Network+

# How To Use This Study Guide

First, let’s be clear about what this study guide is NOT. It is NOT comprehensive, and it is NOT intended to be enough for you to study off exclusively. There are probably whole sections I skipped or glossed over, mostly because I thought they were too obvious to need written down.

**This guide is brief on purpose**. This guide is an excellent resource to review information, to be reminded of terms you’ve learned about but may have forgotten, and to understand how to mentally organize the information so you can recall it easier.

**This guide is thorough, but incomplete**. A lot of this material, especially the first few sections, is not heavily on the Network+ test, but exists to provide background to help you through technical questions commonly asked on interviews. I also took these notes using *multiple* resources. Unlike my [Security+ study guide](https://docs.google.com/document/d/1hXGyKDWdpJLKZWWuu5eVTh-N5simhpSlTTA-Z-dtCj0/edit?usp=sharing), which follows the Darril Gibson book closely, much of the research for these notes was done on my own while taking examcompass tests or reading through various guides. I do hope to clean it up at some point. The less relevant sections will be marked in red.

I really hope this guide helps you pass the test. I know not everyone likes to take notes while they read, but it helps me process information quickly, and it allows me to give back to the IT community in some small way.

If you really appreciate this study guide and found it useful, ***why not buy me a coffee?***

You can send a few dollars my way at [paypal.me/electricintheforest](http://paypal.me/electricintheforest) if you feel so inclined, and if you guys are generous enough, I’ll put that money to more certifications and keep building out study guides as I go.

Thanks for reading,

-Daniel Arsenault

**Please Upvote This Guide on Reddit for Visibility! And feel free to share!**

## A Note On This Uneditable Guide

There are two different versions of this guide. This version is my original unedited guide. You can trust that almost all of this information has been checked by me, and I’ll vouch for it. If you’d rather see a more complete guide, that allows the community to add notes and additions, [click here.](https://docs.google.com/document/d/19_ym7Q3eFi0IDOf-3WOG1fQ0HyDRS8pDQ28J1q35daI/edit?usp=sharing)

For Starters:

This information goes very in-depth on some topics that may or may not be featured on the net+. It is worth learning this material, but focus more of your time on the content lower in this guide.

# OSI Model - Open Systems Interconnection

7 Layers. Developed in the 80s to create a system wherein technology could communicate to each other. Each layer receives data communicates only with the layer above or below it.

When information is transmitted from one device to another, it is compiled on device 1 at the highest available layer, granted a header and footer, and then passed to the next layer. That layer repeats this process until the lowest layer is reached. Then, all that data is passed to device 2, which undoes that process according to the headers in footers, starting from the lowest layer, and proceeding to the highest.

**P**lease **D**o **N**ot **T**hrow **S**ausage **P**arties **A**lways!

1. Physical Layer
   1. M In TCP/IP, the unit here is bits.
   2. Actual physical connections
   3. The pins in your connection, the wires in your cables. How do the transmissions move physically in the world?
2. Data Link Layer
   1. In TCP/IP, the data link sends out “frames” after adding on a frame header and footer.
      1. A frame is the final layer of data encapsulation before data is transmitted.
      2. A frame has a header and footer. The header indicates that a frame is beginning, whereas the footer indicates that the frame is done.
      3. A receiver will ignore data until the frame begin sequence is received.
   2. Direct Node to node transmission. Point-to-point
   3. Ethernet. Once the router figures out the route, this layer handles the process of actually passing that data from each point to the next.
3. Network Layer
   1. In TCP/IP, the networking layer sends out packets. The header of the packet contains the IP address. This could be either IPv4 or IPv6 typically. Note that even if a network only supports IPv4, you can still send IPv6 packets through a process called [Tunneling](https://en.wikipedia.org/wiki/Tunneling_protocol).
   2. Many nodes connected to one medium. That medium makes decisions for how best to pass data between many nodes.
   3. Your Router. It takes the packets segmented by the transport layer and *routes* them
4. Transport Layer
   1. Segments data into packets, approves or denies packets passing through
   2. Forwards Port
   3. 5 classes of connection. Internet uses TP4
   4. This is the layer where TCP and UDP become important, because they each behave differently and have their own headers that they add on to data being sent out.
      1. TCP sends out “segments” and is used when precise, reliable communication is necessary. This means that no data is lost along the way and the protocol ensures lost packets are resent to the recipient.
      2. UDP sends out “datagrams” and is used when consistent, stable communication is necessary. This is typically used for games and teleconferencing where continuously receiving packets is more important than receiving *every* packet. If a packet comes through and its checksum declares that it is incomplete, it is simply tossed aside.
5. Session Layer
   1. Continuous data streams- strong open channels, clean session termination
   2. Like starting a Skype Call
6. Presentation Layer
   1. Encoding and data compression - HTML, CSS, etc. How does the raw data get communicated into a form that can be represented in an application
   2. Webpages from code
7. Application Layer
   1. Determines whether the high-level communication can happen at all. Assesses available network and hardware resources versus the communication requests.
   2. This layer interacts with a theoretical 8th layer, the user, and thus creates a UI that can be interacted with directly.
   3. HTTP, FTP, SMTP, DHCP, DNS

Additional Notes from a friend:

Here is a great illustration of how the layers speak to each other.

Let’s take the Transport layer for example.

Transport of Host A wishes to speak with Transport of Host B.

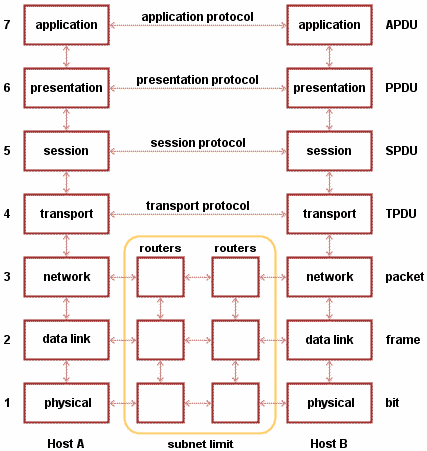
It sends the command down to Network of Host A to establish this connection.

Soon, Network of Host B gives Transport of Host B the connection info.

Transport of Host B approves the connection and starts to communicate with Transport of Host A.

However, this connection is an *ABSTRACTION* in that, even they are “talking”, they aren’t doing so directly. The CONCRETE communication is actually happening through the networking layer (and so on downwards to physical), but, in the eyes of the transport layer, it’s as if they are communicating directly.

Also I love how it shows the routers in the middle. This is exactly what happens when you send packets out; they are received by other routers and sent along to the next router.



# DNS - Domain Name System

### DNS Basics

* **The key functionality of DNS is to translate between human-friendly identifiers (URLs) and a computer-friendly registry (IP and port #) of where to best access a variety of resources.**
* DNS affects URLs (Uniform Resource Locator), E-mail addresses, IP addresses, and more.
* DNS can often be related to a phone book, wherein you look up something easy to remember to gain more specific information.
  + The chief difference in functionality between a phone book and DNS is that DNS will output the location of specific data based on proximal servers.
  + In other words, if I, in America, and someone in China both type in a URL, we may be given a different IP from which to pull the data we’re requesting, based on whichever server is closer to each of us that houses that data.
* Another key function of DNS is that, rather than creating one centralized database which can be difficult to change, DNS typically assigns a domain range to each ‘user.’
  + For instance, a household network with a single internet connection has a ‘range’ of IP addresses with which to connect to the internet. This means computers can switch their IPs based on the network administrators designations.
  + The DNS is broken into domains, and each domain has its own authority to assign addresses. Each domain can also be broken further into sub-domains.
* DNS is structured into authoritative zones, which can be further broken into smaller portions, and are typically represented within a URL and called by each zone’s label.
  + For instance, [www.example.com](http://www.example.com) gives us information about three zones.
  + The highest level domain is “com”.
  + The first subdomain is “example”
  + And the second subdomain is “www”
  + The ‘.’ indicates the distinction between multiple labels.
* Each top-level domain (‘com’ in the example) requires two servers to contain master lists of its NS data. This is to provide redundancy in case one server should fail or become inaccessible.
* ICANN delegates the management of all top-level domains.
* **FQDN - Fully Qualified Domain Name**
  + Two parts, hostname and domain name

### DNS Operation

* In order to resolve the real location of a DNS search, a recursive query system is setup wherein the requesting computer follows a trail of hints to find the authoritative location.
  + For instance, ‘.com’ will be queried first, and then further queries will be made from its recommendations, or ‘hints’ until the final solution is found.
  + However, because this is resource intensive en masse, cached name servers often retain relevant queries for set period of time, determined by the ‘time-to-live’ status of the original query.
* There are three main types of queries that can be made from the clients side
  + **Non-recursive queries** are requests made directly to authoritative servers.
  + **Recursive queries** are requests made to a server, which will then continue to query other servers until it can give an authoritative answer to the client.
  + **Iterant queries** are when the client side queries multiple servers to find the authoritative answer itself.
* Requests can sometimes become circular, when servers refer queries to a location that is also on an unknown server. In these cases, the querying server can look at the *glue*, or alternate server hint provided in the original query response.
* Because query records can be maintained for the duration of the TTL (time to live) set by the server administrator, DNS updates do not happen immediately, and can take up to several days if records are held for long periods of time.
* Servers and Host Names are not One-to-One

### DNS Messages

* Question
* Answer
* Authority
* Additional Space
* Header Section
  + Identification
  + Flags
    - Query/Response (0/1)
    - Reply/Status/Request (4 bit value of 1/2/0)
    - Authoritative? (0/1)
    - Client Request Recursion? (0/1)
    - Replying Server Support Recursion? (0/1)
  + Number Of Questions
  + Number of Answers
  + Number of Authority Resource Records (RR)
  + Number of Additional RR

Assorted info:

* DNS uses UDP 53 for URL queries
* DNS uses TCP 53 for zone transfers- when name servers exchange updated records
* DNS uses **BIND - Berkley Internet Name Domain** software on Unix/Linux servers

### Common DNS Record Types

https://en.wikipedia.org/wiki/List\_of\_DNS\_record\_types

|  |  |
| --- | --- |
| A | 32 bit IPv4 |
| AAAA | 128 bit IPv6 |
| CNAME | Canononical Name Record - Alias of one name to another (useful for making example.com and [www.example.com](http://www.example.com) go to the same place!)  Always points a domain name to another domain name!! |
| DNAME | Delegation Name Record - Alias of all sub-names OBSOLETE |
| IPSECKEY | Works with IPSec to provide security |
| MX | Mail Exchange Records - maps a domain to message transfer servers |

# TCP/IP Transmission Control Protocol/Internet Protocol

* Regulates end-to-end communication of how data should be packetized, addressed, transmitted, routed, and received.
* Fundamentals of networking
* Architecture designed around two principles.
  + End-to-End: For simplicity’s sake, the checks should be done by the sender and the receiver, not every piece in between. The endpoints are responsible for reliability.
  + Robustness Principle: Anything sent should be particular and well-formed, but a device should receive anything that is reasonably readable. The focus, then, is on smooth processes, not perfection.

### TCP/IP Layers

* Unlike OSI, TCP/IP utilizes layers, but not as strictly.
  + Application Layer
    - Creates and utilizes user data, and communicates that to other high-level applications, often through the transport layer’s “pipelines”.
    - HTTP, FTP (file transfer protocol), and SMTP (simple mail transfer protocol) - All ways that applications communicate with themselves and each other.
  + Transport Layer
    - Host-to-host communication, like local networks. Communicates on behalf of applications.
    - UDP is used for unreliable communications, whereas TCP is called for more reliable transmission, flow control, and connection establishment.
  + Internet Layer
    - Exchanges data across network boundaries (internetworking).
    - Responsible for IP address connections.
    - Transmits data to the next IP router closer to the final destination.
    - Defines the host addressing/identification and routing structures inherent in TCP/IP.
  + Link Layer
    - Communication without intervening routers (direct connection?)
    - Makes internet-layer datagrams transmissible to ‘next neighbor hosts’
    - Similar to Physical Layer in OSI! Deals with firmware, software chipsets, etc.

### TCP/IP Vs. OSI

* TCP/IP pre-exists OSI and is less robust, but has different goals.
  + TCP/IP is more flexible, allowing the transport layer to pick either UDP or TCP depending on how much reliability is required.
  + The goal, as shown in the key architectural principles, is ‘running code’ - rather than perfect, reliable transmission.
  + *Personal Note*: TCP/IP is like MP3 whereas OSI is like Raw. One gets the job done, one takes losses as unacceptable.
* Each layer in the TCP/IP tends to treat the other layers as black boxes. Application layer just deals with app data, and sends that to the transport layer to figure out how to actually get it moving. Similarly, routers and such do not evaluate the data they receive, they only care about transmitting it.
  + This can be seen like a post office- we write letters at the application layer, the transport layer is the post office concerned with reading the address and determining the destination/route.
  + The internet layer is where the post offices make sure the letter is at the nearest possible post office.
  + The link layer is the actual post man, getting it into the final destination.
* TCP/IP presumes no specific environment and can function as long as every client has the functionality to send and receive packets of data.

# DHCP - Dynamic Host Configuration Protocol

* Reduces the need for a Network Admin by dynamically assigning network configurations to hosts such as assigning IPs on IP networks
* Instead of configuring each device, admins configure the DHCP server, which queries every new connecting device and assigns several parameters such as…
  + Default Gateway
  + Domain Name
  + Name Servers
  + Time Servers
* These assignments last for a set duration according to the ‘lease’ set by the DHCP server’s settings, and can either be reassigned or altered at the end of the lease.
* A main DHCP server can communicate via relays (big router to repeaters) for the sake of long-distance assignments
* There are three methods of assignment
  + Dynamic allocation - the DHCP server uses the lease system to assign each new device an IP within a set range for a set period of time
  + Automatic Allocation - Similar to dynamic, each device is given an IP, however a table is reserved so that devices can receive the same IP upon reconnection
  + Static Allocation - an IP is assigned manually and specifically to the MAC Address of each connecting device semi-permanently. This is pre-configured.
* DHCP utilizes two UDP ports
* Acts in 4 stages according to DORA -
  + **Discovery** - The client queries the server at address 255.255.255.255 with DHCPDISCOVER
  + **Offer** - The server responds with DHCPOFFER which includes the clients MAC address, offered IP, subnet mask, lease duration, and the IP of the server making the offer
    - The server makes an offer based on the CHADDR (clients hardware address) and responds with YIADDR (Your IP address)
  + **Request** - If a client received offers from multiple servers, it will select an offer and request that IP with DHCPREQUEST. It will also alert the other servers of which offer it accepted. The other servers will terminate their offers.
  + **Acknowledgment** - Once the server receives DHCPREQUEST it will respond with DHCPACK. Once the client receives that packet of data, it will probe the new IP to ensure there are no conflicts.
* *DHCP Inform* can be used if the client wants additional DHCP information after DORA.
* *DHCP Release* can be used optionally to return and terminate an IP address. This is not mandatory.
* Clients can choose optional setting available through DHCP and BOOTP PARAMETERS.
* Reliability of DHCP protocols is ensured through the process of renewing leases that may end.
  + Clients periodically send DHCPREQUEST through unicast (the direct connection made post IP assignment). If that fails, it is presumed the server is down.
  + DHCPREQUEST will periodically be resent to see if the server has come back online.
  + If the server remains down, DHCPREQUEST will be broadcast in the hopes that another server can renew the IP lease.
  + If no renewal is possible, DHCPDISCOVER will be broadcast so that a new IP address can be assigned.

# Linux Boot Processes

This is definitely /not/ on Net+. But employers often ask these questions anyway.

I also highly recommend you play Terminus, a Linux learning game that’ll teach you the basics if you don’t already know them.

<http://web.mit.edu/mprat/Public/web/Terminus/Web/main.html>

1. BIOS (Basic input/output system)
   1. Performs basic checks on essential hardware
   2. Checks for bootloader program in all drives (hard and disc)
   3. Executes and gives control to the MBR bootloader
2. MBR Bootloader
   1. Runs the Master Boot Record to determine default boot options - found in the first sector of the bootable disc
   2. MBR has three partitions
      1. Primary Bootloader Info
      2. Partition Table Info
      3. MBR validation
   3. Possible to change boot priority during this stage
   4. Executes GRUB
3. GRUB - GRand Unified Bootloader
   1. Contains Kernel images and allows their selection
   2. Executes Kernel
4. Kernel
   1. Handles all O/S processes such as memory management, I/O, task scheduling, and interprocess communication.
   2. Initially mounts initrd (Initial RAM Disk) as the original root file system in order to access essential drivers for hardware and hard drive partitions
   3. Then boots the full kernel and mounts the real file system according to GRUB settings
   4. Simplified Process
      1. Configures hardware, I/O, and memory
      2. Identifies and uses initrd to decompress and mount drivers into memory
      3. Configures virtual devices such as RAID and LVM
      4. Unmounts initrd
      5. Mounts the root file system and frees up unused memory
      6. Fully initializes kernel, which runs idle until called
   5. Executes Init, and then goes idle until called by a process
5. Init
   1. First Process PID=1
   2. Runs and terminates every other process
   3. Creates User space
   4. First sets up a Daemon to create the GUI
   5. Init initializes with a runlevel parameter which determines what processes it starts up
   6. Init goes idle once it has started all necessary processes until a process needs to be terminated, or init is called directly.
   7. Default Init is limited in that it runs processes serially, rather than in parallel, potentially slowing boot significantly on I/O processes

### Additional Linux Boot Processes (Alternatives to sysvInit)

* Systemd
  + Made to replace init - also a daemon that calls other daemons
    - Commonly used in place of init on modern pcs
  + Made to run more processes in parallel than init
  + Calls to a configuration file rather than a shell script
* Upstart
  + Serial processes as well
  + Not that good.
  + High compatibility?
* Runit
  + Very fast init, basically

# RAID - Redundant Array of Independent Disks

### General Raid Knowledge

* Raid is a configuration of multiple hard-drives to increase performance and/or redundancy for data
* Redundancy is checked via **parity**, and corrected via **XOR**
  + Parity checks the data for accuracy and responds with an error
  + XOR identifies which of the two competing data streams is accurate, and returns the accurate data set
* **Hybrid RAID** can utilize the power of a few fast SSDs to boost the reliability and performance of a mostly mechanical hard-drive system given the appropriate controller.
* **Striping** is when data is split among several storage volumes so that data (I/O demands) can be retrieved in parallel. Important when data needs to be retrieved quickly.
* **Nested RAID** is when multiple RAID levels are nested through groups of hard drives (a set of 2 RAID 1 mirrored drives are then striped by RAID 0 across another set of RAID 1 mirrored drives)
* <https://raid.wiki.kernel.org/index.php/RAID_setup>

### Important RAID Styles

* RAID 0
  + Provides no redundancy, only performance benefits of Striping
  + Total usable volume is the cumulation of every drive in the RAID
  + Highly vulnerable to drive failures, moreso even than a single large volume
* RAID 1
  + Basic data redundancy, without parity.
  + Read speeds are normally slower than that of the fastest drive, though theoretically the system supports speeds as fast as RAID 0
  + Write speeds are limited to the slowest drive
* RAID 5
  + Block level striping, with distributed parity.
    - Data is maintained as long as n-1 drives remain.
  + Requires a minimum of three drives
  + High speed, and decent data redundancy make this practical, however, when one drive goes bad, the system must rebuild the array (check for and redistribute parity) and because speeds are so slow, the time it takes to do this can often crash a second drive, wrecking the system.
* RAID (0+1)
  + A **nested RAID**
  + Striped drives, that are also mirrored (S1+S2)+(S1+S2)
  + Provides speed improvements from the striping, and redundancy/parity from the mirroring
  + Disadvantaged against RAID 10 due to the long rebuild process if even a single drive goes bad
  + If one drive goes bad, such as M1, its complementary drive is also useless, leaving you essentially with a RAID 0 and no redundancy.
* RAID 10 (1+0)
  + The preferred RAID setup for data-intensive systems.
  + Creates a stripe across two pairs of mirrored drives
  + Performance second only to RAID 0, with redundancy and parity
  + As long as one drive from each mirror is still functioning, data retains integrity
* RAID 50 (5+0)
  + Distributed parity and striping, which is then also striped.
  + Volume equal to 2/3rds the total capacity of all involved drives
  + High performance, fairly redundant
  + Same, and possibly increased, limitations as RAID 5, wherein the rebuild process can put significant strain on the system during drive failure
  + Requires “hot swapped” drives in case of any failure
  + Can handle a failure of a single drive in each set of RAID 5
  + Requires a minimum of six drives

# Cabling

## Misc Cabling

* **RJ Connectors- Registered Jack**
  + Always **copper cabling**
  + Common Configurations - https://en.wikipedia.org/wiki/Registered\_jack#Registered\_jack\_types
    - RJ11
      * Two-wire POTS connection
    - RJ14
      * 4-wire, two line POTS connection
    - RJ25
      * 6-wire, three line POTS connection
    - RJ45
      * 8P8C connector
      * Data Line Connection
      * Primarily Used for Ethernet!
    - RJ48
      * Terminates a T1 connection
* **RS-232**
  + **Serial** transmission of data
  + Old-school Serial Cables!
  + Used to connect reliable PSUs, monitors, mice, etc
  + Low speed, wide voltage swing, pretty shitty tech
  + Common connectors include **DB-25** (25 pin connection!) DB-9 and DE-9
* **Coaxial Cable**
  + **Shielded** cable line
  + RG cables are common standards
    - RG-6 Used in most cable TV and satellite
    - RG-59 Baseband cable used in closed-circuit tv
      * HD over short distances
  + Utilize RF connectors
    - F connector for most cable TV and satellite
    - N connector to couple coaxial cables
    - BNC Connector - Quick Release, Military and industrial usage
      * Composite signals
* **RCA Connector**
  + Your red/white/yellow (and various other color cables)
    - Need a separate cable for each signal, typically color coded
    - Has a serious flaw in that when making the connection, the hot part of the connector makes contact before the ground, causing static
* Distinguishing **UTP** and **STP** Cables
  + Both are **Twisted Pair** Cables
  + UTP is unshielded
    - In non-industrial setting, the twisted wires themselves are enough to prevent interference
    - Doesn’t require a solid ground
    - Cheaper
  + STP is shielded
    - Much larger cables- more difficult to install
    - If improperly grounded, the shielding can actually cause MORE interference
    - More expensive, and require maintenance if ground or shielding is damaged
* **Ethernet Cable**
  + Typically uses RJ45
  + Copper cable
  + 5, 5e (1000Mbps), 6, and 6a(10,000Mbps) cables are common for internet usage
  + Utilized twisted wires to prevent signal interference
  + Standard 100 meter range
  + Modern cables can hit 100Gbit/s (Cat 7), with proposed cables up to 400 Gbit/s
  + Cat 3 still exists, but is 10Mbps, typically used in telephony
  + Two standards exist for wiring RJ45 Ethernet Connections: T568A or T568B
  + **Crossover Cabling**
    - Requires T568A on one side, T568B on the other
    - Connects two similar devices (two computers, two routers)
  + **Patch Cable/Straight Through Cable**
    - It doesn’t matter which standard is used, as long as both sides of the cable match
    - Connects two different kinds of devices
  + **Rollover Cable**
    - Attaches a computer terminal to router’s console port
    - Not for networking
  + **Auto MDIX (Medium-dependant interface)**
    - Allows two devices connected by ethernet to auto-negotiate maximum speeds and duplex capacities
    - Removes the need for crossover cables!
* **GBIC and SFP (gigabit interface converter and small form factor pluggable)** 
  + Big and small versions of a device that convert from electrical to optical
* **Baseband**
  + Digital signaling, bi-directional transmission
  + One channel for both directions of signal!
  + IEE 802.3 - ethernet
  + Very narrow frequency range
* **Broadband**
  + Analog signalling, unidirectional transmission
  + For transmission to be both ways, requires two channels
  + High frequency range

## Single Mode vs. Multimode Fiber

* Fiber cables function through “total internal reflection” wherein light bounces at such an angle that there is no dispersion or refraction.
  + This is one of the chief differences between the fibers- because single mode only allows a very specific frequency to run through it, the integrity of that frequency can be better maintained.
* Modern fiber cables require a repeater every 43-93 miles due to its low **attenuation** (reduction in signal over distance) - losing as little as 3% of its signal strength over 100 meters
* Fiber is more durable, more energy efficient, faster, and more reliable than copper.
  + Highest rates in a single channel are around 111Gbits/s, though 40Gbits/s is more common.
  + The highest rate on a single core is 101Tbits/s
  + The highest rate on a multicore fiber is 1.05 petabits/s
* The **index of refraction** is used to quantify the speed of light in a material, and it is calculated simply by dividing the speed of light in a vacuum by the speed of light in that material
  + A good, single-core fiber has an index of 1.444

### Single Mode SMF

* 1310 and 1550 nm wavelengths
* Single mode only allows a very specific frequency to run through it, the integrity of that frequency can be better maintained.
* **Single Mode Fiber uses a very small core**, less than 10 times the wavelength, usually 8-10 micrometers, compared to MMF’s 50-several 100 micrometers.
* 10Gbits/s over 80 km (50 mi)

### Multimode MMF

* 850 and 1300 nm wavelengths
* Larger core to support multiple transverse modes.
* Greater wavelength acceptance makes for easier connections
* Inferior over long distances to SMF
* Speeds
  + 100 Mbits/s over 2 km
  + 1Gbit/s over 1km
  + 10Gbit/s over 550m

### Fiber Tech Standards

* **SONET - Synchronous Optical Network** 
  + **SDH - Synchronous Digital Hierarchy**
  + Transport protocol to replace **PDH**
  + Allows the synchronized data transfer of multiple digital bit streams over fiber using lasers
  + Transports in STM-1 units, STS3c, and OC3 units
  + Unlike how other files at this layer send - frame first, then payload- this transfer uses “overhead” instead of “headers” and sends the overhead mixed into the data stream
  + **SONET OC rates :** <https://en.wikipedia.org/wiki/Optical_Carrier_transmission_rates>
  + Typically Based on Dual Ring Topology!
* **CWDM - Coarse Wavelength Division Multiplexing**
  + Less than 8 wavelengths per fiber
  + Compact, cost effective, and shorter range than DWDM
* **DWDM - Dense Wavelength Division Multiplexing** 
  + More than 8 wavelengths per fiber

### Fiber Connectors and Cabling

* **ST**
  + Most common connector, spring loaded
* **SC**
  + Snap-in connector
  + A little more expensive than ST, but high performance and growing in popularit
* **LC**
  + Screws on, looks like ST
* **FC**
  + High-performance, small form factor
  + Favored for Single Mode fiber
* **MT-RJ**
  + I don’t know, just know it.
* Other Single Mode Connectors (control the light signal)
  + **APC - Angled Physical Contact**
  + **UPC - Ultra Physical Contact**

# PC Boot Requirements

* Motherboard
  + Hosts the BIOS
  + Hosts the Bootloader
* Power Supply
* RAM
  + Necessary for Kernel and init daemons to be mounted
* CPU
  + Does the work

# 

# Networking+ Cert Study Guides Part 2

See : <http://www.proprofs.com/mwiki/index.php?title=Comptia_Network%2B_Study_Guide>

## Equipment

* **Hub -** Shouts data to every node connected
* **Switch** - Directs data directly to specific recipients
* **Bridge -** Connects two parts of intranet
* **Router**
* **Gateway -** Communicates between devices using different protocols
* **WAP -** Wireless Access Point
* **-** Network Interface Card
* **CSU/DSU**: A CSU/DSU (Channel Service Unit/Data Service Unit)
  + Converts a signal from one form to another
  + Most commonly in cable modems
* Modems
  + Convert physical analog signal to digital signal
* Proxy Servers
  + Basically propaganda- filters data and only communicates what it wants to

## Firewalls

* Packet Filtering
  + Operate at the network level- check the headers and footers (destination) of packets and filter based on that.
* Circuit Level Filtering
  + Operates on the session layer
  + filters based on the presence of a TCP handshake
  + Needs a secure connection
* Application Level Filtering
  + Works on the application layer, obviously, and looks at the actual content of packets.
* Stateful Inspection
  + Most commonly used
  + Operates at both the Network and Application Level
  + Requires a secure connection via TCP
  + Inspects the actual contents of packets
  + Basically Application + Circuit Level

## Frame Types and Ethernet

* Frame Technology in general is how physical connections get interpreted into the higher level data packets in networks
* **802.4 Token Bus Topology Standard**
  + The original networking model, of all computers daisy chained together
  + Data got passed like a “token” between each and every node.
    - This meant no privacy, and massive amounts of traffic
    - Bus standards also required a terminator to “End” traffic
* **802.5 Token Ring Topology Standard**
  + Removed ‘terminators’ but still sucked. Also didn’t really remove terminators, just made them less essential.
  + Competed with ethernet, clearly lost
* **Dual Ring Topology**
  + Used in Fiber **SONET**
  + Two rings running opposite, operate independently
  + Provide redundancy
* **Hybrid Network Topology**
  + Combines two or more DIFFERENT topologies
  + <http://www.conceptdraw.com/How-To-Guide/hybrid-network-topology>
  + Redundant, flexible, etc
  + Expensive and difficult to manage
* **802.3 Ethernet**, traffic is not passed on a token, but allowed to be sent haphazardly on its own
  + Ethernet, Frame Type 802.3, is key to networking.
  + Operates on the Data Link Level
  + **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection
    - Crazy acronym
    - Step 1: See if the line is open and frame is ready to send
    - Step 2: Send frame
    - Step 3: Run collision detection if collision occurs
  + Since ethernet didn’t prevent collision, people worried it was inefficient and slow.
    - It isn’t.
  + Ethernet can Auto-Negotiate network speed and “duplex mode”
    - One-way, or two way communication
    - Whether the node listens, talks, or both
  + **POE - Power over Ethernet**
    - **802.3af -** 15.4 watts over a Cat 5 or better cable
    - **802.3at or POE+** - 25.5 watts over a Cat 5 or better cable
* **MTU - Maximum Transmission Unit**
  + Largest payload size able to be transmitted in a single frame
  + **For ethernet, this is 1500 bytes (or octets)!**
  + Much of the internet actually uses a standard of 576
  + Minimum value is 68
  + **Jumbo Frames**
    - Can get as large as 9000 bytes
    - Local area only
    - Good for SAN (storage area networks)

### Ethernet Media Table

|  |  |  |  |
| --- | --- | --- | --- |
| Name/Max Cable Length | Type | Speed | Use |
| 10Base5 / 500 m. | Special coaxial cable, needs “vampire taps” (cut into wire to read), SHARED MEDIUM (similar to bus) | 10 Mbps | Oldest technology and media; rarely employed today |
| 10Base2 (“ThinNet”) / 185 m. | Coaxial cable with BNC connector. SHARED MEDIUM | 10 Mbps | Also old and rarely used, remember that it requires special circular BNC connector, similar to “cable TV connector” |
| 10BaseT / 100 m. | Twisted Pair wire with EXCLUSIVE MEDIA (connected to hubs rather than to other nodes), RJ-45 | 10 Mbps | Used RJ-45 connectors (look like large phone line connector) |
| 100BaseTX (“Fast Ethernet”) / 100 m. | Twisted pair wire, EXCLUSIVE MEDIA, RJ-45 | 100 Mbps | An improvement on speed of 10BaseT, capable of auto-negotiation of speed |
| 1000BaseT (“Gigabit Ethernet”) / 100 m. | Twisted pair wire, EXCLUSIVE MEDIA, RJ-45, uses two pairs of wires for transmission | 1000 Mbps | Another speed improvement  100 meter range |
| Faster Speed/Other media Ethernet (10GBASE-SR, 10GBASE-CX4, etc) / 2000+ m. | Uses next-generation fiber optic cabling to achieve 10+ Gbps speeds | 10+ Gbps | Another speed improvement and change in connectors, cabling |
| 100BaseFX | 2 kilometer length, full duplex multimode, fiber |  |  |
| 1000BaseTX | Cat6, two pairs of wire, 100 meter range, | 1Gbps |  |
| 10GBaseSR | Multimode fiber, 400 meters, |  |  |
| 10GBaseER | Single mode fiber, 40 kilometers |  |  |
| 10GBaseSW | Multimode, SONET, 300 meters |  |  |

* Tips for the table!
  + Base refers to “baseband”
  + BaseT = Twisted Pair
  + BaseF = Fiber
  + BaseER = Extended Range (singlemode)
  + BaseSR = Short Range (multimode)
  + Higher numbers means higher speeds, duh. Assume MBit/s unless there’s a “G” then assume Gbit/s

## Wireless

* IrDA - Infrared Data
  + 16-25 Mbps
  + Only works along the same lines that light can travel
* Bluetooth (802.15.1)
  + 25-35 foot range
  + Really only good for connecting a user device to a peripheral
* Wi-Fi, duh, 802.11(a/b/g/n)
  + 2.4 or 5GHz
  + 5GHz has theoretically higher speeds, but 2.4 has better range

|  |  |  |
| --- | --- | --- |
| **Name-Standard** | **Speed (Mbps)** | **Usage** |
| 802.11a | 54 | 5GHz band; outdated; used for LAN networking in businesses; expensive |
| 802.11b | 11 | Cheaper 2.4GHz mode; |
| 802.11g | 54/108 | Cross between A and B flavors; 2.4GHz at fast speeds. Also offers backwards compatibility |
| 802.11n | 150/300/450/600 | Works at either 2.4 GHz or 5 GHz |

* + **Signal Modulation**
    - **FHSS - Frequency Hopping Spread Spectrum**
      * Rapidly switch between multiple channels
      * Enables multiple access between devices
      * Any interference only happens momentarily because of the hops
      * Usable in 2.4GHz band
    - **DSSS - Direct Sequence Spread Spectrum**
      * Used by 802.11b, and 802.11g (in tandem with OFDM)
      * When sending a message, the packet is “Spread” with random data to increase bandwidth
      * This allows it to become a “noise” signal which blocks interference
      * Also makes signal less jammable, and secure!
    - **OFDM - Orthogonal Frequency Division Multiplexing**
      * Used by 802.11a, 802.11g, 802.11n, and 802.11ac
      * Resilient to many forms of interference. Super complex though.
      * Something to do with sending multiple signals in parallel
  + **Signal Modulation by Wireless Standard!**
    - **802.11b**
      * Primary: DSSS
    - **802.11g**
      * Primary: OFDM
      * Also: DSSS
    - **802.11a**
      * Primary: OFDM
    - **802.11n**
      * Primary: OFDM
    - **802.11ac**
  + **DCF - PCF - Distributed/Point Coordination Function**
    - Employs collision avoidance methods
* **WiMax - Worldwide Interoperability for Microwave Access**
  + **IEEE 802.16**
  + Competes with LTE
  + Supports mobile, fixed, and nomadic connections
* General Wireless Info!
  + Wireless is more expensive than wired networks
  + Wireless is also affected by most other transmissions
  + MAC bridge can translate wireless frames into ethernet frames and vice versa
  + Wireless isn’t by default secure
    - Security was designed WEP - > WPA - > WPA2
    - WEP is fucking awful, and replaced by nearly everything else. WPA and TKIP function on existing WEP hardware, typically.
    - WPA utilizes TKIP to encrypt data
    - WPA2 utilizes AES to encrypt data better
      * WPA2 was instituted by 802.11i
      * This implementation is known as CCMP
      * **CCMP - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol**
  + Wireless devices can enter ad-hoc mode where they create a mesh, rather than utilizing the star topology of connecting to a router, but this is difficult to run and configure
  + Utilizes CSMA/CA (Collision Avoidance) rather than CD (Collision detection)!
* **Wardriving** is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA).

## IPv4

* Four octets of numbers
  + First octet tells you the size of the network, based on its range
  + Three sizes on networks - netid always represents 255
  + University - range 1-126
    - netid.hostid.hostid.hostid
  + Corporate/Hospital - range 128-191
    - netid.netid.hostid.hostid
  + Small Business/Home - range 192-223
    - Netid.netid.netid.hostid
* Within LANs sharing an IP address, private IPs are setup for each node - NAT

## IPv6

* Written in hexadecimal, and 128 bit
* 0000:0000:0000:1aff:1923:ab00:0000:22a1:3712:0000:0000:0000:acc2:32aa:8eff:bf00
  + You can replace a block of 0000 with “::” but only once. The computer can figure out how many 0’s there are because it knows how long the string should be.
    - 0000:0000:0000:1aff:1923:ab00:0000:22a1:3712::acc2:32aa:8eff:bf00
    - ::1aff:1923:ab00:0000:22a1:3712:0000:0000:0000:acc2:32aa:8eff:bf00
* EUI-64 can be used for IPv6 Auto-configuration
* DHCPv6 is a thing.
* IPv6 Link-Local Address(FE80::/10) is the same as IPv4 APIPA address (169.0.0.0…)
  + Automatic private addressing, when a pc needs an IP, but DHCP is down
* **Unicast**
  + Addressed and routed to a single IPv6 address
* **Anycast**
  + Addressed and routed to any and only one of a set of IPv6 Address
* **Multicast**
  + Addressed and routed to multiple IPv6 Addresses
* Honestly, IPv6 is complex, and not well-utilized yet. Worth checking its wiki page, but don’t break your brain over it.
* <https://en.wikipedia.org/wiki/IPv6_address>

## TCP/IP Stack Protocols, by OSI Layer

### Data Link

* **ARP Address Resolution Protocol**
  + Translates logical IP addresses into physical MAC addresses
  + Basically the connection between layer 2 and 3
* **RARP** Reverse… bla bla. It does the opposite

### Network

* **ICMP - Internet Control Message Protocol**
  + Connectionless protocol that enables Pinging routes
  + Manages control messages
  + Pings return RTT - Round Trip Time
* **IGMP - Internet Group Messaging Protocol**
  + Add, delete, and modify members of multicast group
  + Unlike broadcast, allows you to send message to multiple specific nodes, rather than all
* **RIP - Routing Information Protocol**
  + Allows for routing of internal, and some internet, traffic
  + Adapts to changes in network structure

### Transport

* **TCP** - **Transmission Control Protocol**
  + Connection oriented protocol that allows sending and receiving with receipts
  + Introduces concept of ports, or specific openings on nodes for specific data
* **UDP - User Datagram Protocol**
  + Sessionless TCP - no receipts, no guarantee of delivery

### Application

* **HTTP** **- Hypertext transfer protocol** 
  + transports data on the internet, typically in pages and HTML.
  + *Port 80*
* **HTTPS** - **Secure HTTP**
  + *Uses port 443* and SSL (Secure Socket Layer) to securely transfer data on the internet
* **SMB - Server Messages Block**
  + Allows shared access to files, printers, etc on a network
  + **CIFS - Common Internet File System -** Commonly known as
  + Port 445
* **FTP -** **File Transfer Protocol**
  + *Port 20 (data) / Port 21 (Transmission control)*
  + Securityless transfers of simple data
  + **SFTP** **- Secure FTP**
    - *Uses port 22* and SSH to transfer simple files securely
  + **FTPS**
    - Uses port 990, occasionally 21 and SSH to transfer simple files securely
  + FTPS/SFTP simply secure files differently, but both use SSH and AES
* **TFTP - Trivial FTP**
  + *Port 69*
  + UDP based FTP
  + Unreliable, mostly used for local data
* **Telnet - Telecommunications network**
  + Allows you to fully connect to a remote computer like another user with login and everything.
  + *Port 23*
  + *Clear text commands*
  + Remotely connects to a node
  + Not Secure
* **SSH - Secure Shell**
  + *Port 22*
  + Secure Telnet
  + Allows remote command-line login, remote command execution
  + **SCP - Secure Copy**
    - FT protocol based on SSH
* **NNTP - Network News Transfer Protocol**
  + *Port 119*
  + Carries USENET data back and forth
  + News stuff
* **LDAP - Lightweight Directory Access Protocol**
  + *TCP and UDP Port 389*
  + Allows a node to act as a directory for a specific kind of data
  + Microsofts Active Directory
* **NTP - Network Time Protocol**
  + *UDP 123*
  + Syncs network time with a server
* **POP3 - Post Office Protocol**
  + *TCP 110*
  + Allows for the retrieval and subsequent deletion of mail from a server
  + Downloads mail and stores it locally
* **IMAP4 - Internet Message Access Protocol**
  + *TCP 143*
  + Better, more commonly used, version of POP3
  + Allows your messages to be stored longer on the central server
  + Local host only holds some data
* **SMTP -** Simple Mail Transfer Protocol
  + *TCP 25*
  + Allows you to send mail. Works with POP3 and IMAP4
* **DNS** - **Domain Name Services**
  + *UDP 53*
  + Takes human readable names and makes them into machine logical names
* **SNMP** - **Simple Network Management Protocol**
  + *UDP 161*
  + Manages devices on IP networks like printers, routers, modems, etc
* PRETTY PICTUREs - <https://www.cybrary.it/0p3n/standard-network-ports/>

## NAT and ICS - Network Address Translation and Internet Connection Sharing

* NAT allows for one node to share its connection with several other nodes
  + Home networks only pay for one IP, but have up to dozens of devices
  + It’s like sharing a home address, and also putting your name on letters.
    - The package shows up to the home address, and the second address allows it to specify a person in the household
  + It is VERY DIFFICULT to connect a remote host to a NAT controlled node
    - This is because no port is directly open for the communication
    - It is very easy for a NAT controlled node to open a connection to a remote host
    - Port-forwarding can ease this
  + NAT automatically changes local IP data in packet headers before sending it past the NAT configured routing device
  + **PAT - Port Address Translation**
    - Multiple computers receive the same IP, with a different Port number so the router knows where to send packets
* ICS allows one internet connected device to share its connection with other devices
  + It’s a version of NAT
* **DNAT -** Automatically assigns global IP addresses from a pool
* **SNAT -** IP address statically assigned

# Networking+ Cert Study Guides Part 2

## **DHCP, Port Forwarding, and DMZ Hosts - NAT Tech**

* **DHCP**
  + See Above
* **Port Forwarding**
  + Works with NAT to provide openings for incoming traffic to “internal network” nodes.
    - Basically resolves the major NAT issue.
    - Allows remote hosts to establish reliable connections by keeping a port open.
  + For example, if a file sharing program needs to use TCP 4444 on a specific terminal, that message will normally get sent to the router, which makes no sense.
    - Port forwarding allows the router to redirect that request to the specific terminal on its NAT setup
  + Port Request on **(TCP/UDP) (Port Number)** *Forwards to* **(Internal IP Address)**
* **DMZ Host - Demilitarized Zone Host**
  + Any port request sent to the router is automatically forwarded to this host’s IP.
    - Port Forwarding doesn’t have to be manually configured for each request
      * Convenient but risky
    - All requests can be sent to a single sanitized host
      * That host can deal with the issue securely

## TCP/IP Basic Troubleshooting Tools

* Consider the use of ICMP’s *Ping* when trying to figure out why you can’t reach your company’s Outlook
  + You can ping the router, to see if there’s an open connection or if the internet is down.
* **NMAP - Network Mapper**
  + Security scanner used to discover hosts and services on a network
* **Tracert** - Traces the connection all the way back to a remote host.
  + Allows you to see exactly where the connection is lost
* **Netstat** - Gives info about TCP/IP connections and protocols
  + All connections
  + Listening ports
  + Routing table
  + Etc
* **Ipconfig** - Shows Ip configuration info
  + Ip address, default gateway, subnet mask (/all)
  + Can force DHCP release/renew (/release) (/renew)
* **Ifconfig -** IP configuration in UNIX environment
* **Winipcfg** - GUI based Windows 9x-era ipconfig tool
  + Windows based
* **ARP**  - Returns MAC address of specific IP
* **RARP** - Returns IP from specific MAC address
* **NSlookup** - Troubleshoot DNS - can show IP given Domain Name
* Each of these tools provides relevant information in specific situations, so consider what data is available, and use these tools to find out the rest of the data. It’s like algebra.

## NetBIOS - Network Basic I/O System

* Session layer communication
  + Primarily Names Sessions
  + Starts/Stops NetBIOS “Sessions”
* NetBIOS names are a maximum of 15 characters (pc names)
  + If one name corresponds to one IP, it’s a unique name
  + If multiple names correspond to an IP, its a group name
* NetBIOS default resolves names by broadcasting a request, and hoping the computer with that name will respond. If it doesn’t, each node receiving the broadcast should relay the message further.
  + Because this is cumbersome, specific NetBIOS utilities have been developed
  + **DNS** - See Above
  + **NetBIOS Name Server** - Stores NetBIOS names for easy name resolution.
  + **WINS Server** - Windows NetBIOS server
    - Primary and optional secondary server for redundancy
    - More features than NetBIOS
* Windows lets you store NetBIOS names in one of two files
  + **LMHOSTS File**  - Local Area Network NetBIOS names
  + **HOSTS** File - Remote hosts and Local hosts NetBIOS names
* Uses TCP 139
* Provides error detection and recovery
* Session Layer

## Common Protocol Suites

* **NetBEUI - NetBIOS Extended User Interface**
  + Microsoft Protocol suite for small, windows-only LAN
  + Cannot send past a router
  + Uses generic, non-unique names
* **AppleTalk**
  + Apple protocol suite for larger, mac only LAN and occasionally WAN
  + Limited to networks that only utilize mac
* **IPX/SPX - Internet Package Exchange/Sequenced Packet Exchange**
  + Novell (Netware) networks
  + IPX is similar to UDP - fastest protocol suite, but proprietary and not widely used
  + SPX is similar to TCP
* **DLC - Data Link Control**
  + PC and Non-PC connection
  + Used for older IBM machines, printers, etc
* **TCP/IP**
  + IP addressing
  + Suite protocols at several OSI layers (Session/transport/network/application)
  + TCP Ports
  + ARP (layer 2 to layer 3) translation
  + DHCP (automatic IP addressing)
* **DNS Record Types**
  + (A) - Address Record
    - Maps DNS to IP
  + (AAAA)
    - Maps DNS to IPv6
  + (PTR) - Pointer Record
    - Maps IP to DNS
  + (NS) - Name Server Record
    - Identifies Name server with authority over domain (hints)
  + (MX) - Mail Exchange Record
    - Identifies mail server with authority over domain
  + (CNAME) - Canonical Name Record
    - Allows aliasing of domain

## WAN Tech

* **IEEE 1905.1**
  + Enables easy home configurations of 802.11 wireless, 802.3 ethernet, and 1901 internet over power lines
  + Provides a common interface for the various techs
* IEEE 1901
  + **BPL - Broadband over Power Lines**
* **DOCSIS - Data over Cable Service Interface Specification**
  + Allows the addition of a data line to traditional cable infrastructure
* **POTS - Plain Old Telephone Service (Also PSTN - Public Switched Tele Network)**
  + Utilizes phone networks and analog-to-digital modems
  + Extremely slow, up to 56Kbps
  + Widely used, affordable
* **ISDN - Integrated Service Data Network**
  + Faster than POTS, but completely obsolete
  + Used wires specially setup by phone companies
  + Two 64 Kbps “B” channels
  + Circuit-Switched Network for voice
  + Packet-Switched for data
  + Can be used for video conferencing
* **DSL - Digital Subscriber Line**
  + The successor of ISDN
  + Requires special telecom line as well
  + Up to 10Mbps (occasionally 15Mbps)
  + Requires DSL modem to convert high speed DSL signal to network friendly language
  + *SDSL -* Similar down and up speeds
  + *ADSL -* Most commonly used, high down, normal up
  + *IDSL -* Longer range DSL
* **Cable**
  + Around 60Mbps
  + Uses cable line like cable tv, and coaxial cables
  + Requires cable modem
* **T1/T2/T3 (T3 can be known as E3 in europe, and DS3) AKA T-Carrier or E-Carrier**
  + T(X) lines are dedicated business lines. Reliable.
  + Upgrade to PTSN connections, often used as backbone connections
  + E lines upgrade at 4x each iteration, starting at 2.048Mbit/s. T lines fluctuate.
  + T3 line can be 15,000/mo - up to 45 Mbps
    - Equal to 672 dedicated phone lines!
  + <https://en.wikipedia.org/wiki/T-carrier#Comparison_of_T-carrier_and_E-carrier>
  + Examples of **Circuit Switching** technology
* **OC1/OC3/OC(X) - Optical Carrier**
  + OC1, 51.84 Mbps - very very business line
  + Multiples of OC are multiples of 51.84
  + Fiber optics
* **Leased Line**
  + Less necessary nowadays, it’s a dedicated data line to a LAN
  + Expensive, but reliable due to no competing traffic

### Cellular/Mobile WAN

* **GSM - Global System for Mobile Communication**
  + Utilizes **TDMA** 
    - **Time Division Multiple Access**
      * Each phone gets a time slot to transmit over very short intervals
  + Standard Cellular data system everywhere but USA and Russia
  + Requires a SIM
* **CDMA** - **Code Division Multiple Access**
  + Cellular tech
  + More security than GSM
  + Allows more people to connect at once
  + Built into phones- no SIM
* **LTE - Long Term Evolutions**
  + Built off GSM/EDGE
  + Marketed as 4G, but not truly 4g.
  + Only slightly better than WiMax
* **WiMax - Worldwide Interoperability for Microwave Access**
  + **IEEE 802.16**
  + Competes with LTE
  + Supports mobile, fixed, and nomadic connections
* LTE-Advanced and WiMax-Advanced are TRUE 4g tech.

### Protocols Related to WAN Tech

* ***Packet Switching vs. Circuit Switching***
  + Packet switched includes: Frame Relay and ATM
    - Multiple signals can go down a single channel by taking turns
  + Circuit switched includes POTS, T1, E1
    - The whole channel is taken up for a session-like communication
* **Frame Relay**
  + Utilizes **Packet Switching**
    - Organizes data into packet “blocks” so that multiple people can communicate on one line at once
  + Cheaper than Leased Lines but provides affordable speeds to locations
  + Primarily used to connect rural commercial locations to ISP backbones
  + Outdated
* **ATM - Asynchronous Transfer Mode**
  + Utilizes fiber optic cabling
  + Typically business class or backbone data
  + Well over 600Mbps
  + Cell-oriented packet switching
  + 48 Byte payload, 5 byte header means 53 byte cells!
* **MPLS - Multiprotocol Label Switching**
  + Includes ATM, Frame Relay, T1/E1, and DSL
  + Directs data-dense traffic along short path labels, rather than destinations
    - Avoids complex routing labels to enhance speed
* **MLPPP - Multilink Point to Point Protocol (MP)**
  + Utilize two PPP nodes to increase bandwidth
  + Use two modems! Whoaaa
* **MIMO - Multiple In, Multiple Out**
  + Standard in radio, uses multiple transmitters and receivers to multiple signals
  + Very important in Wifi, 3g, and 4g (802.11n, WiMax, HSPA+, LTE)
  + Nowadays, less than antennas, it refers to multiple data streams using multipath propagation
* **IP/SIP - IP/Session Initiation Protocol**
  + Controls Multimedia sessions over the internet
  + Instant Messaging
  + Telecom
  + Video Chat
  + Pulls a lot from HTTP and SMTP
  + SIP uses port 5060 for non-encrypted traffic
  + SUP uses port 5061 for encrypted traffic
  + **SDP - Session Description Protocol**
    - How **SIP** negotiates and handshakes the session configuration
  + **RTP/SRTP - (Secure) Real-Time Transfer Protocol**
    - **Port 5004/5005**
    - Transfers audio and video over IP
    - Often used for streaming like video conferencing, push-to-talk, etc
    - Port 5004
    - **TLS - Transport Layer Security**
      * Encrypts Streams
      * Secures HTTP
    - **RTCP** - **RTP Control Protocol**
      * Provides out of band statistics and control over an RTP session
      * Port 5005
* H.323
  + Pre-dates SIP, basically the same, but more complex
  + Port 1720
* **MGCP - Media Gateway Control Protocol**
  + Call control protocol for VoiP
  + Uses ports 2427 and 2727
* **VTC - Video Teleconferencing**
  + **Cisco Medianet**
    - Advanced Cisco architecture designed for video and rich-media platforms
    - It’s just all around good for video, end-to-end
    - **Rich Media**
      * Advanced, dynamic and interactive ads, basically
      * Respond when moused over, auto download applets, play video
  + Utilizes **IP/SIP and ISDN**
* **Tunneling Protocols**
  + Basic Info
    - Typically work at layer 4 (transport)
    - Typically replaces TCP/UDP
    - Allows you to use a protocol where it doesn’t natively belong
    - Fucking Trojan Horses, man
    - GRE, PPTP, IPSEC, and VPN are closely connected
  + **PPTP - Point to Point Tunneling Protocol**
    - Makes VPNs work
    - Uses TCP and GRE
    - *PPTP uses port 1723, GRE uses UDP 47*
    - **GRE - Generic Routing Encapsulation**
      * Works with PPTP
      * Tunneling protocol
      * Encapsulates network layer protocols to be transfered via Point-to-point links
* **IP PBX** 
  + Connects VOIP to POTS etc
  + Makes all variations of phone lines work together
* **LWAPP** - Lightweight Access Point Protocol
  + Allows multiple wifi access points to be controlled in one place
  + **CAPWAP** - Control and Provisions of Wireless Access Points
* **IPsec - IP Security**
  + Session oriented security.
  + **NETWORK LAYER -** despite being session oriented, it operates at the network layer, and provides GREAT end-to-end encryption of application data because of this
  + Negotiates mutual authentication between clients and sets up an encryption key that both clients agree on
  + Encrypts every packet sent during the session

## WLAN Tech

* **Roaming** - Ability to connect in one WAP area and another without reauthentication
* **LWAPP** - Lightweight Access Point Protocol
  + Allows multiple wifi access points to be controlled in one place
  + **CAPWAP** - Control and Provisions of Wireless Access Points
* **Channel overlapping-** Multiple channels share the same frequency band and cause interference
* 802.11a-ht, and 802.11g-ht allow 802.11n to send special packets that are compatible with earlier standards, but still speed up those standards!
* **Antennas**
  + Most WAPs use Dipole antennas
  + Dipole antennas, like omnidirectional antennas, cover a 360 degree horizontal distance
  + Dish antennas and unidirectional antennas are great for long range, but lack the area spread and require aiming
* **MU-MIMO - Multi-User MIMO**
  + Allows multiple users to transmit signals further and stronger
* **Beacon Frame**
  + Periodically sent by WAP to announce the presence of the LAN
  + Advertises the SSID, or Service Set Identification (network name)
* **Infrastructure Mode/BSS - Basic Service Set**
  + WLAN that requires a central WAP
  + Every BSS has a BSSID, which is the mac address of the central WAP
* **Ad-Hoc/Peer-to-Peer/IBSS - Independent Basic Service Set**
  + WLAN where devices communicate with each other, without the use of WAP
  + Without the central WAP, one IBSS cannot communicate with another BSS
* **ESS - Extended Service Set**
  + WLAN with multiple WAP
  + ESS have SSID, which is a 32byte maximum string
  + APs in an ESS are connected by **DS - Distribution System**
    - This is typically WDS or MESH
  + ESS enable roaming, where users can connect to multiple APs without reauthenticating
* **Thick(fat) vs. Thin APs**
  + **Thick/Fat APs** provide everything needed for centralized configuration
  + **Thin APs** are basically a radio and antenna controlled by a wireless switch

## Network Management

* **NMAP - Network Mapper**
  + Security scanner used to discover hosts and services on a network
* **Microsoft Active Directory**
  + Implementation of **LDAP - Lightweight Directory Access Protocol**
  + Designed for Microsoft networks
  + Security, Access Control, and Group Policy
  + Can install and update software across the network
  + Assigns roles and permissions to computers along the network
* **VLAN** - **Virtual LAN**
  + Although all computers are physically on the same network, they are logically assigned to different LANs so that they can have different administrators
  + Allows load-balancing of traffic among hosts
  + **Switch Ports** can be used to configure membership of a VLAN
    - MAC address to IP mapping can as well
  + **Port Trunking**
    - Utilized to carry data from multiple VLANs across a network
    - Utilizes **802.1q** or **ISL (interswitch link)** tags in the packet headers to identify the target VLAN
    - **VTP - VLAN Trunk Protocol**
      * Cisco proprietary
  + Establish VLAN connections
    - **Dynamic** - VLAN assignment is designated by software, typically reading MAC address or user ID. The switch queries a database to check this info
    - **Static** - Each port is assigned a VLAN, so any device connecting to that port is assigned to that VLAN
* **LACP - Link Aggregation Control Protocol**
  + Enables several physical ports to act as a single logical channel.
  + Increases throughput by **aggregating** several connections!
  + **NIC Teaming - Network Interface Controller**
    - Form of LACP for network cards. Increases throughput and redundancy
* **Load Balancing Server**
  + Intelligently coordinates traffic and requests so that no part of the system gets overwhelmed
* **Redundancy**
  + Multiples of everything so that if one thing goes down, the system still runs
* **Access Control**
  + The ability to determine who can see/do what on the network
  + **User-Defined:** User chooses what to share
  + **Mandated**: Central server determines permissions (Active Directory!)
* **SDN - Software Defined Networking**
  + Meant to address modern needs of quickly changing tech and data centers
  + Architecture designed to make network management simpler and more dynamic
* **SNMP - Simple Network Management Protocol**
  + Allows for the collection of data from, and management of, devices connected to a network
  + Devices attached to the network have SNMP agents which send back data to the main SNMP controller
    - These alerts are sent via “traps” and are unsolicited by the manager
    - The management station receives notifications from the agent on UDP 162
    - The agent receives requests on UDP 161
  + **Net SNMP**
    - Suite of software that allows SNMP to be deployed
    - Common Commands
      * <https://en.wikipedia.org/wiki/Net-SNMP>
      * Snmpget - communicate updated info with agents
      * Snmpwalk - receives a subtree of management values with getnext commands
  + **MIB - Management Information Base**
    - Database often connected to SNMP
    - Allows users to manage the entities in a communication network
    - Contains information about configuration and device states

## Security and Industrial Usage (Network Management Part 2)

* **UTM - Unified Threat Management**
  + Evolved Firewall
  + Functions as Firewall, VPN, Anti-invasion, Anti-Viral, content monitoring, load balancing, data loss prevention, and reporting
  + One device to run it all- easier to administrate, but centralized point of failure
* IDS v IPS - Both firewall like!
  + Can be separated into (N) or (H) such as (HIPS) or (NIPS)
    - **H - Host Based**
    - **N - Network Based**
  + **IDS- Intrusion Detection System**
    - Notes a “known event” that it finds in packet
  + **IPS - Intrusion Prevention System**
    - Rejects a packet if it contains a “known event”
  + **HIPS, NIPS, HIDS, NIDS**
* **AAA - Authentication, Authorization, Accounting**
  + **Authentication -** Verifying a user identity
  + **Authorization -** Granting access to what that specific user can do
  + **Accounting -** Tracking who has used a resource
* **RADIUS** - Remote Authentication Dial In User Service is a standard utility for AAA
  + Uses UDP
* **TACACS+ - Terminal Access Controller Access Control System**
  + Similar to RADIUS (AAA), but uses TCP
  + Allows a remote access server to forward a user’s credentials to gain access to a system
* **ICS - Industrial Control Systems**
  + General term referring to a control system that helps manage industrial applications
  + The three main types of systems below often have a lot of crossover, but are the general distinction of system categories
  + **SCADA - Supervisory Control and Data Acquisition**
    - Utilizes remote terminals to collect data over large geographical data
    - Useful for oil, gas, and water which can traverse a long distance, and cannot be monitored locally
  + **DCS - Distributed Control Systems**
    - Real time data collection and control management for practical applications
    - This can involve oil, gas, waste water, mining, or any other major industrial application
    - Allows control beyond just a small refinery room
    - Primarily centralizes multiple functions of a specific central location, such as the different aspects and systems of a large refinery
    - **RTU - Remote Terminal Unit**
      * ...It’s a damned remote terminal. What do you expect me to say?
  + **PLC - Programmable Logic Controllers**
    - Used in machinery that- automates high speed, typically binary mechanisms and replaces less reliable tech
* **UC Server/Unified Communications**
  + More of a buzzword than a real product
  + UC is a product, or suite of products that integrates many forms of communication (messenger, calling, video chat, file sharing, etc) into one platform
* **SIEM - Security Information and Event Management**
  + Combined SIM and SEM
  + Combined Real-time monitoring (SEM) with Logged data (SIM)
  + Software allow security specialists to monitor and track a system
* **DMZ - Demilitarized Zone**
  + Refers to the part of a company’s internal, private servers are externally facing
  + Any part of a company’s servers that can be accessed externally is DMZ including mail servers, web servers, and FTP servers
  + Less protected subnet than main servers
  + By keeping DMZ separate and only communicating through certain channels, they provide an extra layer of security
  + **DMZ Hosts are separate things.** They have a similar use in home networks- funneling traffic through a certain point- but they are not true DMZ
* **NAC - Network Access Control**
  + A set of rules that anyone connecting to the network must follow
    - Often includes antivirus definitions
    - Enforces AAA
    - Enforces user roles, policies, and permissions
  + Pre-admission NAC
    - Requires users to meet requirements and validate themselves before connection
  + Post-admission NAC
    - Client is granted or denied permissions after connection
  + **802.1x PNAC - Port based NAC**
    - When a device is connected to a port, the port is switched to unauthorized. Only **EAP** (Extensible Authentication Protocol) data can be communicated through that port until the device is authenticated
  + **MAC Filter**
    - NAC utility that checks the physical address of an **NIC (Network Interface Card)**
  + **ACL - Access Control List** 
    - Lists permissions of an object- who and what can access it
    - **Implicit Deny Policy** - Anything not positively verified by the ACL is refused
* **TEMPEST**
  + NSA specification designed to prevent signal leakage and eavesdropping on sensitive info

### Additional Security

### **NIPS - Network Intrusion Protection System**

* + Umbrella term for hardware or software that protects computers from unauthorized access and malicious activity.
* **HIDS - Host-Based Intrusion Detection System**
  + NIPS, but on the computer, not the network

### **DAI** - **Dynamic ARP Inspection**

* + **ARP** communicates by checking IP to MAC address mappings, but can be subject to MitM attacks
  + DARP validates those mappings, and discards packets with invalid addressing
* **MAC Filter**
  + NAC utility that checks the physical address of an **NIC (Network Interface Card)**
* **CHAP - Challenge Handshake Access Protocol**
  + Periodically re-evaluates client to prevent session hijacking
* **EAP - Extensible Authentication Protocol**
  + Commonly used by 802.11 wireless and Point to point technology for authentication under various protocols
  + **PEAP - Protected EAP**
    - Encapsulates EAP in a Transport Layer Security (TLS) tunner
* **Authentication Processes**
  + Can be broken into several categories:
  + *Something you are*
    - Biometrics
  + *Something you have*
    - Key card, keys, etc
  + *Something you know*
    - Passwords, usernames
  + *Somewhere you are*
    - Physical location
  + *Something you do*
    - Typing style, handwriting, etc
  + Multifactor Authentication
    - Must utilize one item from at least two categories
* **Biometrics**
  + Anything bodily that can be scanned
* **Physical Security Detective Controls**
  + CCTV, IP camera, etc. Physical tech
* **Physical Security Control**
  + Biometrics, cipher lock (keypads), Proximity reader, security guards, video surveillance
* **Mantrap**
  + Prevents tag-alongs getting through security by using airlocks, etc
* **Hash Function**
  + **SHA (Secure Hash Function) and MD5 are common hash functions**
  + Hash is a value derived from longer data. Useless as content, but can be used to detect any changes in large datasets
  + This is important to ensure that data under inspection hasn’t been tampered with at any stage of inspection
* **Stateful Inspection - AKA Dynamic Packet Filtering**
  + Monitors the state of connections and allows packets based on those states
* **eDiscovery**
  + Tracking, collection, and analysis of all data for legal purposes

### Tech Agreements

* **AUP - Acceptable Use Policy**
  + A set of constraints and practices a user must agree to in order to access a network
* **SLA - Service Level Agreement**
  + Defines what a customer will receive from a service provider (standards and quantities?)
  + Specific performance requirements from a vendor
* **MOU - Memorandum of Understanding**
  + The rules and responsibilities two parties must follow while working on a collective goal
* **MSA - Multisource Agreement**
  + Agreement across vendors to set certain standards for compatibility in products from different manufacturers
* **SOW - Statement of Work**
  + Activities, deliverables, and time-line from vendor to client
  + Includes purpose, scope of work, cost estimates, requirements, etc

### Common Attacks To Know

* **Wardriving**
  + Driving around looking for unsecured WAPs
  + **Warchalking**
    - Marking unsecured WAPs
* **DoS - Denial of Service**
  + Spamming the fuck out of someone to kill bandwidth and deny service to authentic users
  + **DDoS - Distributed DoS**
    - Utilized multiple infected terminals to spam from multiple locations
    - Utilizes **botnets**
  + **Reflected DDoS**
    - Tricks a third party into performing the attack to hide the identity of the culprit
    - **Smurf Attacks**
      * Utilizes IP broadcasting to send so many packets that everything shuts down
      * Utilizes IP spoofing
      * Can be detected due to a large number of ICMP network replies
        + **Internet Control Message Protocol** - sends errors
* **ARP Spoofing - Address Resolution Protocol Spoofing**
  + Tricks a local network into confusing the attacker’s mac address with a key route link, like the default gateway of that network
  + This causes data to be sent to the attacker instead
* **Evil Twin - Rogue Access Point**
  + Poses a tainted WAP as a healthy WAP
  + Creates a “rogue” access point
  + Allows owner of the evil twin to access data on connected computers
* **Bluejacking**
  + Unsolicited messages to bluetooth
* **Bluesnarfing**
  + Unauthorized access to a device through bluetooth
* **MitM - Man in the Middle Attack**
  + Hiding in the middle of a communication and changing shit without anyone knowing
  + Basically being a dick hidden proxy
* **VLAN Hopping**
  + Jumping from one VLAN to another to get info from a VLAN that you normally couldn’t access
  + **Double Tagging**
    - Using two IP tags to trick the route
* **Zero Day Attacks**
  + Exploit bugs the developer doesn’t know about at launch
* **DHCP Snooping**
  + NOT AN ATTACK
  + Security protocol used to identify rogue DHCP servers and drop them
* **Logic Bomb**
  + Virus that only activates under certain conditions
* **Worm**
  + Standalone, self-replicating virus
* **Trojan**
  + Virus that disguises itself within a useful program
* **Ransomware**
  + Virus that encrypts or blocks functions on a computer until a specific action has been performed (often, sending money)
* **Grayware**
  + Not technically malware, but bad for your system

## Network Storage

* **SAN - Storage Area Network**
  + Enables mass **block-level data** storage to be accessed by the network
  + Works with disk array, tape libraries, and optical jukeboxes
  + Dedicated local network of storage devices
  + **iSCSI - Internet Small Computing Systems Interface**
    - Protocol for connecting data storage units to one another over a network
    - Allows SAN style storage to appear as disks to most clients
* **NAS - Network Attached Storage**
  + Enables **file level data** storage to be accessed by the network
  + Works better in RAID arrays, and primarily with hard disks or SSDs

## Advanced Routing

* **DSCP** **- Differentiated Services Code Point**
  + Allows different IP packets to be labelled and handled differently
  + Allows for effective management of QoS (quality of service) and Traffic management
  + **CoS - Class of Service**
    - Identifier in packet header that defines QoS standard
* **AS - Autonomous System**
  + A collection of IP routing prefixes under control of a single Administrator (normally an ISP)
  + Presents a clearly defined routing policy for the internet
  + *Basically* a set of rules that a large group uses for their routing and internet connection, that needs to be officially registered
  + Autonomous Systems can communicate through **BGP**
  + **Autonomous System Number** is assigned by ICANN and is essential to run an AS
  + Four Types of AS
    - Multihomed AS
      * Maintains connection to other AS for redundancy
    - Stubbed AS
      * Only connected to one other AS- can be a waste if parent AS has similar settings
    - Transit AS
      * AS that allows other AS to talk through it to other AS
    - Internet Exchange Point AS
      * Physical Infrastructure that allows ISPs and AS to send traffic between one another
* **IGP - Interior Gateway Protocol**
  + Allows gateways to communicate routing data between each other *within* an autonomous system
  + Two categories of Protocols:
    - **Distance Vector Routing**
      * Each router advertises a DV (Distance Value) and all other routers check that data against each other, to fill a routing table with DV metrics, rather than full route data
      * Includes RIP and RIPv2 and IGRP
    - **Link State Routing**
      * Every router understands the full network topography, and calculates its routes accordingly
      * Includes OSPF and IS-IS
    - **Hybrid Routing Protocols**
      * Have features of both
  + **RIP and RIPv2 - Routing Information Protocol**
    - Distance-Vector Routing Protocol
    - Only works for routes less than 15 hops
    - Broadcasts routing table every 30 seconds to all other routers
    - **Preventing Incorrect Routing Info**
      * **Split Horizon**
        + No Backtracking!
        + Distance-vector, reduces routing loops
      * **Route Poisoning**
        + One router tells all the other routers that a route is bad
      * **Holddown**
        + If a router hears that a route is bad, it sets a timer that prevents it from checking that route again until the timer expires
    - RIP is shitty, but easy to use
    - RIPv2 supports **CIDR - Classless Inter-Domain Routing**
      * Simplified information about subnets and routing info
    - RIPv2 doesn’t broadcast all routing table data anymore, it only multicasts it!
  + **OSPF - Open Shortest Path First**
    - Link-state, interior routing protocol
    - Works within a single domain or AS
    - Basically just stays constantly updated on network topography and auto-calculates routes
    - Doesn’t use TCP or UDP, just uses protocol 89 to transfer data
  + **IS-IS** **- Intermediate System to Intermediate System**
    - Runs the backbone of large ISP data transfers
    - Determines best route to efficiently move data through a packet switched network
    - Link-state protocol that floods each router with topography information
  + **STP - Spanning Tree Protocol - 802.1d**
    - Creates a spanning tree of active links between nodes in topography
    - Only allows one single best path to be active, and deactivates useless links
    - Designed to prevent looping and broadcast static
    - Replaced by **SPB**
    - **SPB - Shortest Path Bridging**
      * Allows all links to remain active and evaluates them for a cost
      * Reduces user era
      * Makes the pathing more dynamic
      * Allows the system to adapt faster to plug and play activity
    - **802.1w - RSTP - Updated STP** Rapid reconfiguration of STP
* **EGP - Exterior Gateway Protocol**
  + Allows two gateway hosts to share routing information throughout a network of separate Autonomous systems
  + **BGP - Border Gateway Protocol**
    - Hybrid Routing Protocol
    - Path-Vector protocol/distance vector protocol
    - Does all the heavy lifting between AS networks
    - iBGP (internal) is good for large private networks
    - eBGP (external) runs gateways between AS’s
* Redundancy and Backups in Routing
  + **VRRP - Virtual Router Redundancy Protocol**
    - Allows for automatic assignment of available IP routers to available IP clients
  + **HSRP - Hot Standby Router Protocol**
    - Allows for a second router to be setup as a failsafe if the primary default gateway goes down
    - If one router goes down, the next highest priority router will take over its IP

## Remote Access

* **RDP - Remote Desktop Protocol**
  + Microsoft proprietary GUI that allows you to connect to another computer
  + Needs port 3389 open
* **RAS - Remote Access Service**
  + Outdated dial up microsoft thing
* **PPP - Point-to-Point Protocol**
  + Data link layer protocol
  + Versions of it are used for DSL connections
  + Can enable authentication between two nodes
  + Less outdated dial up access thing?
  + Replaces **SLIP - Serial Line Internet Protocol**
    - Low overhead, but less features than PPP
* **PPTP** 
  + More secure PPP
  + Packages PPP packets into “pills” that can’t be sniffed or looked at
  + Often used to create VPNs
* **L2TP - Layer 2 Tunneling Protocol**
  + Uses IPsec (IP security) to encrypt data from client to server
  + More versatile than PPTP, and more secure
* **SSL - Secure Socket Layer**
  + Public Key Encryption
  + Used in HTTP, FTP, and other application layer tech
  + Provides security through the transport layer
  + HTTPS is the most known use
  + **TLS - Transport Layer Security**
    - Updated SSL
    - Secures HTTP
* **Kerberos**
  + **Port 89**
  + Unix-like, but also employed on windows
  + Allows for client-server authentication using a shared key
* **Banner**
  + Initial information displayed by remote server after connecting to a service

## Cloud Computing and Services

* **PaaS - Platform as a Service**
  + Gives users a full platform for web app development
  + Reduces the needs for developers to recreate the full infrastructure suite
  + Platform delivers networks, [servers](https://en.wikipedia.org/wiki/Server_(computing)), [storage](https://en.wikipedia.org/wiki/Storage_(memory)), [OS](https://en.wikipedia.org/wiki/Operating_system), 'middleware' , etc
* **IaaS - Infrastructure as a Service**
  + Third party hosts hardware, storage, servers, etc for the user
  + Third party is often in charge of routine maintenance
* **SaaS - Software as a Service**
  + On-demand software that’s centrally hosted and usable on a subscription
  + Adobe suite is kind of like this, and so are MMOs

## Repair Tools

* **Crimping Tool**
  + Connects ends to twisted pair wires
* **Punch Down Tool**
  + Connects wires to fixed locations (like wall jacks)
* **TDR tool - Time Domain Reflectometer**
  + Times the bounce back of a signal down a wire
* **Tone Generator**
  + Helps identify a cable by the tone generated
* **Oscilloscope**
  + Frequency and voltage of analog and digital signal
* **Cable Certifier**
  + Verifies performance and compliance with ISO and TIA standards
* **Electrostatic Discharge**
  + LIGHTNING FROM YOUR HANDS

# Extra Ports Info!

* Well-known/System Ports
  + 0-1023
* User Ports/Registered Ports
  + 1024-49151
* Dynamic/Private/Ephemeral Ports
  + 49152-65535
* Port Numbers and their Applications
  + 20 - FTP (Send file data)
  + 21 - FTP (Session info)
  + 22 - SSH, FTPS, SCP!
  + 23 - Telnet
  + 25 - SMTP
  + 49 - TACACS+
  + 53 UDP/TCP - DNS
  + 67 UDP - DHCP and BOOTP
  + 69 - TFTP
  + 80 - HTTP
  + 88 - Kerberos
  + 110 - POP3
  + 119 - NNTP (Network News Transfer Protocol)
  + 123 - NTP (Network Time Protocol)
  + 137,138,139 - NetBIOS
  + 143 - IMAP
  + 161 - SNMP (Agents receive requests)
  + 162 - SNMP (Controller receives data)
  + 389 TCP - LDAP Lightweight Directory Access - 389
  + 443 - HTTPS (over TLS/SSL)
  + 445 - SMB Server Messaging Block - 445
  + 1701 - L2TP, L2F Layer 2 Tunneling Protocol - 1701
  + 1720 - H.323
  + 1723 - PPTP Point to Point Transfer Protocol - 1723
  + 1812,1813 - RADIUS RADIUS - 1813,1812
  + 2427 - MGCP Media Gateway Control Protocol - 2427
  + 2727 - MGCP
  + 3389 - RDP Remote Desktop Protocol - 3389
  + 5004 - RTP Real-time Transport Protocol - 5004
  + 5005 - RTP (Default)
  + 5060 - SIP (unencrypted) Session Initiation Protocol - 5060
  + 5061 - SIP (encrypted with TLS)

# Misc Missed Info

* MAC addresses
  + 48 bit hexadecimal
  + Hard coded into NIC
  + Physical address
  + Each device only has one, and it’s totally unique
  + Can be seen on linux with Ifconfig
  + Can be seen on Windows with ipconfig /all
* **Hypervisor**
  + Runs Virtual Machines
  + Allows you to have multiple non-native OS run on a platform
  + VSPHERE
* **AES - Advanced Encryption Standard**
  + Replaces **DES - Data Encryption Standard**
  + Used with SSH and stuff
* Network+ Troubleshooting Theory
  + Identify the Problem
  + Establish a Theory of Probable Cause
  + Test the theory to determine cause
  + Establish a plan of action to solve the problem and identify effects
  + Implement the solution or escalate as necessary
  + Verify full system functionality and implement preventative measures if applicable
  + Document findings, actions, and outcomes
* **Common command Line Windows/Linux**
  + **Ipconfig -** Shows TCP/IP settings - WINDOWS
  + **Netstat -** Displays protocol statistics and current TCP connections - WINDOWS
    - -a shows all active protocols and listening ports
  + **Ifconfig** - Ipconfig for unix
  + **Pinging IPv6**
    - In windows - ‘Ping -6 host1’ or ‘ping host1 -6’
    - In Linux - ping6 host1
  + **Nbtstat** - Windows command to troubleshoot Netbios name resolution issues
* **SNR - Signal to Noise Ratio**
  + ...Measures the ratio of actual signal to background noise.
* **LG - Looking Glass Server**
  + Read only portal to all the routers in an organization
* **Demarc** 
  + The juncture at which the ISPs cabling ends and local cabling begins
* **Smart Jack**
  + Placed on the demarc!!
  + Remote line diagnostics
* Demultiplexer
  + Single in, multi out
* **MDF - Main Distribution Frame**
  + Cabling rack that connects and manages telecommunication wiring between itself and **IDFs - Intermediate Distribution Frame**.
  + MDF connects between public and private lines entering a building
  + IDF connects between MDF and equipment

A+

A+ Notes are not comprehensive, and only contain the information I considered less common knowledge, or more detailed. These notes are **INCOMPLETE.** This section is only here if you need a little background for networking.

# BIOS and Basic Booting

* **BIOS - Basic In/Out System**
  + Performs the initial hardware checks with PC initialization
  + Allows the operating system to interact with hardware
    - Device Drivers also serve this purpose
  + **EPROM/EEPROM - Erasable Programmable Read-Only Memory/ElectricallyEPROM**
    - A memory chip that can retain its data even when powered off. Used to store mission-critical data that doesn’t require initialization, like BIOS.
    - Flash memory also serves this purpose!
  + **MSinfo32.exe -** Allows user to view basic info about BIOS
  + **POST - Power On Self Test**
    - Basic hardware diagnostic tests, indicates status through beeps!
  + **CMOS Ram -** RAM supported by a series of small batteries so that it can retain BIOS settings even after power-down
  + Highest BIOS permissions are Supervisor Password
  + Can configure CPU performance, Memory performance, User/Supervisor Passwords
  + Hardware Diagnostics
  + **LoJack or CompuTrace**
    - Tracks your device to find it if stolen or lost
    - Built into bios so automatically installs on storage device
    - Includes Phone Home which sends location data to central location
    - Includes Theft Mode to lock down or delete files from PC
  + Secure Boot Capability will only run applications with known-good signatures
* **UEFI - Unified Extensible Firmware Interface**
  + Updated BIOS tech
  + Supports HDD over 2 TB
  + GUI
  + Mouse Support
  + Network Capable
  + Backwards/Forwards Compatible
  + Modular Design
* **TPM - Trusted Platform Module**
  + Enables disk encryption, password protection, and other security features
  + Retains Encryption keys, signatures, etc
  + Enables DRM
  + Integrates with Windows BitLocker for full disk encryption
* **PXE- Preboot Execution Environment**
  + Enables booting from a network device
  + Apple Netboot does the same on apple

## Motherboards and Basic Hardware

* Over 40 types of motherboards, but a few main types.
* **ATX - Advanced Technology Extended**
  + **Standard, Micro** form factors
    - Micro merely has less expansion slots
  + 20 Pin or 24 pin power connector for Mobo. Occasionally addition 4/8 pin connector
  + Includes I/O backplate
* **ITX**
  + **Mini, Nano, Pico, Mobile** form factors
  + Developed by VIA tech in 2001
  + Mini-itx is compatible with ATX cases
    - Usable for single-use computing like streaming media or security
* Each part of the Mobo is connected via ‘bus’
  + ‘Width’ of bus is the bandwidth, how many bits can pass through the pathway at a time
  + Each bus has a clock speed, which is how fast the bus can go, counted in Hertz, though advanced technology can multiply that clock speed
* **PCI - Peripheral Component Interconnect**
  + Communicates data in parallel between the south bridge and the PCI device
  + **PCI-X -** PCI eXtended
    - Designed for servers, still parallel, but much higher speed
  + **PCIe - PCI Express**
    - Transfers serially, so much faster
    - 1, 2, 4, 8, 16, and 32 full duplex transfer lanes (x1, x2, x4, etc…)
    - Because the slots can have varying physical lengths and lanes, its easier to architect around on a mobo design
    - V1.x - 250 MB/s, V2.x - 500 MB/s, v3 - 1GB/s, v4 - 2GB/s
  + **MiniPCI**
    - Similar design, but much smaller bus!
    - Good for laptops
* **Intro to Memory**
  + **DIMM - Dual Inline Memory Module**
    - Standard Memory chip
    - Can be DDR, DDR2, DDR3, etc
      * Can tell the DDR by where the tab in the middle of the connections is
      * DDR - 184 pins
      * DDR2/3 - 240 pins
    - Electrical Contacts are different from different sides
    - 64 bit data width on a DIMM
    - **SO-DIMM - Small Outline DIMM**
      * Small form for laptops
      * DDR/DDR2 - 200 pins
      * DDR3 - 204 pins
    - **Micro-DIMM**
      * Mobile devices
* **CPU Sockets**
  + Very specific per motherboard/processor combo
  + Two Main Connection types:
    - **ZIF - Zero Insertion Force**
      * Many tiny pins on the CPU, many tiny holes on mobo connector
    - **LGA - Land Grid Array**
      * Many tiny pins on the mobo connector, many holes on cpu
* **Motherboard Chipsets**
  + Variation between bus speeds, cooling systems, layouts, etc
  + **Northbridge - Central Memory Connector** 
    - Connects the CPU to the Memory
    - Very high bandwidth
  + **Southbridge - Central Manager**
    - Manages connections- interface slots, peripherals, usb, ethernet, HDD, etc
    - Bios might connect to south bridge
    - GPU connects through south bridge
  + **Super I/O**
    - Single chip that handles a lot of I/O for serial and parallel ports, keyboards, mouse, and other low bandwidth devices
  + Modern Mobo, like chipsets utilizing ivy bridge, combine many functions in the CPU
    - This reduces the reliance on slower bus, and allows more devices to be consolidated and handled by higher-speed handlers
* **Jumpers and Connectors**
  + Connects small fans, LEDs, reset button, NIC connectors, power buttons, speaker, etc
  + Jumpers allow you to disable or enable features of the mobo, often labeled JP
    - You just move the connector to cover both of the pins you want to jump
    - Might change bus speed, enable/disable ports, or resets BIOS

## Advanced Memory

* **RAM - Random Access Memory**
  + **SRAM - Static RAM**
    - Very expensive, but ultra fast
    - Takes a lot of space
    - Often in processor cache
      * L1, L2, L3 caches
  + **DRAM - Dynamic RAM**
    - Our favorite memory
    - Constantly refreshed- otherwise data disappears
    - Can put data anywhere and access it through referencing memory address (unlike tape drives)
  + **SDRAM - Synchronous DRAM**
    - Synchronous with common system clock
    - Queues up one process while waiting on another
    - NOT **SRAM - Static RAM**
    - **SDR SDRAM - Single Data Rate SDRAM**
    - **DDR SDRAM - Double Data Rate SDRAM**
      * DDR Memory is typical in computers
      * Multiplies data rate by the clock speed
      * DDR-200 = 200 Million transfers per second (100 MHz)
        + Clock speed = 100 MHz
        + DDR means two transfers per clock
        + 200 million transfers
        + Multiply by 8 to get throughput in MB/s
        + 200x8 = 1,600 = PC1600
    - **DDR2**
      * Twice as fast as DDR
      * 4 transfers per clock
        + DDR2-400 = Clock speed = 100 MHz
        + DDR2 means four transfers per clock
        + 400 million transfers
        + Multiply by 8 to get throughput in MB/s
        + 400x8 = 3,200 = PC2-3200
    - **DDR3**
      * Twice as fast as DDR2
        + 8 transfers per clock

DDR3-800 = Clock speed = 100 MHz

DDR3 means four transfers per clock

800 million transfers

Multiply by 8 to get throughput in MB/s

800x8 = 6,400 = PC3-6400

* **ROM - Read Only Memory**
  + Where the BIOS is stored
  + Also video game cartridges!
  + **PROM - Programmable ROM**
    - Engineer would program it
  + **EPROM - Electronic PROM**
    - Can be reprogrammed occasionally
  + **EEPROM - Electrically Erasable PROM**
    - Flash memory, like SSD
* Checking Memory
  + **Parity Memory**
    - Adds parity bit to a byte to detect most simple errors
    - Can’t correct errors
  + **ECC Memory**
    - Expensive for enterprise systems
    - Able to detect and correct errors on the fly
* Registered Memory
  + “Buffered” memory
  + Used mostly on servers to stabilize the OS
  + You can see the chips in the middle of the stick of RAM
* Multi-channel Memory
  + Multiple sticks to increase throughput in pairs or trios
  + Matched memory must be identical
* Single-Sided v Double-Sided memory
  + *Can* be physical, but more specifically “ranks” of memory.
  + Think about it like virtual separation between the RAM

## Storage Devices (Brief)

* CD-Rom
  + 700 Megabytes
* DVD - 4.7 Gigabytes
  + RW - Rewritable
  + DL - Dual Layer
* Blu-Ray - 50 Gigabytes
  + BD-R - Blu-ray Disc Recordable
* HDD - Hard Disk Drive
* SDD - Solid State Drive
  + Flash Memory
* SSHD - Solid State Hybrid Drive
  + More hard disk than solid state, normally.
  + Uses flash memory cache to increase I/O rates
* Flash Drives
* SD - Secure Digital Card
* Tape drives
  + Good for archival content
  + **LTO - Linear Tape Open**
    - **Ultrium form-factor**
* **RAID - See Section in Network+**

## CPU Socket Types

* **ZIF - Zero Insertion Force**
  + Many tiny pins on the CPU, many tiny holes on mobo connector
* **LGA - Land Grid Array**
  + Many tiny pins on the mobo connector, many holes on cpu
* **Main Types!**
  + **Intel**
    - LGA 775 - 775 Pins
      * Also called Socket T
      * Pentium 4, Intel Core 2 Duo, Xeon, and Celeron
      * 2004
    - LGA 1366 - 1366 pins
      * Socket B
      * Replaced 775
      * Intel Core I7
      * 2008
    - LGA 1156 - 1156 pins
      * Also replaced 775
      * Integrates Northbridge into the chip
      * Socket H1
      * I3/I5/I7
      * 2009
    - LGA 1155
      * Socket H2
      * Supports Sandy Bridge and Ivy Bridge CPU
      * 2011
    - LGA 1150
      * Socket H3
      * Haswell and Broadwell architecture
      * 2013
    - LGA 2011
      * Socket R
      * Replaces 1366 and 1567
      * Sandy Bridge-E/EP and Ivy Bridge-E/EP (enthusiast/xeon class)
      * 2014
  + **AMD**
    - AM3 - 941 Pins
      * Replaces Am2/Am2+
      * 2009
      * PGA
    - AM3+ - 942 Pins
      * 2011
      * PGA
    - FM1 - 905 Pins
      * 2011
      * AMD 10H cpu architecture
      * A-series process
      * DDR3 support, integrated PCI-e
    - FM2 - 904 pins
      * “Piledrive” cpu architecture
      * 2012
    - FM2+ - 906 pins
      * Micro PGA-zif package
      * 2014
      * “Steamroller” CPU architecture
* CPU Characteristics
  + CPU Clock - MHz or GHz (primarily GHz)
  + Actual Speed
    - Clock speed, architecture, bus speed, bus width, L1/L2 cache size, OS
    - We no longer market on clock cycles, instead on key features
    - No clear benchmark for performance
  + Multi-core
    - Each core in a multi-core could have its own L1/L2 cache, but could share an L3 cache
  + Caches
    - Very very fast memory
    - Increased throughput significantly
    - L1 - First check
    - L2 - Secondary Data
    - L3 - Tertiary Data
  + **HTT - HyperThreading Technology**
    - Pretends to be multiple cores
    - 15-30% improvement
  + Intel Virtualization Technology VT (AMD-V)
    - Enables virtualization within processor
    - Greatly improves virtual OS
  + 32 bit v 64 bit
    - 64 bit has more data ‘width’
    - Bigger integer size, larger memory addresses, larger bus size
    - Can move twice as much data as 32 bit
    - OS must be optimized for 64 bit
  + Integrated GPU
    - Helpful, but not that great
  + Integrated Security - NX bit - No eXecute bit
    - Intel calls it XD bit eXecute Disable
    - Memory areas where code can’t run
    - Windows calls it DEP - Data Execution Prevention
* CPU Cooling
  + Heat sink of copper or aluminum
  + Connected to chip via thermal paste
  + Water cooling
  + Some devices just use heatsinks, no fans

## Computer Interface Speeds and Distances

### Cables

* **USB 1.1**
  + Low Speed - 1.5 Megabits per second, 3 meters
  + Full speed - 12 megabits per second, 5 meters
* **USB 2.0**
  + 480 megabits per second, 5 meters
  + A/B/Mini/Micro Plugs
* **USB 3.0 Superspeed**
  + 5 Gigabits per second, 3 meters
  + A/B/Micro Plugs
* **Firewire IEEE 1394**
  + Daisy chain up to 63 devices
  + 4.5 meters per link
  + **FireWire 400 - Alpha Mode - 1394a**
    - 100/200/400 Mbit/s half-duplex
  + **FireWire 800 - Beta Mode - 1394b**
    - 800 Mbit/s full duplex
    - Optical up to 100 meter
* **SATA 1.0**
  + 1.5 Gbit/s 1 meter
* **SATA 2.0**
  + 3 Gbit/s 1 meter
* **SATA 3.0**
  + 6 Gbit/s 1 meter
* **eSATA**
  + 2 meters, matches internal sata of device
* **DB-15 - VGA**
  + Analog only, 5-10 meter range
* **HDMI - High Definition Multimedia Interface**
  + Digital, 20 meter range
  + 19 pin Type A connector
    - Proprietary
  + MiniHDMI Type C connector
  + 4-14 Gbps depending on type (1.0 = 4, 2.0 = 14)
* **DVI - Digital Video Interface**
  + Single Link
    - 3.7 Gbps HDTV at 60fps
  + Dual Link
    - 7.4 Gbps HDTV at 85fps
* **Digital Toslink**
  + Oldschool consumer grade fiber
  + 10 meters
* Go look at Network Plus connects for RJ11, RJ45, etc
* **Thunderbolt - High Speed Serial Connector**
  + Based on mini-display port
  + V1 = 10 Gbit/s
  + V2 = 20 Gbit/s
  + V3 = 40 Gbit/s
  + 3 meters on copper, 60 meters on optical
  + Supports daisy chaining

### Wireless

* **Infrared -IrDA**
  + 4Mbit/s, line of sight
  + 1 meter
  + Laptop, phone, camera
* **NFC - Near Field Communication**
  + 106, 212, 424, kbit/s
  + 10cm range (3.9 inches)
* **Bluetooth**
  + Class 1
    - 100 milliWatts (mW) 100 meter range
  + Class 2
    - 2.5mW 10 meters
  + Class 3
    - 1 mW, 1 meter
  + V1 - 1 Mbit/s, V2 - 3Mbit/s, V3 24Mbit/s, V4 - 24Mbit/s (lower power)
* 802.11 - see networking details.

# Computer Power

### Connectors

* **SATA Power**
  + 15 pins, includes +3.3V, +5V, and +12V
* **Molex connector**
  + 4 pins, +12V, +5V
  + Storage devices, drives, fans, peripherals.
* **4 pin ATX +12V**
  + Older mobos, primarily for CPU
* **8 pin EPS +12V power**
  + EPS12V
  + 4+4 connector (Not the same as PCI express!)
  + Powers multiple CPUs, mostly on servers
* **PCIe 6-pin, 8-pin**
  + Additional power for PCIe
  + 6pin 75 watts, 8 pin 150 watts
  + Primarily for GPU
  + Often 6+2 pins
* **20-pin and 24-pin mobo power**
  + +3.3v, +/-5V, +/-12V
  + 20 pin was Original ATX standard

### PSU Specifications

* **Amp -** rate of electron flow per second
* **Voltage** - electrical “pressure” pushing the electrons
* **Watts -** Volts \* Amps
* **AC** - Alternating Current
  + Great long range efficiency.
  + 110-120 volts and 60Hz in NA
  + 220-240 volts and 50 Hz in Europe
* **DC - Direct Current**
* **Voltage Rails**
  + **Single Rail**
    - One 12 volt rail power supply
  + **Multiple Rails**
    - Each output on PSU has separate 12v rail
    - Additional protection from multiple rails - overloads won’t smoke up
* To identify the size of the PSU you need, just add up the watts of every device you want to connect, and then double that.
  + Modular PSUs are better so you don’t have unnecessary cables connected

# Devices

## Printers

Nah

## Laptops

* Express Cards
  + Come in 34 mm/54mm
  + External slotted expansion
  + Can connect to USB 2.0 bus (480Mbit/s), USB 3.0 bus(5Gbit/s), or PCIe bus(2.5Gbit/s)
* SO-DIMM - Small Outline Dual In-LIne Memory Module
  + Laptop sized memory
* Everything else can be connected via USB adapters pretty much
* Smart Card reader - A security card reader built into your laptop

## Displays

* **TN LCD - Twisted Nematic Liquid Crystal Display**
  + Very fast response time and low power draw
  + Poor viewing angle
* **IPS LCD - In Plane Switching LCD**
  + Great color representation, but more expensive than TN
* Backlighting
  + **CCFL - Cold Cathode Fluorescent Lamp**
    - Old school, high voltage, thick.
  + **LED backlit LCD displays**
    - LEDs… light the display
* **OLED**
  + Organic LED
  + Fades over time
  + Light, flexible, no glass needed
  + Doesn’t require backlight
* Wireless and bluetooth antennas often wind around the display

## Mobile Devices

Ugh god its cellphones and tablets. Did you know they have cases? Have you heard of bluetooth?

Go research NFC. Leave me alone I can’t take notes on dumb things like this.

# Hardware Troubleshooting

## Basic Windows Utilities

* Windows XP Mode
  + Available in Windows 7, allows for full virtualization of Windows XP through Windows Virtual PC
* Administrative Tools
  + Basic tool set for administrators and advanced users
* Windows Defender
  + Shitty antivirus
  + Basically called Windows Security Center in Vista
* Action Center
  + 7/8/8.1
  + Monitors both security and maintenance tasks
* Event Viewer
  + Logs events
* Windows Aero
  + Defines how the windows and UI look and feel (7/Vista)
* Modern (Metro) UI
  + Replaces Windows Aero in 8/8.1

## Transferring Windows OS

* Windows Easy Transfer
  + Allows you to move user data from one computer to another in Vista, 7, and 8
* Can only “in-place upgrade” from 7 to 8
* Windows 7 Upgrade Advisor
  + Gives info about future software compatibility and what to do to preserve data and functionality after windows 7 upgrade
* Windows Upgrade Assistant
  + Checks compatibility for in-place upgrades (7/8)
  + Checks hardware compatibility with new OS for old pcs (xp, vista)