use Web crawling or spidering software to update their web content or indices of others sites' web content. Web crawlers copy pages for processing by a search engine which indexes the downloaded pages so users can search more efficiently. Including a robots.txt file can request bots to index only parts of a website, or nothing at all.

AMP - Accelerated Mobile Pages. AMP was created by Google as a way to load content onto mobile devices at a much faster rate. At its core, AMP is kind of like a stripped down HTML. AMP content features prominently on Google's Search Engine Results Pages (SERPs) to create a better mobile experience for smartphone and tablet users

Torrent - A torrent file is a computer file that contains metadata about files and folders to be distributed, and usually also a list of the network locations of trackers, which are computers that help participants in the system find each other and form efficient distribution groups called swarms. A torrent file does not contain the content to be distributed; it only contains information about those files, such as their names, sizes, folder structure, and cryptographic hash values for verifying file integrity. In a nutshell, a torrent file is like an index, which facilitates the efficient lookup of information (but doesn't contain the information itself) and the address of available worldwide computers which upload the content. Torrent files themselves and the method of using torrent files have been created to ease the load on servers. With help of torrents, one can download files from other computers which have the file or even a fraction of the file. These "peers" allow downloading of the file in addition to, or in place of, the primary server.

PirateBay - A torrent indexer, which means that it's a central hub for all file transfers that Pirate Bay users share. However, no files are actually stored on Pirate Bay servers. The Pirate Bay is one of the most popular sites on the Web for torrent peer-to-peer (P2P) file sharing.

Torrent client - a program that manages the download through the BitTorrent protocol.

Public-key cryptography - A cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. The generation of such keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security. In such a system, any person can encrypt a message using the receiver's public key, but that encrypted message can only be decrypted with the receiver's private key. What'sApp uses this and thus has end-to-end encryption.

Proxy - A proxy server is a server that acts as a middleman in the flow of your internet traffic, so that your internet activities appear to come from somewhere else. Proxies are great for low-stakes tasks like watching region-restricted YouTube videos, bypassing simple content filters, or bypassing IP-based restrictions on services. However, they only hide your IP, they don't encrypt your traffic. Anyone with access to the stream of data (your ISP, your government, a guy sniffing the Wi-Fi traffic at the airport, etc.) can snoop on your traffic. Note: When a web site does use HTTPS, an ISP cannot see URLs and content in unencrypted form. However, ISPs can still almost always see the domain names that their subscribers visit. DNS queries are almost never encrypted. Further, certain exploits, like malicious Flash or JavaScript elements in your web browser, can reveal your true identity. This makes proxy servers unsuitable for serious tasks like preventing the operator of a malicious Wi-FI hotspot from stealing your data. Finally, proxy server connections are configured on an application-by-application basis, not computer-wide. You don't configure your entire computer to connect to the proxy–you configure your web browser, your BitTorrent client, or other proxy-compatible application. If you're using an HTTP proxy to connect to any sort of sensitive service, like your email or bank, it is critical you use a browser with SSL enabled, and connect to a web site that supports SSL encryption. As we noted above, proxies do not encrypt any traffic, so the only encryption you get when using them is the encryption you provide yourself.

SSLStrip - A tool that lets routers trick computers into talking with a server over HTTP instead of HTTPS. If you log in to an account over that connection then a malicious hacker could theoretically intercept your information via his/her router because your connection is no longer encrypted. When browsers detect an SSLStrip attack, they cross out the https:// with a bright red slash.

Man-in-the-middle attack - When someone uses an SSLStrip to do the above. They could use your information to impersonate you on social media, e-commerce, emails, etc. These attacks occur because of the innate insecurity of public wifi networks.

VPN - Virtual Private Network. They effectively let you turn a public wifi network into a private one. It's sort of like end-to-end encryption between you and the websites you're visiting, so your router can't harm you. Virtual Private Networks, like proxies, make your traffic appear as if it comes from a remote IP address. But that's where the similarities end. VPNs are set up at the operating system level, and the VPN connection captures the entire network connection of the device it is configured on. This means that unlike a proxy server, which simply acts as a man-in-the-middle server for a single application (like your web browser or BitTorrent client), VPNs will capture the traffic of every single application on your computer, from your web browser to your online games to even Windows Update running in the background. Furthermore, this entire process is all passed through a heavily encrypted tunnel between your computer and the remote network. This makes a VPN connection the most ideal solution for any sort of high-stakes network use where privacy or security is a concern. With a VPN, neither your ISP nor any other snooping parties can access the transmission between your computer and the VPN server. If you were traveling in a foreign country, for example, and you were worried about logging into your financial websites, email, or even connecting safely to your home network from afar, you could easily configure your laptop to use a VPN.

Bit - Each 1 or 0 is a bit.
Byte - 8 Bits
Kilobyte - 1,000 Bytes
Megabyte - 1,000,000 Bytes
Gigabyte - 1,000,000,000 Bytes
Terabyte - 1,000,000,000,000 Bytes
Petabyte - 1 Quadrillion bytes
Exabyte - 1 Quintillion bytes

CPU - Central Processing Unit. A small square chip, made up of smaller sections called cores. The more cores, the faster and more tasks a computer can do at once. It's tough to compare CPUs because there are so many factors that affect speed and power, but in general you can just use the serial numbers of the chips to compare. For example, the Intel i9 is more powerful than the Intel i7. Intel chips, also known as x86, have traditionally been more powerful than ARM, but used more battery. So ARM has traditionally been used in phones while Intel in computers. However, recently ARM has improved. In fact, Apple announced that all Macbooks would switch from Intel chips to ARM in 2020.

Hard Drive - Permanent memory. Made up of a disk and an “Arm” that writes information to the disk. This is a moving parts item. Makes noise and can break over time.

Flash Memory - Permanent memory that uses the stationary, “fill in the cells” design opposed to the moving parts of the hard drive. Flash drives, SD cards, (cameras, phones, tablets), SSDs all use flash memory.

SSD - Solid State Drive. A special kind of flash memory designed for laptops. Beats the hard drive in almost every way except price per Byte. Though even that has converged to be almost identical over the years.

SD Card - memory for portable devices.

RAM - Random Access Memory. This is temporary memory storage, short term. Everything you are currently doing takes up some RAM. Each time you restart your computer you wipe your RAM. All apps and open tabs, etc. are using RAM, that’s why there aren’t any running apps on your phone or computer when you restart it. When you use all your RAM, then it’ll ask for some extra space from the SSD, but this slows things down as storage is slower than RAM. Big gaming computer have heavy RAM, but low battery life, where as a lot of servers have little RAM because they don’t really run apps or similar processes so they don’t really need it.

Port (Port 80) - a **port** is an endpoint of communication. Physical as well as wireless connections are terminated at ports of hardware devices. Ports are identified for each protocol and address combination by 16-bit unsigned numbers, commonly known as the **port number**. Inbound packets are received, and the port number in the header is used to decide which application is to be passed the packets. Port 80 is the port number assigned to commonly used internet communication protocol, Hypertext Transfer Protocol (HTTP). It is the port from which a computer sends and receives Web client-based communication and messages from a Web server and is used to send and receive HTML pages or data. Port 80 is one of the most commonly used port numbers in the Transmission Control Protocol (TCP) suite. Any Web/HTTP client, such as a Web browser, uses port 80 to send and receive requested Web pages from a HTTP server. It manages all HTTP-based requests that originate from a computer, regardless of the number of requests and initiating Web clients. Similarly, the HTTP server responds to all requests received at port 80. Alternatively, HTTP may use port 8080, rather than port 80, typically to deploy a caching or proxy server. Port 53 is DNS. Port 22 is SSH. Port 443 is HTTPS.

SSH - a cryptographic network protocol for operating network services securely over an unsecured network. Uses public key encryption. Typical applications include remote command-line login and remote command execution, but any network service can be secured with SSH. SSH provides a secure channel over an unsecured network in a client–server architecture, connecting an SSH client application with an SSH server. Windows 10 uses OpenSSH as its default SSH client. The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet, although files leaked by

Edward Snowden indicate that the National Security Agency can sometimes decrypt SSH, allowing them to read the contents of SSH sessions.

Why a Mac? - So it appears to be more of a preference thing. In terms of gaming Windows has the lead by a mile. Way more games are made for Windows and that culture has been established for a long time. Macs are in general more expensive than windows. Macs are more of a status symbol though. Macs also generally don't have the GPU capabilities that PCs do. But again, all of this can change if you just change out the parts of the computer. Like you could get a more powerful GPU or CPU, etc. A computer ultimately is just a collection of parts, and at this point the biggest difference seems to be that Macs use Mac OS and PC uses Windows or Linux. https://www.digitaltrends.com/computing/how-much-mac-pro-cost-as-pc/
However Mac OS is based off Unix, which means that the terminal prompt is very Unix like and there's only one. Whereas for PC, you have to use the command prompt, or the newer PowerShell, or the windows subsystem for Linux, or any sort of attempt to recreate the Linux Bash Shell on Windows 10 etc., which are sometimes decent, but again, you might need to update this software in the future and it just isn't native to the system. You could run a virtual machine but that drains battery. So for software engineering, in general, use Mac, and get used to using terminal. Also you can only really develop for iOS on Macs, if that matters to you.

Localhost - This lets you essentially use your computer as a server, a virtual server. Usually your local host IP address is 127.0.0.1 but this varies. Using this address will trigger a loopback which is what creates the simulated server. Using your machine as a server will enable you to test out some stuff on your own computer. In other words, you can pretend to be connecting to a Web server or another host computer, but you're keeping it in-house and close to home by using localhost.

Environment - a sandbox of various language and package configurations such that none of the packages clash with each other's various versions. Because many packages are dependent on one another.

Magic Commands - can be used within Jupyter Notebooks to communicate with your operating system. They start with '%'.

Numpy - gains a lot of its efficiency from being typed. That is, all elements in the array have the same type, such as integer or floating point. The default type is a float. (Each float uses either 32 or 64 bits of memory, depending on if the code is running a 32-bit or 64-bit machine, respectively).

Terminal

- So if you learn MacOS terminal, you're also learning by extension UNIX, and further LINUX, for the most part. It's the central hub for programming on a Mac.
- It's a command line environment
- Pwd -> gives you the current working directory
- Ls -> lists out everything in the current working directory

- Cd -> change directory
    - cd ~ -> changes directory back to home directory
    - Cd .. -> goes back one folder
    - cd . -> takes you to your current directory, os doesn’t really do anything
- Mkdir -> make directory
- Cp file1 file2 -> this makes a copy of file1 and stores it as a file named file2, within the same directory
    - cp -r directory1 directory2 -> copies directory1 and every file inside and moves it to directory2, within the same directory
- Mv file2 ~ -> move command. Moves file2 to the home directory
    - Can also be used to rename a file:
        - mv file2 file3 -> essentially renames file2 as file 3, within the same directory
- rm -> deletes a file
    - rm -r directory1 -> removes the directory1 and everything inside directory1

1. So you type out a program in c in Xcode.
2. You save it as a .c file in some directory.
3. Then you use the cc command in the terminal to compile it
4. Then it ends up as an a.out file in that directory.
5. Then you can execute that program by doing ./a.out
6. You can also rename the program using the methods already discussed
7. a.out is the compiled output of your C compiler. You can name the file whatever you want by using the -o flag. This is an executable file.
8. When you type a command such as ls or mv the terminal searches for files with these names in directories listed in PATH environment variable. To see the list of these directories, type echo$PATH
9. If you type a.out the file will be searched in these directories where it will not be found. dot (.) refers to the current directory.
10. ./a.out tells the terminal to execute the file named a.out in the directory (.) ie current directory

Further Terms

- Broadband services vs 4G vs mobile services
    - really just telephone providers vs ISPs
    - ISPs: Comcast, AT&T, Verizon, CenturyLink, Cox, Spectrum
    - Telephone companies: Verizon, AT&T, Sprint, T-mobile
- kernel
- Quantum Computing: https://www.wsj.com/articles/the-race-to-save-encryption-11559646737?mod=djemTECH
- What's a MAC Address?
- https://en.wikipedia.org/wiki/Port_(computer_networking)
- https://en.wikipedia.org/wiki/Embedded_system
- https://whatis.techtarget.com/definition/Apache

- WPA2
- 802.11
- Touchscreens
- Bandwidth
- Latency
- Malicious Flash or JavaScript elements
- NFC

Chrome Keyboard Shortcuts

Open a new tab	Command and T
Close the current tab	Command and W
Reopen last tab closed	Command and Shift, then T
View next tab	Command and Option, then ->
View previous tab	Command and Option, then <-
Jump to a specific tab	Command and select the appropriate number
Open a hyperlink in a new tab	Command and click the link
Open a link in a new window	Shift and click the link
Put a cursor in the search bar	Command and L
Erase the current search	Command and delete
Highlight the next word in search	Shift and Option, then ->
Highlight the last word in a search	Shift and Option, then <-
Go back to the previous page	delete
Go forward to the next page	Shift and delete
Reload the current page	Command and R
Open the find bar	Command and F
Scroll to the next keywords in find bar	Enter
Scroll to previous keywords in the find bar	Shift and Enter
Save the current page as a bookmark	Command and D
Open the settings page	Command and the Comma key
Open the downloads page	Command and Shift, then J
Open a new window	Command and N
Scroll down the web page	Tap the Space Bar