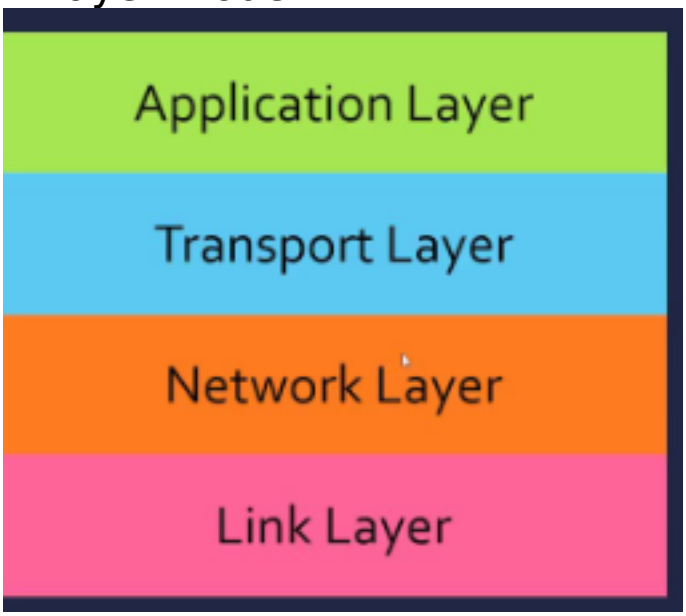
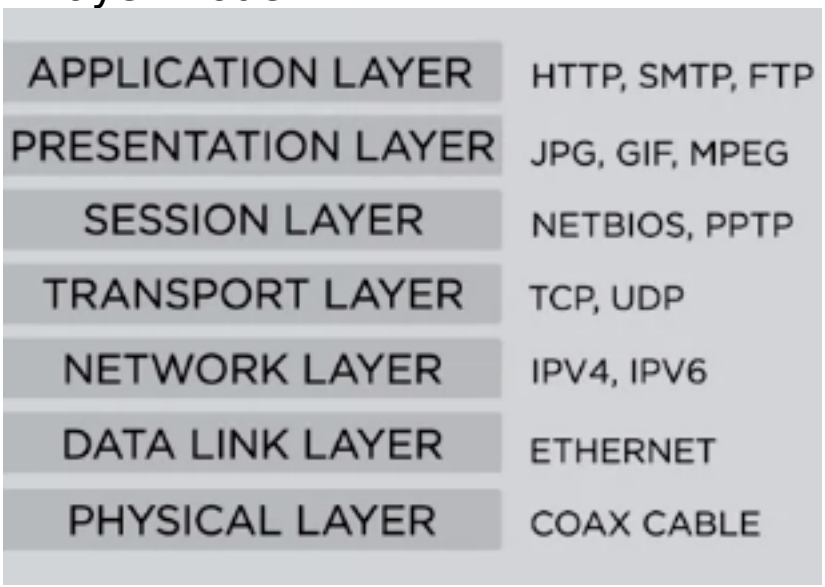
Networking Notes

4 Layer model:



Acronym for 4 layer model:
- Linus Never Talked Again
- Link Layer, Network Layer, Transport Layer, Application Layer

7 Layer Model:



Acronym for 7 layer model:
- Please Do Not Throw Sausage Pizza Away
- Physical, Data Link, Network Layer, Transport, Session, Presentation, Application

Basics

Cabling

Cabling:

- There are 3 modern ways to interconnect devices so they can transmit data which are:
  - Copper wires within cables
  - Fiber optic cables
  - Wireless transmissions

Twisted-Pair Copper Wire:

- Twisted-pair (TP) are wires grouped in pairs & twisted together to reduce interference (though interference is still possible)
- TP is used by modern ethernet
- TP cables are the most commonly used cable types in networking
- TP cables are color coded
- TP cables are inexpensive so they're commonly used in schools & homes
- TP uses electric pulses for data transmission (like all copper cables)
- Crosstalk (which is a type of interference) can occur when cables are bundled together for long lengths, the electric impulses from 1 cable can cross over to an adjacent cable. This occurs most frequently when cables aren't properly installed. When data transmission is corrupted due to interferences of any kind, the data must be retransmitted, this process can degrade the data carrying capacity of the medium.
- There are 2 common types of TP cables:
  - **Unshielded TP (UTP)** - Common in NA & inexpensive offering high bandwidth & an easy installation. It can come with many different numbers of pairs inside the jacket but the most common # is 4. Each pair being color coded.
  - **Shielded TP (STP)** - Common in EU & expensive but offers protection against interferences (EMI & RFI), recommended where interference is high. Difficult to install, not flexible.

Coaxial Cable:

- Coaxial cables are normally made of either copper or aluminum
- Used by service providers for TV as well as connecting various components which make up satellite communication systems
- Coaxial cables have a single rigid copper core which conducts the signal & the core is typically surrounded by a layer of insulation.
- Coaxial cables transmit data in electric pulses like all copper cables
- Coaxial cable provide improved shielding compared to UTP & therefore can carry more data but coax is difficult to install, pricy & harder to troubleshoot compared to TP so TP has been used as a replacement to coax.

Fiber-Optic Cables:

- Fiber-optic cables are made of either glass or plastic with the same width size as a human hair
- Fiber-optic cables have high bandwidth (ability to carry large amounts of data at the same time) & are normally used by large enterprise environments & data centers.
- Fiber-optic transmits data via light pulses instead of electric which means EMI won't affect it.
- Fiber-optic cables are more resistant to outdoor environment conditions than copper cabling which makes it a good choice for extending networks from 1 building to another.
- Fiber-optic cables can reach distances of several miles or kilometers before the signal needs to be regenerated.

Copper Termination Standards

Wiring Standards:

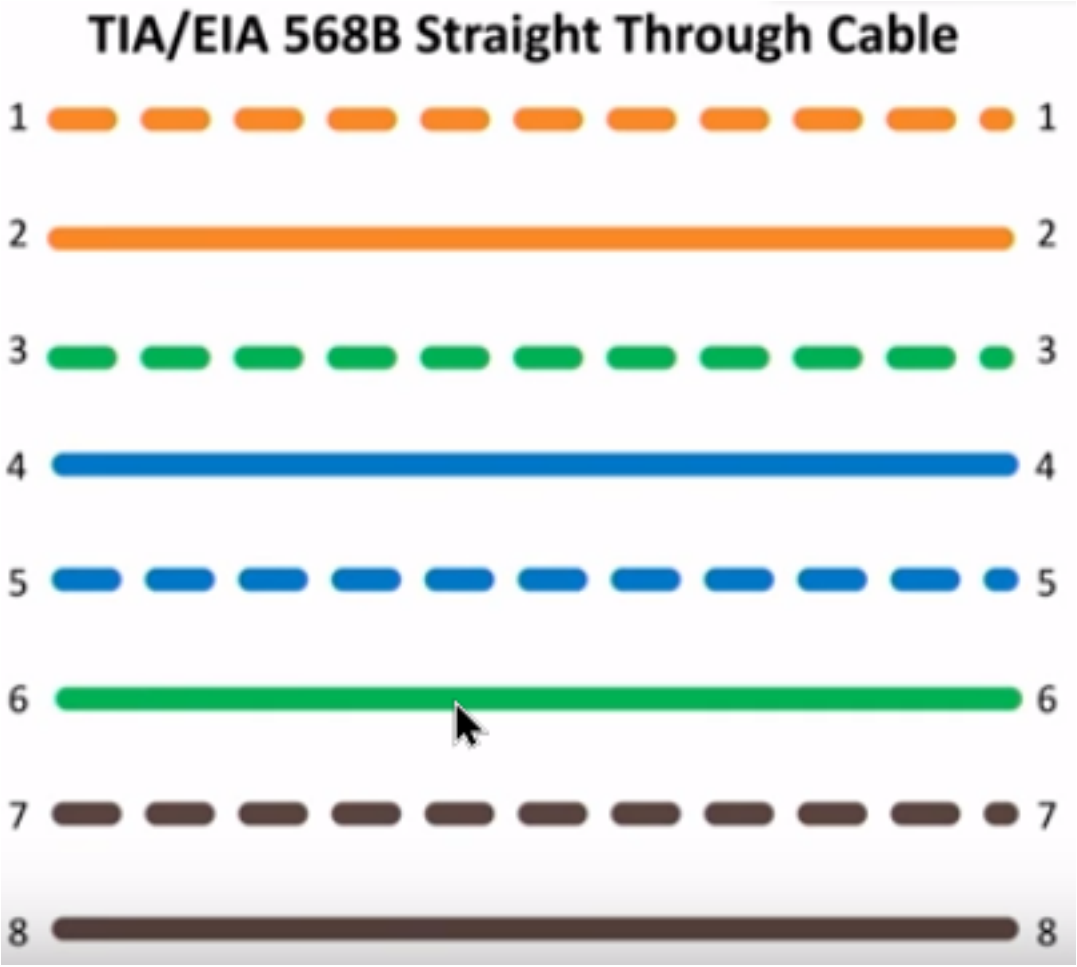
• Cables can foul up a perfectly good plan which is why they should be tested prior to implementing them

T568A & T568B Termination:

• When terminating copper cables, you can choose from 2 standards which are the T568A & the T568B standards, if you choose 1 then you have to stick w/it throughout your cable installation.
• It doesn't matter which standard you use, what matters is you stay consistent in regards to your choice.
• DO NOT terminate 1 side of the cable with 568A & the other with 568B, you'll run into problems.
• Many organizations traditionally use the 568B standard for termination.

Straight-Through Cables:

• AKA patch cables, they're the most common Ethernet cables
• Connect workstations to network devices (such as switches)



Ethernet Cross-Over Cables:

• When connecting like devices to each other, cross-over cables are used
  ■ Connecting MDI to MDI
  ■ Connecting MDI-X to MDI-X
  ■ Connecting workstation to workstation
  ■ Connecting switch to switch
• In some cases, performing the cross-over inside the cable isn't necessary but instead you perform the

crossover inside the device you're using which is called Auto-MDI-X
• Auto-MDI-X is on most modern ethernet devices & it automatically decides to cross-over via detection
• Ethernet crossover doesn't deal with 568B or 568A standards, it isn't related to a termination standard

Network Termination Points

110 Block:

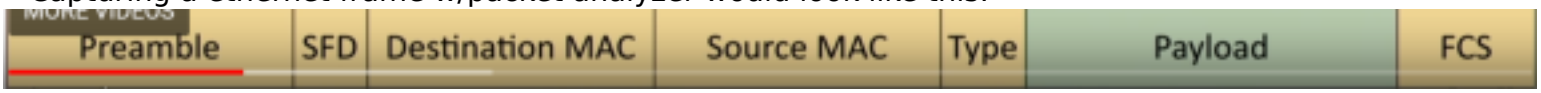
• 110 Blocks are primarily connected to “patch panels” which are used to connect people from their desk or workstation through to the closeted networking area. How it works is the patch panel which has the 110 block is connected to the switches & cables are left in place between the desks & the patch panel, if someone moves the cable is plugged into differnet switch & if someone new is hired, a new cable would be added to the patch panel through to the networking equipment.
• Wire-to-wire patch panel
• Replaces the older 66 block & allows for higher speed networks to be connected so cat5 & cat6 cables can now be plugged in to this 110 block.
• Wires are “punched” into the block & connecting block is placed on top. Any additional wires are punched into the connecting block

Ethernet

The Ethernet Frame

The Ethernet Frame:

• Capturing a ethernet frame w/packet analyzer would look like this:



• **Preamble** - An alternating number of 1s & 0s that lets the receiving system know that the info that's about to arrive is part of an ethernet frame
• **Start Frame Delimeter** - A specific set of 1s & 0s that tells the receiving system that everything after this point is part of the communication
• **Type** - Describes whats inside the frame (**EX**: IPv4 traffic)
• **Payload** - Whatever is being sent to the destination
• **Frame Check Sequence** - Part of every ethernet frame which is a CRC checksum that's generated from all the data sent in the frame. When the receiving system receives data, it calculates the checksum independently & compares it to the FCS, if it's a match the data was received correctly but if it doesn't, it indicates corruption & the frame will be dropped.

Duplex

Half-Duplex:

• A device configured this way cannot send & receive data at the same time.
• All LAN hubs are half-duplex devices.
• Switches are normally configured in full-duplex but can be configured in half-duplex

Full-Duplex:

• Data can be sent & received at the same time.
• Both the switch & the end station (or end user) have to be configured for full-duplex to work properly.
• Collision isn't possible with full-duplex.

Half-Duplex Ethernet:

• Traffic sent to another device on the same hub would be broadcasted to all other devices on the same hub since hubs don't have a way to intelligently forward traffic.
• If 2 devices communicate/send data simultaneously, you have a collision. When collisions occur, every device connected to that network knows a collision occurred & waits a random amount of time (this amount of time being unique for every device) & then tries to communicate/send data again.

Full-Duplex Ethernet:

• On a switch network, the switch intelligently determines where to route traffic instead of broadcasting it like a hub.
• Once data is received, the switch resolves the destination MAC address on the data to determine the IP of the destination.

Wireless Network

CSMA/CA:

• Used on wireless networks
• CA - Collision Avoidance
• Collision detection isn't possible in wireless networks due to not being able to listen for data when transmitting data.
• Wireless networks use **RTS** (Ready To Send) & **CTS** (Clear To Send) where a device communicates with an access point & tell it it's RTS & the access point will grant access to that specific device to send data & only that device can send data in a specific time frame.
• RTS & CTS solves the “hidden node” where 2 devices cannot hear/communciate w/each other but can hear/communicate w/the access point.

Peer-to-Peer Network

Small Peer-to-Peer Network:

• A peer-to-peer network contains computers that run both clients & server software at the same time.
• Small peer-to-peer networks consist of 2 computers connected to each other through wired or wireless connections, these computers can then exchange data & services w/each other.

Large Peer-to-Peer Network:

• Multiple PCs can be connected to create a larger peer-to-peer network but this requires a network device (such as a switch) to connect the PCs

Advantages of Peer-to-Peer Network:

• Easy setup
• Less complex
• Lower cost due to no need for network devices & dedicated servers

Disadvantages of Peer-to-Peer Network:

• The main disadvantage of a peer-to-peer is the network performance is slown down for a host if it's acting as both a client & a server at the same time (delivering & requesting information)
• No centralized administration
• Not as secure
• Not scalable (cannot expand if needed unless you buy more PCs)

MAC Addresses

MAC Addresses:

• 48 bits/6 bytes long
• 2 parts:
    • **Organizationally Unique Identifier (OUI)** which is associated w/the manufacturer. By looking at the OUI, you should be able to identify the manufacturer. (The first half)
        ■ **Network Interface Controller-Specific** (the serial number) (the last half)

Summary of Network Switching

Summary of Network Switching:

• Switches are responsible for forwarding or dropping frames.
• **Switches intelligently update their lists of MAC addresses when they forwards traffic**, this list is based on the source MAC address of traffic (when forwarding traffic, it takes note of the source MAC & location so it can better handle any future traffic addressed to that same MAC address).
• Switches maintain a loop-free environment by using STP (Spanning Tree Protocol).
• When there are 2 switches in a network, neither know what MAC addresses are in the other's address table in other words, they work independently.

Learning the MAC Addresses:

• Switches examine incoming traffic to make a note of the source MAC Address, then it fills out their table if it doesn't already have that MAC address.

Flooding For Unknown MAC Addresses:

• When the switch doesn't have the destination MAC address in the table, it first examines the source & takes note of it in the table. Then it sends the packet to everyone in the network to find the destination, if the packet isn't addressed to their MAC address, their ethernet adapter will drop the packet (although, this can be circumvented via promiscuous mode).

Broadcast Domains & Collision Domains

Collision Domains:

• Relevant only when half-duplex was in place (not relevant anymore)
• Collision domains were the normal process when people are trying to communicate on a network, it was common & not a bad thing. The reason for this was everyone was practically connected by the same coax cable via ethernet (like a peer-to-peer network) but with hubs all the wires were sent to 1 device but still every device heard the other devices communicating.
• When hubs were still in place, everyone heard everyone's signals & when other people sent data at the same time collisions occurred & no one could interpret the data sent.
• Switches w/full-duplex communication removed collision domains.

Broadcast Domains:

• Things such as ARP requests (resolving MACs to IPs), OS notifications, some dynamic routing protocols, etc are broadcasted to everyone on the network. Bridges/switches pass the broadcast to everyone on the switch while routers won't do anything w/the broadcast once it gets it.
• Technically, you can block a broadcast by implementing a router in the network.

Protocol Data Units

PDU:

• A unit of info that is sent by a protocol at a particular OSI layer (EX: A switch operating at the Ethernet PDU, the PDU tells the switch where to forward that frame).
• For TCP , the PDU is a TCP segment
• for UDP, the PDU is a UDP datagram

MTU (Maximum Transmission Unit)

• The size of the PDU is determined by the MTU
• Determines the max size of IP packet to transmit without fragmentation
• fragmenting slows things down & losing the fragments along the way of being sent causes all the fragments to be sent even if only 1 fragment was lost.
• Sizes are usually configured once

Network Segmentation

LANs:

• In a LAN there are 2 separate switches & 2 different broadcast domains.
• Devices that are connected on 1 switch cannot communicate w/devices that are connected on the other switch (unless the traffic is routed between the different LANs)
• It's difficult to scale (size up) (having 100s of thousands of networks that need segmenting will be difficult to manage if you did segment them)

VLANs:

• The separation in VLANs is in the same 1 switch to segment the network. The separation isn't physical but logical hence virtual
• The devices are still in separate broadcast domains & the devices still cannot communicate w/each other if they are in separate VLANs as there is a logical separation.
• It's possible to configure multiple VLANs on a single switch.
• The only way for the devices in the different VLANs to communicate w/each other is if you route the

traffic between the differnet VLANs. (this doesn't just go for VLANs, it applies also to LANs)

802.1Q Trunk:

• This is a protocol that's used if you need 2 devices on different VLANs to communicate w/each other
• With the .1Q trunk protocol, a normal ethernet frame has an added piece called the VLAN frame which specifies which VLAN to send the packet to.

Spanning Tree Protocol (STP)

Spanning Tree Protocol (STP) (AKA 802.1D):

• If you connect 2 switches together & there isn't any loop protection, you create a loop with the 2 cables which forces the switches to send traffic back & forth forever.
• To stop looping once it has began, you need to pull a cable from 1 of the switches.
• Spanning Tree Protocol (STP) is the network protocol used to protect against this looping
• If looping isn't stopped, it has the ability to bring down the network by overwhelming it.
• To fully prevent looping from occuring, implement 802.1D or Spanning Tree Protocol (STP)

STP Port States:

• **Blocking** - The switch believes if it continued to forward traffic then a loop would've occurred so it instead blocks traffic from going through that port.
• **Listening** - The switch isn't passing/forwarding traffic but it's listening for other devices to then learn & add the MACs to its table.
• **Learning** - This is where the switch still won't forward traffic but rather add the MACs it was listening for to its table.
• **Forwarding** - Once traffic is allowed through the port, it begins passing/forwarding it through.
• **Disabled** - This is where the port has turned off which means traffic can no longer go through this port.

Rapid Spanning Tree Protocol (RSTP):

• The latest standard (802.1w)
• Faster convergence (STP took 30-50 sec while RSTP takes only 6 sec)
• RSTP is just faster than STP.
• RSTP & STP can both be existing on the same network.

Longest Prefix Match

Longest Prefix Match:

• Since Internet routers can have many links, the Longest Prefix Match determines which link to forward a packet over.
• LPM is the algorithm IP routers choose to compare entries for the destination in the packet & from the routing table

TCP Service Model

TCP:

• Part of the transport layer
• Connection is established via 3-way handshake (SYN, SYN/ACK, ACK)
• Provides a reliable byte delivery service between 2 applications
• TCP ensures reliable delivery of packets by:
    1- Ack packets which indicate correct delivery.
    2- Checksums which detect if data is corrupted (just like a hash)
    3- Sequence numbers that detect if any data is missing (these sequence numbers indicate how many packets to expect & if packets arrive out of order, these sequence numbers can be used to put them back in order)
    4- Flow-control prevents overrunning/overwhelming of the receiver/destination (like a DoS attack, sending data to the point where the receiver cannot keep up)
• TCP delivers data in the correct sequence (TCP will send data the same way it was sent). If the data arrives out of order, TCP will correct the order using the sequence numbers.

Connection Teardown:

• There is a 3-way handshake-like method of “tearing down” a connection:
    ■ The client sends a “Fin” packet
    ■ The host's response is a Data + Ack packet (the data signifies the last bit of data to be sent to the client to close the connection)
    ■ The host then sends the “Fin” packet to indicate the closing of the connection
    ■ The client responds with an “Ack” packet to acknowledge the closed connection.

TCP Segment Format

TCP Segment Format:

• The **destination port** tells the tcp layer where the data should be delivered to.
• The **source port** tells the tcp layer which port should be used to send data back again if needed (**EX**: When requesting a web page). When a user starts up an application/connection, a unique source port is auto generated (there are lots of ports reserved for this purpose) & this is where that port goes.
• The **sequence number** indicates where the first piece of data/byte is (**EX**: If the first sequence number is 1,000 & this is the first byte/piece of data, then the sequence number is starting at 1,000)
• The **acknowledgement sequence #** tells the other end which byte/piece of data to expect next. It also indicates that every byte before the acknowledgement sequence # has been recieved successfully (otherwise, the sequence number wouldn't be changing).
• **Checksum** (Helps detect corrupt data, like a hash).

UDP Service Model

UDP:

• UDP is simpler than TCP due to it being unreliable it should only be used by applications that don't need reliable delivery (such as simple request & response applications: DNS or NTP). Some other applications use UDP due to them having their own special needs for retransmission, congestion control & sequencing datagrams.
• UDP takes application data & creates a UDP datagram, then hands it to the Network layer. The datagram identifies the application that the data should be sent to at the other end.
• The UDP datagram is encapsulated inside the data field of the IP datagram
• Unlike TCP which has over 10 fields, UDP only has 4 fields.
• The 16 bit length field specifies the length of the whole datagram (header + data) in bytes.
• The UDP checksum is optional when using IPv4, if it's not included, it autofills with all 0s. But when it is filled, it calculates the checksum of the UDP header & data. When calculating the checksum, it even

includes part of the IPv4 header as well.
• The reason for the UDP datagram checksum using part of the IP header is that it allows the UDP layer to detect datagrams that were delivered to the wrong destination.
• The UDP service is indeed small due to the service it offers being simple, providing a simple message protocol for sending data from an application from one host to another application that may or may not be delivered (remember, it's unreliable) to another application on a remote host.

UDP Properties:

• Connectionless - No connection established
• Datagram Service: Packets may show up in any order so if application cares about in-sequence packets, it needs to re-sequence packets itself.
• Unreliable delivery:
    ■ No acknowledgements to let sender know data reached receiving end
    ■ No mechanism to detect missing or out of sequence datagrams
    ■ No flow control

UDP: Port Demultiplexing

UDP: Port Demultiplexing:

• Port numbers in UDP work the same as they do in TCP
• Many people refer to UDP as just a Demultiplexing mechanism which divides up the stream of UDP datagrams & sends them to the correct process.

ICMP Service Model

ICMP Service Model:

• Internet Control Message Protocol is used to report errors & diagnose errors at the Network layer
• ICMP runs above the network layer in the 4 layer model & technically it's a transport layer protocol
•**EX** of error message ICMP - “Destination network unreachable”
• ICMP sends a reporting message which is a self-contained message reporting error but it's unreliable as it uses a simple datagram service with no retries.

Making the Network Layer Work:

1. The Internet Protocol (IP)
    ■ The creation of IP datagrams
    ■ Hop-by-hop delivery from end system to end system
2. Routing Tables
    ■ There are algorithms that populate router forwarding tables which instruct instruct routers on how to deliver packets hop by hop to the destination.
3. ICMP
    ■ Helps communicate network layer info between end hosts & routers
    ■ typically used to help us diagnose problems
    ■ Reports error conditions

ICMP Message Types

ICMP Message Types:

ICMP Type	ICMP Code	Description
0	0	Echo Reply (used by ping)
3	0	Destination Network Unreachable
3	1	Destination Host Unreachable
3	3	Destination Port Unreachable
8	0	Echo Request (used by ping)
11	0	TTL Expired (used by traceroute)

• Note: You do not need to remember these, just good for reference
• **Destination host unreachable** - Occurs if the datagram gets to the last router before the host but the router doesn't know where the host is located.
• **Destination port unreachable** - The port that's inside the datagram isn't recognized on the receiving end host/system.
• **Traceroute** - Uses ICMP as well, the goal being to find the routers on the path from the source to the destination IP address while measuring the round trip time while doing so. It sends UDP messages that are encapsulated into an IP datagram (what's inside the datagram doesn't matter) with a TTL set to 1 from the source to the 1st router, the router decrements the TTL & sends back a TTL expired message back to the source address. The source now knows that that's the first hop & it knows from measuring the time it took from when it sent the original message to when it received the TTL expired message, it now knows the round trip time to that router. The source also knows the IP of the first hop since the router has to attach it's address when sending the TTL expired message. This is done again but the TTL is incremented by 1 (it's incremented by 1 each time). The UDP message that's being sent is using an odd port number to purposely trigger a ICMP PORT UNREACHABLE message back to the source, when this occurs then the source knows that the traceroute made it to the destination & is complete (the reason for it using an odd port number is because the packet only gets forwarded to the port once it is at the destination address).

Prioritizing Traffic

Prioritizing Traffic:

• Since there are many devices & many applications on these devices running we have different applications that may be considered “mission critical”.
• Different applications have different network requirements such as voice being real-time while streaming vids have a buffer & so on. Due to all these different devices & different needs for the applications, we understand that some applications are “more important” than others so we need to set a priority on some applications/traffic over other traffic.

Packet Shaping:

• Packet shaping or traffic shaping is a way to prioritize traffic, it allows you to control bandwidth usage or data rates for certain applications so you can set important applications to have higher priorities over other applications.
• There are many differnet ways to set this up, it can be implemented through a firewall, a router, or a switch.

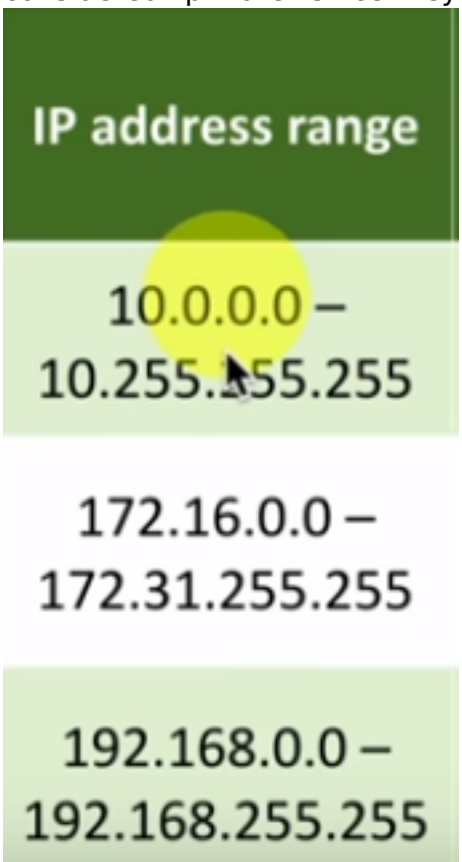
Quality of Service (QoS):

• This describes the process of controlling traffic flows (prioritizing traffic performance)
• There are many different ways to implement QoS but there are certain standards such as:
    ■ **Class of Service (CoS)** - you can configure in an OSI Layer 2 network & this is a type of prioritization that is performed inside the Ethernet frame header in an 802.1Q trunk so it's specific in communications between switches. CoS is commonly performed in the internal network.
    ■ **Differentiated Services (DiffServ)** - Implemented through OSI Layer 3, the bits are modified within the IPv4 header & are usually set outside the application so a device would recognize the application (the device can be a router) & once it recognizes the application, it sets the appropriate amount of bits (bits = data type)
    ■ **DSCP (Differentiated Services Code Point)** - Set inside of the IP header in the differentiated service field.
• Note: In some environments both Class of Service & DiffServ could be taken advantage of to set priorities in your network.

Network Address Translation

NAT (Network Address Translation):

• Since there are no IPv4 addresses to assign then we have to use **NAT** in order to make the communication work given the restriction on IP addresses. Though, NAT can be used for much more.
• We knew ahead of time we'd run out of IPv4 addresses so we created certain addresses that are considered “private” since they cannot be routed across the Internet, below is a photo of these IP ranges.



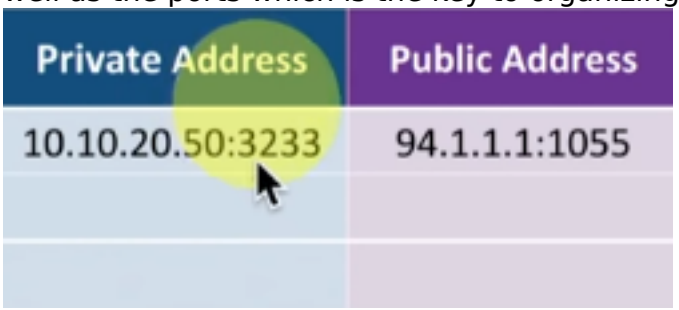
• These addresses are used inside an internal network & then we implement **NAT** to translate these private addresses into something that is a public address that can be routed over the Internet.
• NAT works just like a regular user attempting to connect to the internet except the router that connects the user, will see that the user is using a private IP address & change the source IP in the packet to something that is routable to the internet (**EX**: the router's own external IP) & when a response comes

back then the packet reaches the router & looks up in the table the IP of the user who originally requested the packet & performs another NAT to finally get the packet back to the original user.

NAT Overload/PAT

NAT Overload/PAT:

• Since in a company's internal network there are normally more than 1 device using private IPs that need to connect to the internet then NAT overload (aka Port Address Translation) is used for Network Address Translation.
• How NAT Overload/PAT works: It works like a normal user attempting to connect to a webserver, the user's system reserves a port to receive back data & its source IP & fills out the destination IP in the packet & sends it to the router & the router realizes it needs to perform a NAT & inside the router is a NAT table where it keeps track of all the private addresses translated into public routable addresses as well as the ports which is the key to organizing what data to send back to who (see img for example).



Port Forwarding

Port Forwarding:

• Another type of NAT, sometimes referred to as a Destination NAT or Static NAT due to the public destination IP address is being translated to a private IP address no matter what, it doesn't change hence “static”.
• Since this NAT is “static”, it doesn't timeout or expire. It's available 24x7.
• Found on routers
• allows someone on outside to gain access to internal devices so if someones hosting a web server & that device is using a private IP address then port forwarding would be used to take the external communication & allow access to that internal private IP (note: just BC it's called port forwarding doesn't mean only ports can be mapped to IPs, it goes both ways)
• To do so, you need to take an external IP/port number and map it to an internal IP/port, it doesn't have to be the same port.

End-to-End Principle

End-to-End Principle:

• Refers to 2 principles,
    ■ The first deals w/**correctness** (if you don't follow the end-to-end principle when designing network systems, the chances are it has a flaw & may transfer data incorrectly). In this principle, things can be implemented while in transit (or in other words, in the middle) & on end to end systems.
    ■ The 2nd is called the **strong** end-to-end principle is much more general. This principle states to only implement things from end to end systems, nothing in the middle transfer route. The reasoning for this principle is flexibility & simplicity.
• **The end-to-end principle overall refers to why the network doesn't do more to help** (**EX**: auto

compressing files to help fasten the transfer rate or auto encryption).
• Summarizing the end-to-end principle, the network can help you but you can't depend on it, so for example say you want an application to automatically have end-to-end security so you look to the network to have this option, well in this case this security can only be done correctly by the application itself so making it a “feature of the network" isn't possible.
• The reason why end-to-end checks in terms of validating the integrity of files from end user to end user is more efficient instead of verifying it along the route is because if any computers or devices along the route have corrupted memory & that file is moved into memory & the file becomes corrupt, then the next destination wouldn't be able to do an integrity check since these aren't performed on anything sent from memory, plus the integrity check was already performed.. This is the idea of correctness, the network can help ensure integrity is valid from source to final destination but it shouldn't be relied on.
• Another way to view the end-to-end principle is that you have to perform actions from end system to end system, you can do things in between but those things that occur in between shouldn't be relied on. These “things” include things like integrity checks, file compression, etc

Error Detection

Error Detection:

• Networks today usually use 3 different detection algorithms:
  ■ Checksums
  ■ CRC (Cyclic Redundancy Codes)
  ■ MAC (Message Authentication Codes)
• Ethernet appends a CRC to the end of the data for integrity checking (placed in the footer)
• TLS appends a MAC to the end of data for integrity checking (placed in the footer)
• IP prepends a checksum (places it in the IP header)
• The only way a layer can be sure it communicates data correctly is to perform an end to end check (related to the end-to-end principle)

Error Detection Algorithms:

Checksum:
• Adds up all data in the packet (what TCP & IP use)
• Very fast, not resource intensive to compute, even in software
• Not very robust (pretty weak error detection guarantees, easy to fool checksum)

Cyclic Redundancy Code (CRC):
• Computes remainder of a polynomial which is easy on today's hardware (used by Ethernet & many link layers)
• More expensive than checksum in terms of being resource intensive (easy today, easy in hardware)

Message Authentication Code (MAC):
• Combines packet with cryptographic technique to generate a value (like symmetric encryption)
• Robust to malicious modifications, but not robust to errors
• Messages have a chance of collision (having the same code)

Checksums

Checksums:

• IP, UDP, & TCP use 1 one's complement checksum which means they add up the data using one's complement arithemtic (just a version of binary older computers used)
• **Benefits**: fast, easy to compute & check.
• **Drawbacks**: Poor error detection so it only guarantees detecting a single bit error. It can detect other

errors but actual guarantees are both weak & complex.

Cyclic Redundancy Check (CRC)

Cyclic Redundancy Check (CRC):

• CRC designed to detect certain forms of errors: stronger than checksum
    ■ Can detect if there is an error in any message with an odd number of bit errors, 2 bit errors, or any single burst of errors equal to or less than “c” bits long. CRCs can't guarantee detecting errors besides these.
• Link layers typically use CRCs due to fast computing in hardware, CRCs can be computed incrementally as you read/write the packet, & since CRCs have good error detection for physical layer burst errors.

Message Authentication Code (MAC)

Message Authentication Code (MAC):

• Uses cryptography for mathematical purposes (beyond the scope of this)
• MAC doesn't have as good error detection as CRC but it protects against malicious threat actors in terms of modification. It's primarily a security mechanism
• MAC cannot guarantee detecting any errors

Circuit Switching

Circuit Switching:

• Circuits are established between endpoints prior to data passing (like a phone call where the other person needs to pickup before data can pass)
• If the circuit is in use & even if it's idle (still in use, technically), nobody else can use it which is quite an inefficient use of resources.

Circuit Switching:

• Technically, a telephone service is a circuit switching network, it's referred to as a POTS (Plain Old Telephone Service) or a PSTN (Public Switched Telephone Network)
• A T1 is another type of circuit switching network, it creates a circuits between 2 sites. That circuit is always there once established until it is explicitly disconnected

Packet Switching:

• Packet switching is when data is grouped into packets & then sent (this data can include voice communication, video streams, etc)
• This info is sent over a network which is shared w/everyone else so someone else can use it even if you aren't using it & are just idle, unlike in circuit switching.
• Packet switching also supports Quality of Service (network prioritization) so 1 person can have higher bandwidth than others.
• Connections such as SONET, ATM, DSL, Frame Relay, MPLS, Wireless, Cable modems & Satellite can be considered packet switched networks.

Software Defined Networking (SDN)

Software Defined Networking (SDN):

• Relatively new way to think of building & managing networks
• Networking devices have 2 functional planes of operation
    ■ **Data Plane** which is responsible for transferring data from 1 point to the 2nd
    ■ **Control Plane** which is responsible for administration & ongoing service of that device)
• A benefit of the SDN is that it's directly programmable, so since the data plane is completely separate from the control plane then you can make configuration changes & look at log info & it's a completely separate process from the data plane
• SDNs are **agile** which means changes can be dynamically (changes can be made any time)
• SDNs are centrally managed (like a SIEM). This type of management is called a single pane of glass
• An SDN can be programmatically configured how things occur on the network without the need for user interaction, **EX**: An SDN can be constantly monitoring part of the network & if the network needs resources then these resources can be deployed automatically.
• SDNs are vendor neutral so you don't have to have 100% of vendor's products
• The main reason SDNs are so useful is due to networks shifting towards virtualization.

Distributed Switching

Distributed Switching:

• Distributed switching removes the physical segmentation aspect with switches. It's done through virtualization. A virtual network distributed across all physical platforms.
• When a VM moves from one virtualization platform to another, the network configuration doesn't change, there isn't any impact due to it running in a distrbuted switching environment so technically servers will always connect to the right VLAN.

Networking Devices

Hub:

• Hubs are often referred to as “multi-port repeaters” since traffic that passes through 1 port is broadcasted to every other port meaning every device receives everyone's traffic since hubs don't have an intelligent way of forwarding traffic.
• Hubs are considered OSI layer 1 which is physical layer
• All devices are considerably sharing the network on hubs so you can't have full-duplex connections. All devices on hubs are running at half-duplex.
    ■ **Half-duplex** - can only send data or recieve data, cannot perform both at the same time. If both are performed at the same time, a collision occurs where devices detect a collision & each device waits a unique amount of time in order to send a retransmit data again.
    ■ **Full-duplex** - can send & receive data at the same time.
• The more devices on a hub, the larger the chance for collision which leads to it being less efficient as network speeds increase
• Hubs are only available for 10 mb/100 mb ethernet

Bridge

Bridge:

• A bridge is like a switch with 2-4 ports

• A bridge performs forwarding decisions in software based on the MAC addresses of what happens to be on both sides of the bridge (bridges connect different physical networks so hence both sides of the bridge)
• Bridges are used to connect 2 separate different physical networks, it connects different topologies. But it can also connect similar topologies to minimize the number of collisions that might be occurring.
• Bridges make forwarding decisions based on destination MAC addresses on ethernet frame. They are also a OSI Layer 2 device
• **EX of modern bridge**: Wireless access point where there is a wired ethernet network on 1 side of the bridge while on the other side is a wireless network.

Switches

Switches:

• Switches are an evolution from older style bridges since these are devices with 100s of interfaces instead of the 2-4 that you'd have on a traditional bridge.
• Switches make forwarding decisions in hardware using tech known as ASIC (Application-Specific Integrated Circuit)
• Switches are an OSI Layer 2 device, it forwards based on destination MAC address just like a bridge.
• Switches have many ports & features such as **Power over Ethernet** where you plug in a device to your switch & that device receives power directly from the network switch.
• Switches can be thought of as internal devices since they primarily communicate within the internal network but when multilayer switching is enabled, it also can communicate with the external network (routing between the different VLANs which are logically in a different network)

Multilayer Switch:

• This is where the switch routes not only with layer 2 but also layer 3 (routing) functionality where it routes between the different VLANs that are connected to the switch.
• Acts as both a switch & router, bundled as a single device

Router

Router:

• Forwards traffic between differnet IP subnet, making forwarding decisions based on the destination IP address in the IP packet
• Routers are layer 3 devices
• Routers can be thought of as being used to communicate with the extranet or the external network since they operate at layer 3.
• Routers can connect different types of network topologies

Firewall

Firewall:

• Firewalls make decisions on whether traffic is allowed or not allowed into a network based on OSI layer 4 information (TCP/UDP, could be a TCP/UDP port number).
• Modern firewalls can even look into the application that's going across the network to make the decision on whether certain applications are allowed in the network, these are referred to as Layer 7 firewalls or next generation firewalls.
• Many firewalls have additional abilities such as being able to act as a VPN endpoint at one location &

configure another firewall as a VPN endpoint at another remote site which would allow traffic as well as any data that flows from the main location to any remote site to be encrypted.
• Some firewalls can be configured as a proxy which is a common security technique
• Most firewalls can even be configured as a layer 3 device (network layer) so they can route all traffic going in & out of the Internet, here they make security decisions based on layer 4 TCP/UDP ports or layer 7 applications AND they even route traffic between different IP subnets (like a router in the case of routing traffic between different IP subnets)

Wireless Access Point (WAP)

Wireless Access Point (WAP):

• This isn't a wireless router
    ■ A wireless router is a router & a WAP in a single device but a WAP isn't a wireless router
    ■ A WAP is just the wireless part of a wireless router
• WAP is a bridge that extends the wired network onto the wireless network (on one side we have the wired network while on the other side we have the wireless network)
• WAP is an OSI layer 2 (data link layer) device

Modem

Modem:

• Named after modulator / demodulator function that the device performs.
    ■ Device converts analog sounds (sound waves & radio waves are analog signals so technically in this case they are transmitted through phone lines) to digital signals (this is how you move data through the telephone line)
    ■ You need a modem on both sides of the connection. **EX**: If devices in 2 locations needed to communicate, you could place a modem in both locations & the devices would be able to communicate via phone lines which have limited bandwidth for data.
• POTS modems now used for backup & utility functions

Converting Media

Converting Media:

• OSI Layer 1 (physical layer)
• Media converter is used to change copper network to fiber network or vice versa
• Media converter can also be used to extend a copper wire over a long distance where the copper is converted to fiber to extend it over the distance & then convert it back to copper.

Wireless LAN Controllers

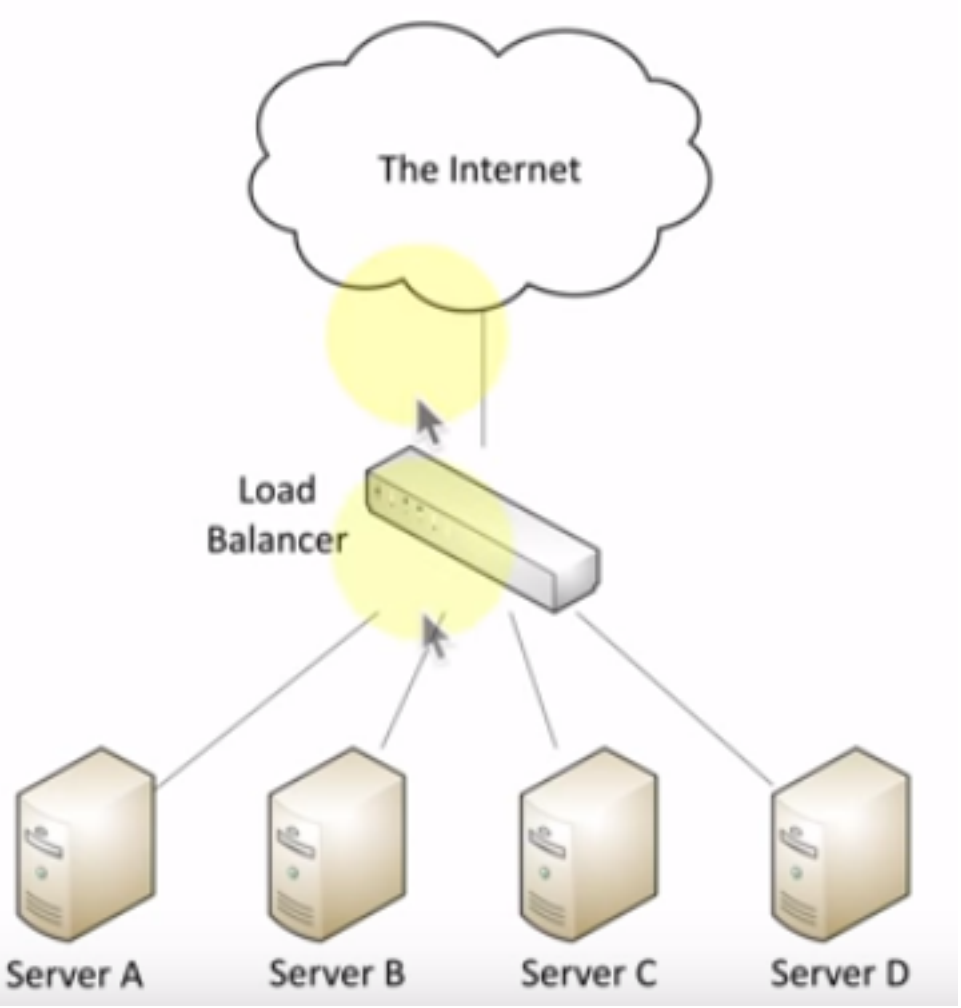
Wireless LAN Controllers:

• Centralized management of Wireless Access Points from 1 single console, AKA single “pane of glass”
• From this single controller, you can deploy new access points, constantly monitor wireless network, configure & deploy changes to all WAPs, & report on usage on the WAPs
• Wireless LAN controllers (aka the centralized management) are usually specific to the brand of access point you're using in your network, so if you're using Cisco WAPs in your network, you'd have to use a centralized Cisco management system.

Load Balancers

Load Balancers:

• Load balancers distribute the load to multiple servers & it is invisible to end-users
• Load balancers are used when a company provides a service to their users
• Load balancers are often used for large-scale implementations for web servers
• When load balancers are being implemented for fault tolerance there are usually multiple servers behind the load balancer so if 1 server fails, the load simply distributes among available servers.

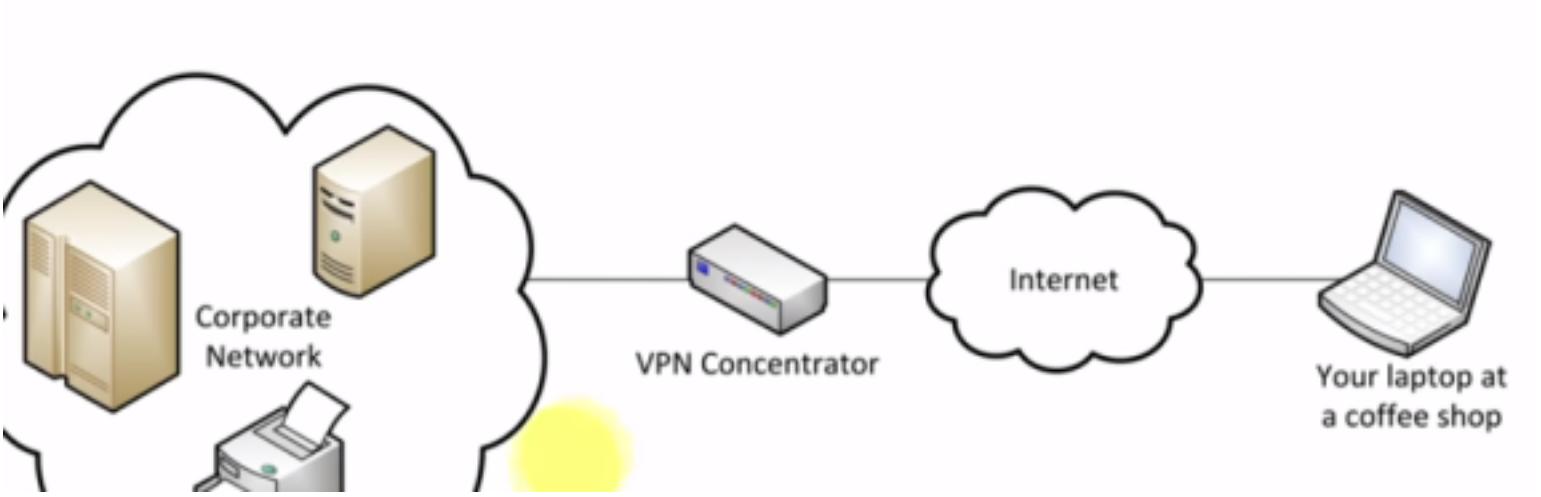


• The load balancer will normally monitor the responses from the servers so if 1 server begins to slow down, the load balancer could balance the load across the remaining servers.
• The load balancer could also handle all the intiation of TCP 3 way handshakes for intiating connections & then the servers don't have to deal with this which can free up resources
• Load balancers can also handle TLS offloading which is when TLS encryption connections are dealt with by the load balancer since encryption can be resource intensive.
• Load balancers can even be configured to cache responses so that way when a 2nd user asks for the same exact site/makes the same request as the 1st user did, the load balancer doesn't need to bother the servers for the response, it simply goes into its cache to retireve the request. This means the request doesn't take up resources plus a faster response for the user but I am sure the cache can be infected with malicious links (**EX**: A threat actor requests google.com & then performs an attack to gain access to the load balancer's cache and changes google.com's IP address to a malicious site's IP address so when people ask for google.com, the load balancer returns the malicious site)

VPN Concentrator

VPN Concentrator:

• A VPN concentrator allows support for VPNs. It allows someone on the outside to communicate through encrypted form to the internal network. When the concentrator recieves that encrypted connection, it decrypts the connection/data & puts it on the intranet/internal network. Any data sent back to that same user would be encrypted by the concentrator & sent back to the user.
• The concentrator can be a stand alone device or it can also be implemented into the firewall. And instead of using dedicated hardware, you can even use specialized software on a dedicated server to implement it.
• On the end user's device software would be needed to communicate with the VPN concentrator, this is sometimes built into the OS.



AAA (Authentication, Authorization, Accounting (logging)) Network

Identification:

• This is who you claim to be such as through a username or email

Authentication:

• Prove you are who you claim to be
• Normally done with password or other authentication factors

Authorization:

• Based on your identification & authentication, what do you have access to in terms of resources?

Accounting:

• Accounting has to do with logging the resources used such as: Login time, data sent & received, logout time

• This AAA framework typically runs on a AAA server which handles requests to login to the intranet

RADIUS (Remote Authentication Dial-In User Service)

RADIUS (Remote Authentication Dial-In User Service):

• 1 of the common AAA protocols, supported on a wide variety of platforms & devices (such as WPA2 Enterprise)
• RADIUS protocol is normally used to centralize authentication for users
• RADIUS is available on almost any server OS

UTM (All-in-one security appliance)

Unified Threat Management:

• This includes firewalls, IDS, IPS, proxies, VPN concentrators, spam filter, URL filter & more into a centralized device
• Sometimes referred to as Web security gateway
• Certain UTMs can even provide routing & switching capabilities
• Certain UTMs can even be configured to provide bandwidth shaping (where you prioritize certain applications that communicate to the Internet)

Content Filtering

Content Filtering:

• Content filtering controls traffic based on the data within the packets
• There is a corporate control of outbound & inbound data so basically you can control what comes in & what leaves the network so you can control if users can see NSFW content, etc.

Abstraction

Abstraction:

• The concept of abstraction is a representation of the key features of a system without unnecessary details
• This matters because abstraction is used in engineering drawings where too many unnecessary details can be confusing.
• Obviously abstraction could be used in areas other than in engineering, such as in computer science.

States:

• A state is a temporary configuration of a computer system that affects how the system responds to interaction
• Any computer has 2 states: being on & off. When it is on it can actively respond to interaction & perform numerous activities but when it's off, it cannot.
• Different software has different types & numbers of states (**EX**: a cursor when you are in a word document has the states of typing, cursor absent, select, etc)
• Certain software is designed to not check if an Internet connection drops midway of downloading an email (there are other examples as well of this) so technically the application could just break and not function correctly from there on, this is a state it's in. The way to fix it is to turn it off & back on, & this is why turning it off & back on works.
• There are several other reasons why powering off & back on devices work, most commonly it's due to

clearing out the ram

Network Requirements in Virtualization

Network Requirements:

• Most client-side hypervisors have their own (internal) network so they don't have to communicate w/ the outside network.
• When using a VM, you can also use a shared network address so that the VM & the physical host machine use the same public IP. In this case, each VM has a different private internal IP address & when data is received, NAT is performed to convert the public IP used by the VMs (the same as the host IP) to the private IP to see where the data is supposed to be sent.
• You can also configure a VM to have its own IP address instead of using the same public IP as the host machine, this is considered a **bridged network address.**
• You can even configure a VM to have a private address so that it can't communicate with anyone which is common with test machines in test environments.

NAS vs SAN

NAS vs SAN:

• **NAS** = Network Attached Storage (NAS)
    ■ this allows you to take a storage device & connect it to an ethernet network.
    ■ If you need to change a single character (or a byte) within a file, you have to rewrite the entire file onto that device in order to do so
• **SAN** = Storage Area Network (SAN)
    ■ A bit more efficient than NAS due to block level access which is similar to the storage drive that's in PCs. If you need to change a byte within a file, you only need to change that block of data instead of having to rewrite the entire file onto that device.
    ■ SANs are used to collect storage & have access to it from multiple servers. Scaling with SANs is easy & it provides centralized access to your storage.
• Both NAS & SANs consume lots of bandwidth so they are commonly connected to high speed networks that can support the data being transferred back & forth & networks that are isolated to prevent interference from any other activites that may be going on in that same network

SAN (Storage Area Network)

Fibre Channel (FC):

• A type of Storage Area Network (SAN)
• Fibre channel is a specialized high-speed hardware device that connects servers to storage, it can transfer data at 2,4,8, & 16 gigabit per second rates
• Fibre channel supports both fiber & copper cables.
• Both the server & the storage would connect to a Fibre Channel switch & the storage would use some common protocols (such as SCSI, SAS, or SATA) to transfer data over the SAN.

InfiniBand

InfiniBand:

• Used if high speeds are needed with Storage Area Network (SAN)

• Has its own switches & adapter cards, similar to how Fibre Channel would be implemented
• With infiniband you can connect to the Storage Area Network (SAN) with both copper & fiber using Quad SFP connectors
• Infinibands are used where high speeds & low latency is needed

Fibre Channel over the data network

Fibre Channel over the data network:

• Fibre Channel over Ethernet (FCoE) doesn't require any specialized hardware & uses Fibre Channel but over an ethernet network.
• With FCoE, there is no need for a Fibre Channel switch.
• FCoE usually connects with an existing Fibre channel infrastructure & since it's at the ethernet frame level, it isn't routable but since it's ethernet you can use an ethernet card in a device rather than using a fiber adapter.

Fibre Channel over IP (FCIP):

• If the storage & the devices that need access to that storage (**EX**: Servers) are on different IP subnets, FCoE cannot be used since routability isn't an option to consider but FCIP can be used!
• FCIP tunnels fibre channel within existing IP packets which allows you to route this traffic from 1 subnet to another while still being able to communicate to a fibre channel device.

WAN Services

ISDN:

• ISDN = Integrated Services Digital Network
• ISDN networks usually aren't stand alone WANs today, they usually are used to support traditional PBX connections or radio/broadcasting services where they want to connect 2 locations & wish to transmit high quality audio between those 2 locations.
• Can be delivered via **BRI (Basic Rate Interface)**
    ■ has two 64 kbit/s B channels which are responsible for transmitting data
    ■ one 16 kbit/s signaling D channel is responsible for setting up & terminating the call & once the call is set up, the data can be sent either over 1 or both of the two B channels.
• For a larger ISDN implementations, **PRI (Primary Rate Interface)** connection should be used:
    ■ Delivered either over a T1 (can support 23 B channels & 1 D channel) or E1 line (can support 30 B channels, 1 D channel & an alarm channel)

T1/E1

T1/E1:

• Some traditional WAN connections might be brought in over a T1 or E1 line

T-Carrier Level 1:

• A way to connect 2 locations using Time division multiplexing.
• T1 is commonly implemented in North America, Japan & South Korea
• There are 24 channels on a T1 line & each channel can support 64 kbit/s so technically each line can

support 1.544 Mbit/s

E-Carrier Level 1:

• E stands for Europe
• E1 has 32 channels & each channel can support 64 kbit/s so technically each line can support 2.048 Mbit/s

DSL (Digital Subscriber Line)

DSL:

• AKA ADSL (Asymmetric Digital Subscriber Line)
• Common in home networks
• Allows us to use existing telephone lines as high speed digital connections
• Asymmetric due to download speed being faster than upload speed which is usually due to clients downloadng more than they upload. A client's upload is normally just requesting a webpage which isn't resource intensive but on the other hand, downloading a web page is a lot more resource intensive.
• There is around a 10,000 foot limitation from the central office (CO) or else you lose the connection. Of course, the closer you are to the CO, the better speeds you will have.
• 52 Mbit/s download & 16 Mbit/s upstream is common

WAN Transmission Mediums

WAN Transmission Mediums:

• There are several mediums in which you can connect your WAN

Satellite Networking:

• Communicate to a satellite, considered non-terrestrial communication. This type of connection is pricy compared to regular terrestrial communication but the speeds are quite quick.
• Satellite networks are installed in locations where it would be difficult to use regular WAN transmission mediums
• Satellite networks have high latency compared to terrestrial networking (best response is 250 ms up & 250 ms down.
• Satellite Networking also use higher frequencies to communicate (usually in the 2 GHz range) which is considered a line of sight & it requires that nothing is in between you or the satellite in terms of interferences (interferences such as rain fade from rain which disrupts the connection between you & the satellite)

Copper:

• Easy installation with relatively cheap price & easy to install & maintian
• Copper has limited bandwidth availabilities due to limitations in the electrical signals
• Copper is used by cable modem, DSL, T1/T3 local loop for WANs
• For most WANs the connection medium is a combination of both copper & fiber.

Fiber:

• Fiber has high speed data communications as it transfers data via light frequencies so the limitations that come with electrical signals are dismissed.
• Fiber does have a higher installation cost when compared to copper & the equipment is costly, it's more difficult to repair but it does communicate well over long distances.
• Fiber is common in large installation in the WAN core of our ISPs since it supports very high data rates. The ISPs can put many customers over a single stand of fiber & they usually support multiplexing using optic fiber
• Fiber is slowly approaching home & businesses

Wireless:

• Wireless WANs use the cellular network for communication
• Wireless WANs are normally used for very specific systems such as security systems, daily POS reporting & updates. Wireless can also be used for roaming communication where you have no way to plug in & connect but of course this is limited for the coverage for that WAN provider & there are differences in speed depending on how far you may be from the provider's antenna.

WAN Technologies

ATM

Asynchronous Transfer Mode:

• A common communication protocol used over SONET networks
• Uses 53-byte “cells” which include 48-bytes for data & 5-bytes for routing headers
• These “cells” provided high throughput (throughput measures amount of completed work against time consumed, so like bandwidth), real-time, and low-latency since you knew when the next 53-byte cells would come through the network. Due to these benefits, ATM was common in data, voice & video transmissions.
• ATM had a max speed of OC-192 (about 10 gb/s) which was limited by the segmentation & reassembly (SAR) that had to occur due to ethernet frames being larger than 53 byte frames so the ethernet frames had to be broken up & then be put inside the ATM network & then the frames would reassemble on the other side.
• ATM faded when IP tech became popular

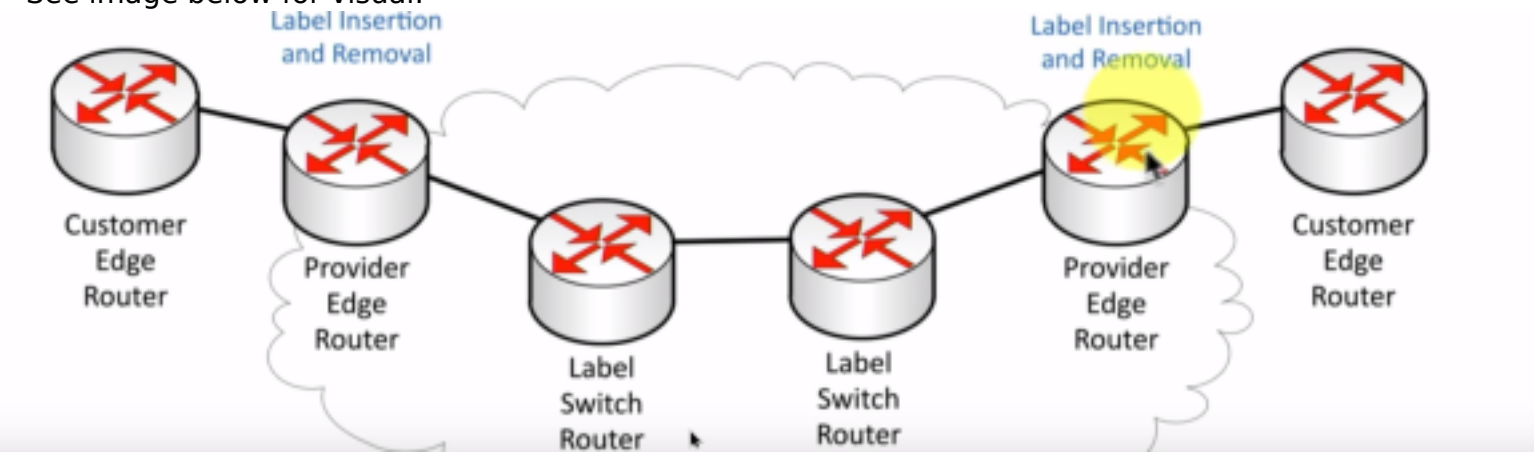
MPLS (Multiprotocol Label Switching)

MPLS (Multiprotocol Label Switching):

• This takes takes the best of both ATM & Frame Relay topologies & ditches the disadvantages of the 2
• MPLS data is put onto WAN with a label that designates what the destination is which makes routing easier (similar to frame relay)
• Many different types of traffic can be sent over MPLS (IP packets, ATM cells, ethernet frames, etc)
• MPLS has become common for providing WAN connectivity & it's simple to find services & hardware to support MPLS

MPLS Pushing & Popping:

• As data is sent into MPLS cloud, there is a label that is **pushed** onto the packets so the destination is known
• When the data arrives on the other side, the label is **popped** off & the data is provided to the customer
• See image below for visual:



PPP (Point-to-Point Protocol)

PPP (Point-to-Point Protocol):

• This is a way to connect 2 devices so you can then send other types of protocols over that WAN link
• Considered an OSI Layer 2 (Data Link protocol)
• PPP is commonly used for dial-up links, serial links, mobile phones & even for DSL for home & business
• **Advantages** of PPP:
  ■ PPP can be used for authentication of the network
  ■ Data can be compressed using PPP
  ■ PPP can be used for error detection
  ■ You can build multiple PPP connections & multilink those together for larger bandwidths

PPoE (PPP over Ethernet):

• An extension of PPP
• Encapsulates PPP within an ethernet frame
• PPoE is common with DSL networks, more specifically with telepohone providers
• PPoE is easy to implement since most operating systems understand PPoE, no complex routing decisions to make and the architecture of PPoE is similar to operation of dial up network.
• You can use PPoE to connect to a network & then decide which ISP to use at that point

DMVPN (Dynamic Multipoint VPN)

DMVPN (Dynamic Multipoint VPN):

• A popular Cisco WAN technology
• Common on Cisco routers
• You can connect to your network & have your network decide when & where it would like to connect to other locations
• Essentially, you're having all your sites's build their VPNs as needed (or ad hoc)
• Tunnels are built dynamically & on demand depending on what location needs to speak with another location. **EX**: It's common to have 1 main office & multiple remote sites. Usually, you want these remote

sites connecting to the main office but what if 1 remote site wanted to communicate with another remote site. In this case, you'd have to communicate with the main office & have it routed back to the remote site; **But with DMVPN, since tunnels are dynamic (ephemeral in other words), you can dynamically build a tunnel/for a secure connection, send the communication needed & then tear down the connection.**

WAN Termination

Demarcation Point:

• The point where you connect with the outside world. Often a network interface on the outside of building (see photo). Or it can be on the inside of the building

• WAN demarcs are common in businesses & offices but they are also seen in homes. In homes, it's common to be provided a demarc point by a phone or cable provider where they provide that “hand off point” (the device) to the rest of the devices in the home
• On your side, you connect your CEP (Customer Premise Equipment or Customer Prem)

CSU/DSU:

• CSU = Channel Service Unit
• DSU = Data Service Unit
• The main function of a CSU/DSU is to connect routers to a T1 line (T1 lines are a way to connect 2 locations through multiplexing)
• Sits between router & circuit installed from dmarc
• The CSU connects to the network provider
• The DSU connects to the data terminal equipment (DTE) (DTE is commonly a router in your environment). The DSU is also responsible for managing the interface with the DTE.
• Sometimes the CSU/DSU could be an external device but commonly the CSU/DSU functionality is built into the router so you connect from the dmarc straight to the router where the functions are performed.

CSU/DSU Connectivity:

• Note: This is is the CSU/DSU is an external device & the CSU/DSU functionality isn't built in the router
• From the dmarc, you often connect with an RJ-45 light connection (AKA Rj-48c wiring) that might also connect through a 15 pin connector to a network interface on a CSU/DSU
• A common way to connect between the CSU/DSU & the router is a v35 connection which is a blocky connection or a 25-pin serial connection between the CSU/DSU & the router
• Some CSU/DSUs include monitor jacks which allow you to connect diagnostic equipment which can be connected without disrupting the connection that's already in place.

Smartjack

Smartjack:

• Sometimes the Wide Area Connection at the dmarc is a bit more intelligent & instead of having just a cable handoff, we have a smartjack (or a **Network Interface Unit (NIU))**
• Smartjack is more than a simple interface, it can be a circuit card in a chassis. The smartjack is normally inside the provider's side of the communication.
• **The smartjack is a way for your Wide Area Network provider to perform some additional functions** such as setting up a loopback to provide diagnostics directly from the interface at the dmarc.
• The smartjack can even provide alarm information and reconfiguration details for the wide area network provider so they can remotely make changes on the smartjack & essentially to your WAN without having to be in person

Network Operations

Network Documentation

Internal Operating Procedures:

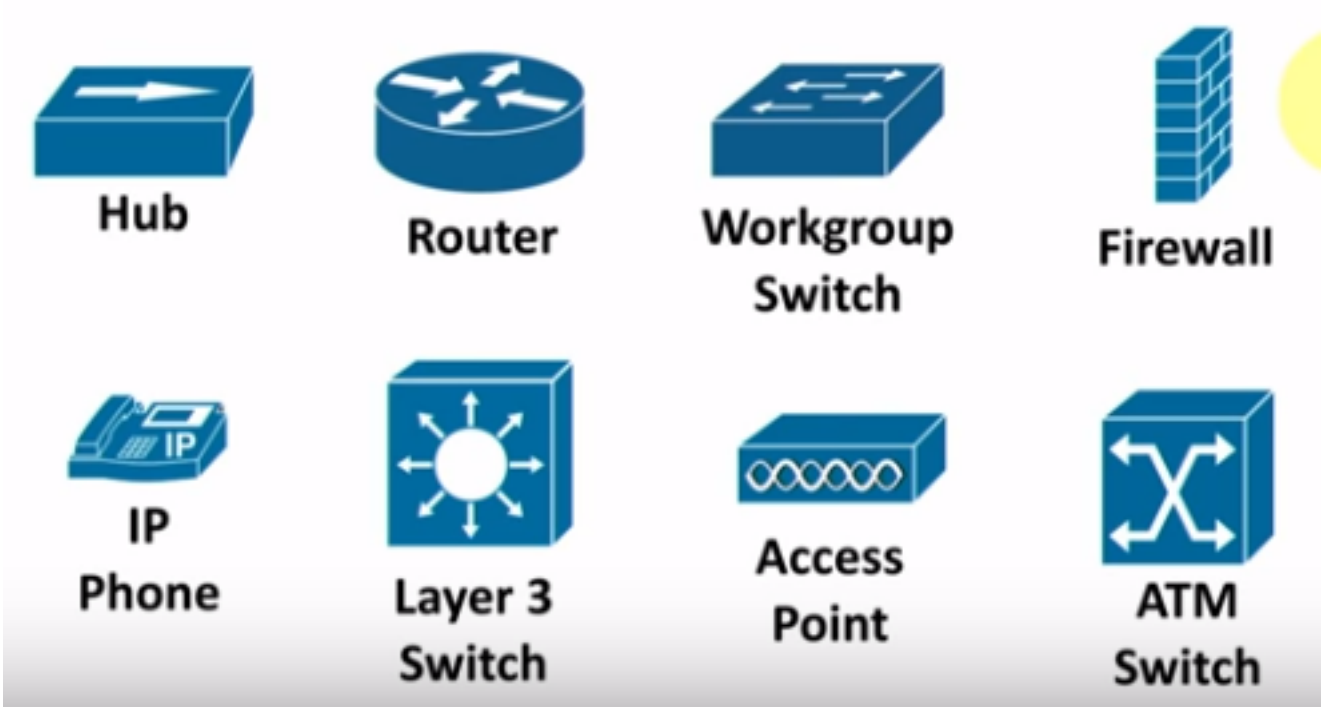
• Since organizations all have different business objectives & goals (& different processes & procedures), it's important to document how to handle internal operating procedures such as how to notify the team if a system goes down or if there are facilities issues.
• There can also be procedures that must be followed in order to perform specific tasks such as software upgrades, these procedures may include testing the software upgrades and going through a change & control process
• It's important that this documentation of the procedures is available to those inside the organization so it can be reviewed and understood by insiders

Mapping The Network:

• Lots of documentation in the networking world is based on the infrastructure of the network
• Networks are built in long periods of time through multiple phases. And even once the network is completed, you may not know where the wiring goes since most will be tucked away in the walls/ceiling so it may take an additional effort to document all that info
• Network documentation is essential (both physical & logical). It is helpful with new hires as well or when contracting 3rd parties.

Network Symbols:

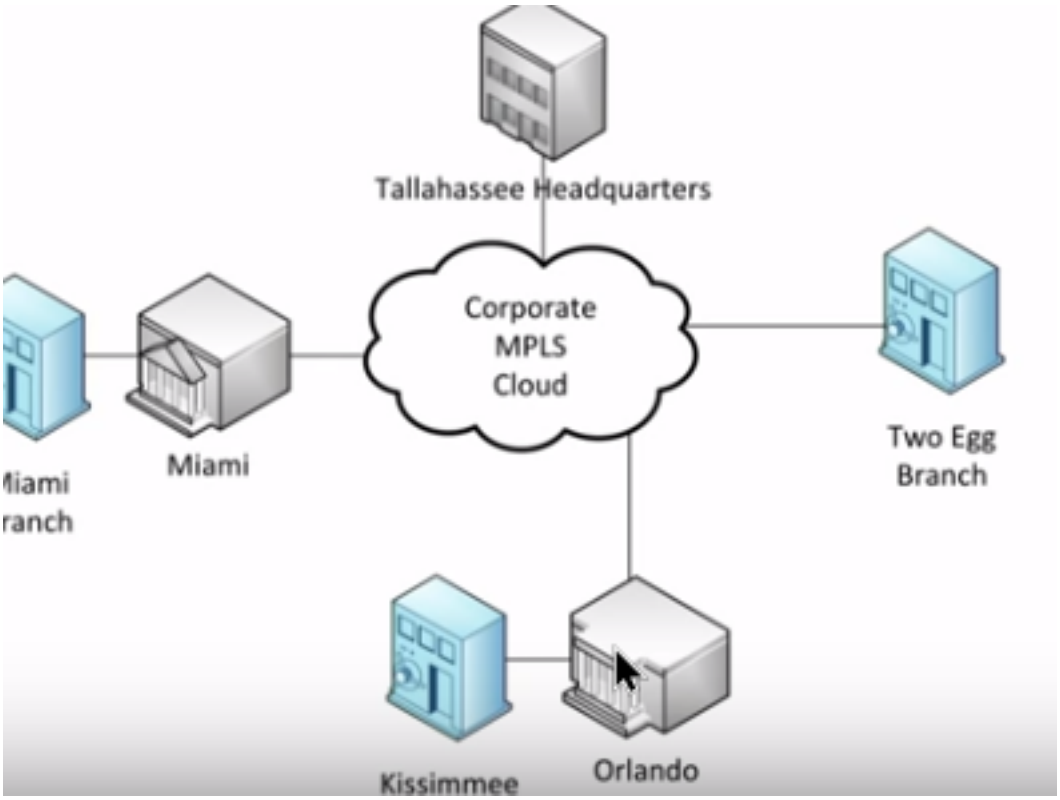
• The following are a set of standard network symbols.



Logical Network Maps

Logical Network Maps:

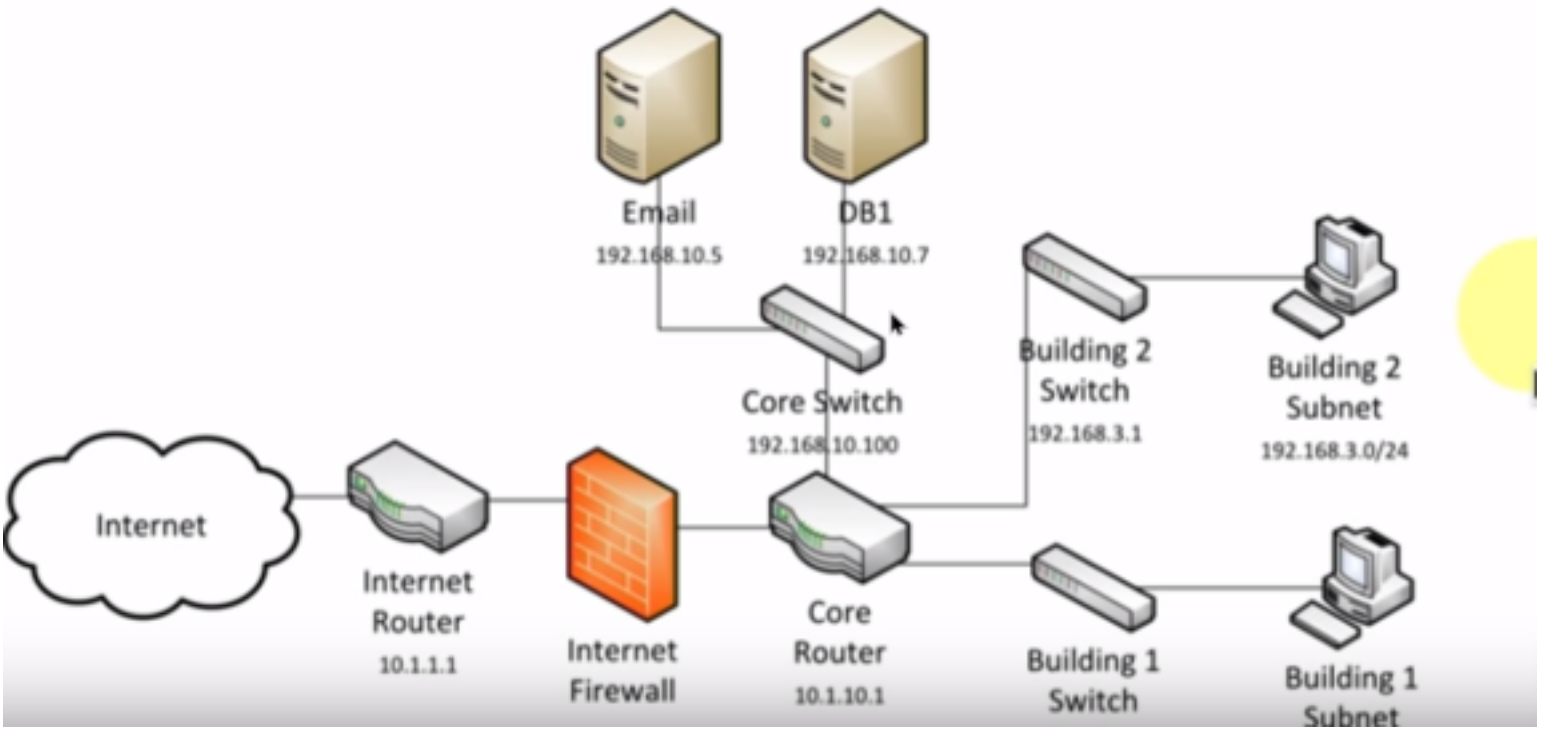
• When building logical network maps, you're creating a wide perspective of how the network may be configured. Logical network maps don't show specific components or exactly where wires are going but you should be able to determine what sites are connected & how they connect to each other
• Logical network maps can be created via specialized software such as Visio, Omnigraffle, gliffy, etc
• Logical network maps are useful for planning and/or working with 3rd parties, if more details are needed you can move onto the physical network map.



Physical Network Maps

Physical Network Maps:

• Physical network maps show individual components inside the network, identify specific interfaces on devices, it may show IP addressing & gives you an idea of where cables & wires may be running between devices
• Some physical network maps wil show the physical layout of the rack that's in the data center (see image below for example)



Change Management

Change Management:

• Any time a change is made to any hardware or software, there is an associated risk with the change.

You may have overlooked or ignored the fact that it's possible that the particular change will break another piece of that software
• Due to the risk that's associated with making changes to different components, organizations often have clear policies that state any changes that are to be made must be ran through a group of people or a single person that will document the change, ensure a fallback plan exists just in case the change doesn't work properly, & everyone is aware that change is occurring
• If change management/change control isn't already part of the policies, it can be extremely difficult to implement unless everyone is in on the idea

Managing Your Cables

Managing Your Cables:

• The ANSI (or Administration Standard for the Telecommunications Infrastructure of Commercial Buildings) provides info on how to document the network (sample reports, how to draw out the network, how work orders should look, etc)
• There are lots of cables going through your network and you need some way to identify & label these cables so you could use identifiers (such as labels, color coding, bar coding).

System Labeling:

• Many people will work on the same workstation or server so there needs to a way for someone to know what specific components you're referencing. This can be done by creating a unique system ID for each device which may have an asset tag, a system name, and a serial number. When labeling, you want to make the labels clearly visible.

• With the photo, you can quickly identify the device by loooking at the tags and the serial number and refer to the system label

Circuit Labeling

Circuit Labeling:

• Most organizations have lots of WAN circuits coming into the building, so labeling these is a good idea
• WAN circuits can operate fine but then begin to have some problems due to something that may be between one site and the remote site, due to this you would need document exactly which of the WAN circuits are having a problem.
• Specifically, it is ideal to document the Demarc interface of the WAN circuit, the CSU/DSU, the router (**NOTE**: these are the components of a WAN). You should also label other info such as the WAN provider circuit ID, the WAN provider phone number, & the internal reference name you can use when putting internal reports together.

Baseline

Baseline:

• This defines how the network “normally" operates. It identifies the application response time, network throughput, etc.
• A network's baseline should be an ongoing documentation meaning it should be reviewed every once in a while to be updated.
• Baselines could be used to tweak the amount of resources to allocate in the network, **EX**: A baseline may examine the amount of traffic your web server gets on a weekly basis, this will tell you the days to expect most traffic so you can properly allocate more resources to the server on those specific days.

Inventory Management

Inventory Management:

• This includes documenting a record for every asset (routers, switches, cables, fiber modules, CSU/DSU, etc
• Some organizations may even add an asset tag to the device (can be a barcode, RFID, visible tracking number) so not only are you keeping a database of where the device is, you have a tag that IDs the device & has a visible tracking number which can be used to reference how it is associated with your database.

Inventory Management Software:

• Master database that may include all corporate assets
• The software likely has other functions such as help desk and a reporting functionality
• As the organization gets larger, you can add additional assets/inventory and you'll know exactly where it is all located.

Business Continuity

Fault Tolerance

Fault Tolerance:

• Fault tolerance maintains uptime when failure occurs.
• Fault tolerance adds additional complexity as it adds processes to follow & it can add additional cost as the environment that has to be managed and maintained increases.
• Fault tolerance can be added for an individual device then you may be adding additional storage devices & configuring RAID
• Fault tolerance can also be added for multiple devices for a large scale fault tolerance in place such as adding multiple load balancers for server farms.

High Availability:

• Redundancy doesn't always mean always available (When say a server fails, it will take time to get the redundant server up and running, the time between the server failing and the other server finally getting up and running is considered down time still.
• HA (High Availability which means always on, always available) configurations may be a must-have for some organizations that need to always be up.
• With HA, you would most likely need to install multiple devices that will always be running & working

together. You also want to watch out for any single points of failure.
• Higher availability almost always means higher costs, there will be upgraded power, high-quality server components, & you will likely be buying multiple devices at a time instead of single devices.

NIC Teaming (Network Interface Card)

NIC Teaming:

• Often called LBFO (Load Balancing / Fail Over)
• Provides a combination of bandwidths since you're using multiple network connections and you also have multiple paths so if 1 path disappears, you still have another path to communicate out of that server.
• Using multiple interface cards & teaming them together in the OS, to the OS it looks like a single NIC.
• The NICs used are constantly communicating with each other using multicast to perform health checks of all the other NICs, if any don't respond, it's taken out of service & the remaining cards continue to provide connectivity.

UPS

UPS:

• A common power redundancy component
• Uninterruptible Power Supply provides short-term backup power. Useful in blackouts, brownouts, & surges

UPS Types:

• Offline/Standby UPS (only switches over to battery if main power source is lost)
• Line-Interactive UPS (can slowly bring power up from battery, useful when brownouts occur)
• On-line/Double-conversion UPS (alwas running from battery, if power is lost then no switch out is needed, you continue to use the battery until power is restored)

UPS Features:

• Auto shutdown - if power goes out, it continues to run but as battery goes lower, it sends a signal to your computer to auto shutdown so nothing is lost in the system
• Battery capacity
• Outlets
• Phone line suppression (used by phone lines to prevent any voltages from coming through the phone line connection)

Generators

Generators:

• long-term power backup
• uses fuel (fuel storage is required) to create power source for the entire building (can include every electrical outlet in building or only certain electrical outlets in the building).
• The generator isn't running when power is running through to your building, so it may take a few

minutes to get the generator up to speed, you can use a UPS while the generator is starting.

Dual-Power Supplies

Dual-Power Supplies:

• On individual servers, dual-power supplies can be used to create power redundancy if the server can support redundant power supplies.
• This is designed so that each power supply can handle 100% of the power load
• Power supplies are normally hot swappable which means you can normally hit the button, pull out a power supply while the system is running, put in a new power supply and turn it on without having any impact on the system it's running on.

Cold Site

Cold Site:

• A cold site is an empty building with no hardware
• When migrating to a cold site, you have to bring everything with you from data to hardware to employees.

Warm Site

Warm Site:

• A warm site is somewhere in between cold & hot (There are different variants of warm sites, some may have some hardware while some may just have staff)
• Warm sites typically will have hardware ready & waiting, all you need to bring when migrating is the software & data.
• The end idea of a warm site is that you at least have “something” to work with when recovering systems. This “something” can refer to almost anything.

Hot Site

Hot Site:

• Hot sites are the most expensive recovery site option
• With hot sites, there is an exact replica of everything that the original site has
• Hot sites should be constantly updated with the latest software & data
• When maintaining a hot site, you typically buy two of everything, what you buy for your main site, you buy for your hot site too.
• In many hot sites, there's an automatic replication that occurs, so when the main site data is updated, the hot site's data is also updated.
• When you need to migrate to a hot site, all you have to do is simply flip a switch.

Backup & Recovery

Taking Snapshots

Taking Snapshots:

• Snapshots are used in the virtual world for backups
• Snapshots capture the current configuration and/or the data in the VM
• With snapshots you can also live boot media which means run the operating system from removable media. Specifically, you can have an OS running on one laptop, take a snapshot, and when you boot from the same media on another device, it will be as if you never left the 1st device.

Recovery

Recovery:

• Mean Time To Restore (**MTTR**) refers to how long it takes to restore system(s) to a particular point in time
    ■ **MTTR** can also refer to the Mean Time To Repair a system
• There can also be a Mean Time Between Failures (**MTBF**) which refers to the amount of time in between failures which can be used to predict the time between failures (EX: if a server has an MTBF of 30 minutes then that means it fails after every 30 minutes)
• When you're working with a company/organization & providing a service, there is normally an **SLA** (Service Level Agreement) which states the recovery expectations if an outage occurs & that certain services/systems will be available for a certain amount of time.
    ■ With SLAs there is normally an agreement that if the services/systems are down for longer than agreed upon, then there may be a monetary penalty.

File Backups

File Backups:

• A good attribute when backing up files is the ability for the system to recognize which files have been changed since the last backup and which have stayed the same, the way this is done is by the **system reviewing the archive bit, if it's turned on then that particular file has changed since the last backup**

Full Backup:

• When performing a full backup, you don't care if the archive bit has been turned on or not
• You backup every file in the entire file system
• When performing a full backup, you will be clearing that archive bit so that when you go back the next time you can see what files have been changed since the last backup.

Incremental Backup:

• Incremental backups grab all the files that have the archive bit set since the last incremental backup & backs those files up (since the archive bit indicates changes have been made)
• With incremental backups, if a full recovery is needed then it is more of a workload (when compared to differential backup at least) when recovering the system since incremental backups only back up data that has changed since the last incremental backup. There are more incremental backups so a full recovery consists of gathering lots of backups & piecing them together. With a differential backup, to perform a full recovery, you would only need to recover the latest differential backup since differential backups backup data from the last full backup (this includes everything that has happened in the system

since the last full backup).

Differential Backup:

• A differential backup grabs all the files that have the archive bit set since the last full backup & backs those files up

Network Monitoring

Log Management

Log Management:

• Network devices gather an enormous amount of info which is normally provided in the format of a log file
• There is usually one central point where all the logged info is combined, it's usually sent from all these devices using a standard **syslog** protocol. This means in this server, you will be collecting a lot of log files which means you need a massive amount of storage, there is never enough storage space for log files.
• Since there is so much storage that it takes up, **data rollup** becomes important which is when we decide to stop storing a certain data after a certain amount of time and increase the interval at which the data is collected (**EX**: We may take performance samples every minute for our servers but after 30 days, we may increase the interval to take samples every 5 minutes)

Data Graphing

Data Graphing:

• It's common to take the info you're storing and create a graphical representation of what's being stored.
• The data being collected may be **raw logs** so you would need to convert it in order for it to be easier to graph but sometimes the data is in a **summarized metadata format so it's easier to graph.**
• **SIEM** (Security Information & Event Management) software is used by many organizations to combine the information collected from logs & create reports on the stored info. But creation of reports can consume lots of resources.
    ■ The SIEM turns raw data into something visual (a graph)
• The SIEM may even have built-in graphs so there is little to program/develop.

Patch Management

Patch Management:

• If vulnerabilities are found on devices (after a vulnerability scan) then it's time to patch
• Patch management should be applied when they're released to provide system stability & security fixes.
• With Windows, service packs are available which bundles multiple patches together to a bundle download.
• Some patches are released monthly (**EX**: Microsoft's monthly patches) but some patches are released in a not-so-routine fashion, these patches can be emergency patches meaning they're fixes for things like zero-days & important security discoveries.

Rollback Options:

• Sometimes a patch will cause unwanted bugs/disrupt the functionality of a system which would cause someone to want to rollback to the last update, this is possible (**EX**: Microsoft allows you to delete updates/patches)

Baseline Review

Baseline Review:

• After collecting all of this network info, you can begin creating a baseline of how the network normally operates.
• If you note the network's behavior is deviating from the baseline, then you may need to investigate further

Protocol Analyzers

Protocol Analyzers:

• Sometimes you need to get into the details of what an application may be doing over a network, this is where a protocol analysis comes in
    ■ A protocol analyzer captures every frame going through the network & then provide a decode that gives more info about the network & the application performance.
    ■ A protocol analyzer can capture data from an ethernet connection or directly on a wireless network. Some infrastructure devices & security components can also capture packets which can then be opened & viewed with a protocol analyzer application.
    ■ These protocol decodes make it easy to view everything that's occurring across the network, you can view traffic patterns, identify unknown traffic, see the application performance across the network (this for a specific protocol), or you can create filters to narrow down view to exactly what you're looking for.
• Some protocol analyzers allow you to capture data over a long period of time (EX: days) which allows you to perform big data analytics & determine what's really happening w/applications on the network.

Interface Monitoring

Interface Monitoring:

• If a monitoring system on a network, **interfaces** are going to be a key component of what is being monitored.
• You need to know whether an interaface is up or down, this can be one of the important things you need to know about that particular device.
• If an interface has been available but is suddenly unavailable, then an investigation may likely be needed.
• Interface monitoring doesn't need any special rights or anything, you simply ping the interface. Green = Interface is up & running. Red = interface isn't responding to ping queries, indicating it's down.
• The function of interface monitoring is likely an automated function that continues to run all day periodically checking to see if an interface is available. If an interface is suddenly unavailable, alarms and alerts should be created to alert the proper people of what's going on.
• You can go in deeper depth of interface monitoring with SNMP (Simple Network Management Protocol)

SIEM

SIEM (Security Information & Event Management):

• This is usually a device that combines all log files from all different devices & gives you the ability to monitor & create reports on all that logged information.
• the SIEM can even perform real time monitoring of the info it receives.
• Since the SIEM gathers & stores so much info, it can create interesting long & short-term reports. The SIEM may have a built-in report function but it may allow you to create custom reports.
• If a security event occurs, the SIEM is a key component of the forensic analysis

SIEM Dashboard:

• This provides you with a way to view all the logged information in a not-so-detailed format with a more graphical view.

Syslog

Syslog:

• This is a standard way of collecting all the log files among many different devices & transferring them.
• It's common to have all the devices report back to a SIEM using the syslog protocols.
• It's common for the SIEM to be equipped with tons of storage in order for it to collect all this log information

SNMP (Simple Network Management Protocol)

SNMP:

• Another way to monitor the network & all of the devices is to query the devices for more info, **SNMP is used to provide the query**
• SNMP allows us to use a standardized info base to query a device & return details of how the device may be performing.
• You set up a management station to perform queries, the station is set up with the name or IP address of the remote device you want to monitor, then you specify the **version** of SNMP that is supported by the remote device.
    ■ **SNMPv1** = Info sent in cleartext. Allowed management station to send a single query to remote device & get a single response from remote device.
    ■ **SNMPv2** = Management station can request many different items at once & receive many responses at once. But info was still sent in cleartext.
    ■ **SNMPv3** = The new standard. Allows for message integrity, authentication, & encryption.
• SNMP info can be very detailed so people that query the devices through SNMP should only be the ones who actually require this access.

Monitoring the Interface

Monitoring the Interface:

• There are many other metrics that can be gathered from these interfaces besides whether they're available or not available. These other metrics can be caught before they become larger problems that can have a much larger impact on the network.

• If you're monitoring with SNMP, you can remotely monitor all the devices, most metrics are in MIB-II (standardized management information base, almost every device supports gathering statistics from this database), & proprietary MIB may be available (some devices have proprietary MIB data bases which allows gathering of metrics/details that are very specific to certain devices).

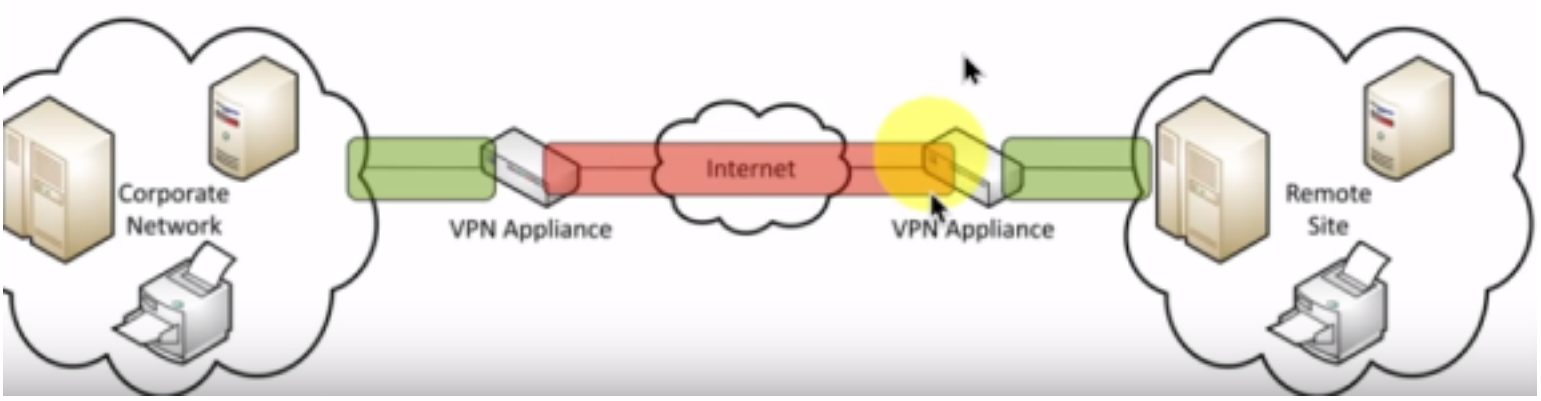
Remote Access

IPSec (Internet Protocol Security):

• Security for OSI Layer 3
• IPSec gives option for authentication & encryption for every packet sent across a network
• IPSec provides confidentiality & integrity for packets
• IPSec is popular & can be found in many vendor's implementation (meaning you can have 1 vendor on one end of the WAN and another vendor on the other side of the WAN, & you'd be able to communciate w/each other using IPSec.
• Two core IPSec protocols:
    ■ Authentication Header (AH)
    ■ Encapsulation Security Payload (ESP)

Site-to-Site VPNs:

• Site to site VPNs are a common implementation of IPSec
• Common implementation is a corporate network and one remote site on the other side of the network. A private tunnel is built from the corporate network to the remote site in an effort to shield traffic from being exposed to the Internet in the clear, this private tunnel is usually built by using a VPN appliance installed on both ends of the connection. But sometimes this is already integrated into an already existing platform (EX: Firewalls will provide IPSec endpoint support within the firewall)



• The green represents where data is sent unencrypted while the red is where the data is encrypted

SSL VPN (Secure Sockets Layer VPN):

• Another VPN type that's commonly used for end user VPN access is an SSL VPN
• Instead of using IPSec to provide encryption, SSL/TLS is used (commonly runs over TCP 443)
• Since SSL/TLS is a common protocol, most firewalls allow this traffic to pass without any additional configurations.
• SSL VPNs can use a simple user/pass to authenticate users, there is no requirement to set up digital certificates or shared passwords like with IPSec
• SSL VPNs is widely supported & can be ran from inside a browser from a VPN client.

Client-to-Site VPNs:

• A common configuration to use for an SSL VPN
• Software is installed on remote user's workstation (sometimes the software is built into existing OS) & is connected to a VPN Concentrator which is often a firewall that's installed at the remote location. The user simply starts their VPN & authenticates to the VPN concentrator & anything from the remote user to the VPN concentrator is sent encrypted.

DTLS VPN:

• Datagram Transport Layer Security, this basically uses the security of SSL/TLS with the speed of datagrams (using UDP instead of TCP)

Remote Desktop Access:

• Allows someone to share a desktop from a remote location
• RDP (Microsoft Remote Desktop Protocol) which can be used for Mac OS, linux, & others
• VNC (Virtual Network Computing) which uses Remote Frame Buffer (RFB) protocol & also has clients for many OSes & many of those clients are open source

SSH (Secure Shell):

• Encrypted console communication to remote devices (TCP/22)
• Looks & acts the same as Telnet (TCP/23)

Web-Based Management Console:

• With many devices, a web-based management console can be used to manage the device with your browser
• By using HTTPS, an encrypted connection is ensured between the remote device & our browser
• The important features are in the browser, but you may still need access to the CLI to run certain things that aren't in the web based management system

Out-of-Band Managment:

• Used when the network isn't available or the device isn't accessible from the network
• Accessed through a separate management interface such as a serial connection or USB (see photo)

• If the device isn't physically accessible you can connect the serial connection or USB to a modem & dial in through phone lines in order to manage the device.
• Some organizations may connect devices to a console router & you would dial in to the console router & specify which device to communicate with over the out-of-band management interface.

Policies & Best Practices

Privileged User Agent:

• Network/Sys admins have access to almost everything, but just because they can access almost everything doesn't mean they should
• The **expectation** of people with high privileges in a network is to use other non-privileged methods when appropriate (So when performing actions that don't require elevated privileges)
• A person with high privilege should only use privileged access for assigned job duties
• Since you have high level privileges, you may be asked to sign a privilege user agreement which means you will maintain the highest level of professionalism & maintain the confidentiality of the company's data.

Password Policies

Password Policies:

• It's important for users to update their passwords every so often, many organizations have policies which set their users's passwords to expire after a certain amount of time (this is dependent on what the organization sees as appropriate)
• In organizations where there is a high level of security associated with the data (like in critical systems) the passwords may change more frequently
• If a user finds themselves locked out of their account due to a lost password, the password recovery process shouldn't be trivial. The recovery process should provide a complete identification & authentication of the user before recovering/resetting their password

On-Boarding

On-Boarding:

• Bringing a new person into the organization (new employee or transfer)
• IT agreements need to be signed (or a separate AUP that needs to be signed)

• There are also a number of processes that occur behind the scenes of the onboarding process which includes creating user accounts & associating that user account with proper groups & departments
• The new person also needs to be provided with the required IT hardware whether that be laptops, desktops, tablets, etc and these devices need to be preconfigured & ready to go. Sometimes the new person's personal devices will be added to the mobile device manager (MDM) instead

Off-Boarding:

• This process should be pre-planned
• What happens to the hardware? Do we document the fact that it was returned by the departing employee?
• What happens to the user's data? Do we delete it? (There may be important company data that should be kept associated with the departing employee's account)
• The departing employee's account is usually deactivated instead of deleted to preserve the data (just in case there's anything of importance in the acc)

Licensing Restrictions

Licensing Restrictions:

• There are many licenses in organizations (there may be separete licenses for operating systems, applications, hardware appliances, etc). And all these different licenses require different methods to apply them
• One reason to keep licenses up to date is that if they're expired then we could run into problems with availability if the license was to expire (**EX**: Some applications will work perfectly fine up until the date the license expires & then it won't work at all. Some applications may work after the date their license expires but they will have limited functionality.)

International Export Controls

International Export Controls:

• if you need to send any info, equipment, or data to another country then there may be country-specific laws controlling export
• These international export controls not only apply to shipment of physical items (**EX**: Sending hardware to another country) but also applies to the transfer of software or information
• Components that can be used for both civilian & military use may have a different set of international export controls associated with them (**EX**: A firewall, hacking tools, IPS, etc)
• If these international export controls aren't followed, penalties can be severe so it's important to check w/local legal team to be 100% sure with whatever you're sending to another country is complying with all regulations.

Data Loss Prevention

Data Loss Prevention:

• Every organization needs to have a formal set of policies & procedures related to DLP, these will be policies that dictate how an organization will be handling PII (**EX**: Social security numbers, credit card numbers, etc)
• These detailed policies need to define what is allowed in terms of:
    ■ how is sensitive data transferred?

    ■ Is the data encrypted? If so, using what algorithm?
• Many organizations will also deploy DLP tech/solutions on their servers & network which can watch & alert on policy violations (these solutions watch for data going across the network)
    ■ Often requires multiple solutions in different places.
    ■ If someone does violate the policies &/or procedures then you have the ability to block the info with the DLP tech/solution

Remote Access Policies

Remote Access Policies:

• Controlling the flow of data from 1 side of the network to the other is difficult when people work remotely.
• Remote access policies not only apply to employees but they also apply to any third-parties that may be connecting to a VPN to gain access to internal resources.
• Remote access policies usually have specific technicaly requirements such as:
    ■ Requiring an encrypted connection & the policy may specify the type of encryption to be used.
    ■ Confidential credentials to be used when logging in
    ■ How the network, hardware, & software should be used when using remote access

Security Incidents

Security Incidents:

• Having policies & procedures in place for when particular security incidents occur is important (**EX**: If a user clicks on an email attachment & executes malware which then communicates with external servers, there needs to be policies & procedures on how to handle that)
• There is a wide array of possible attacks that can occur & policies & procedures need to be put in place in order to deal with specific attacks.

Incident Response Policies

Incident Response Policies:

• Incident response policies define how incidents are identified. Incidents can be identified via (NOTE: Incidents being identified simply means that the incident is known, not what type of incident it is/how the incident is categorized):
    ■ automated monitoring
    ■ alarming
    ■ alerting
• How is the incident categoried? (NOTE: Your policies/procedures should be aware of how to handle different categories of attack)
    ■ Email issue
    ■ brute force attack
    ■ DDOS
    ■ etc
• There should also be a set of policies which determines who responds to an incident:
    ■ There is normally a large list of predefined contacts
• All these procedures need to be created well before any incidents occur & everyone needs to be aware of what these procedures/policies are & training needs to be conducted every so often to prepare for the attack.

BYOD

BYOD:

• Bring Your Own Device/Bring Your Own Technology
• Employee owns the device & it is also used for company use by the employee so there is a mix of personal & business data on these devices which is why it's important to establish a policy early on on exactly how this data is managed.
• Employee-owned devices are difficult to secure because there are many factors such as:
    ■ How is the data protected?
    ■ What happens to the data when a device is sold or traded in?

AUP

AUP:

• AUP defines what's acceptable use of company assets
• AUP covers many topics such as:
    ■ Internet use
    ■ use of telephones
    ■ use of computers
    ■ use of mobile devices
    ■ etc
• Every organization has a different view on what's acceptable in terms of when using the network which is why it's important to document this AUP policy

System Life Cycle

System Life Cycle:

• What happens when all your technical assets when they reach the end of their life?
• There needs to be a set of policies & procedures that assist in the disposal of these assets
    ■ includes: Desktops, laptops, tablets, mobile, devices, etc
• Disposal may not only be technical procedures but there may also be legal procedures as some info must not be destroyed due to the type of business you run (some businesses need to store data for a certain amount of time before they even consider disposing of the data)
• You don't want critical info in the trash so you need to be sure any company-related data is wiped before disposal

Physical Destruction:

• Sometimes physical destruction is the only way to be 100% sure that data on a device that needs to be disposed won't be exposed
• Shredder/pulverizer can be used to destroy equipment
    ■ Heavy machinery
    ■ Provides complete destruction
• Some people simply drill a hole or hammer the storage devices
• Some type of storage media such as magnetic tapes can have everything deleted by using a degaussed which removes the magnetic field & destroys the drive data & the electronics
• Some documents can simply be set on fire in order to ensure destruction

Physical Security Devices

Video Surveillance

Video Surveillance:

• CCTV (closed circuit television)
• often coax-connected devices
• Now, it's more often to use IP-based cameras that can communicate across the network using ethernet-based connections
• Camera properties are important:
    ■ Focal length - Shorter focal length is wider angle
    ■ Depth of field - How much is in focus
    ■ Illumination requirements - see in the dark
• Cameras can also provide notification of activity (motion detection)

Asset Tracking Tags

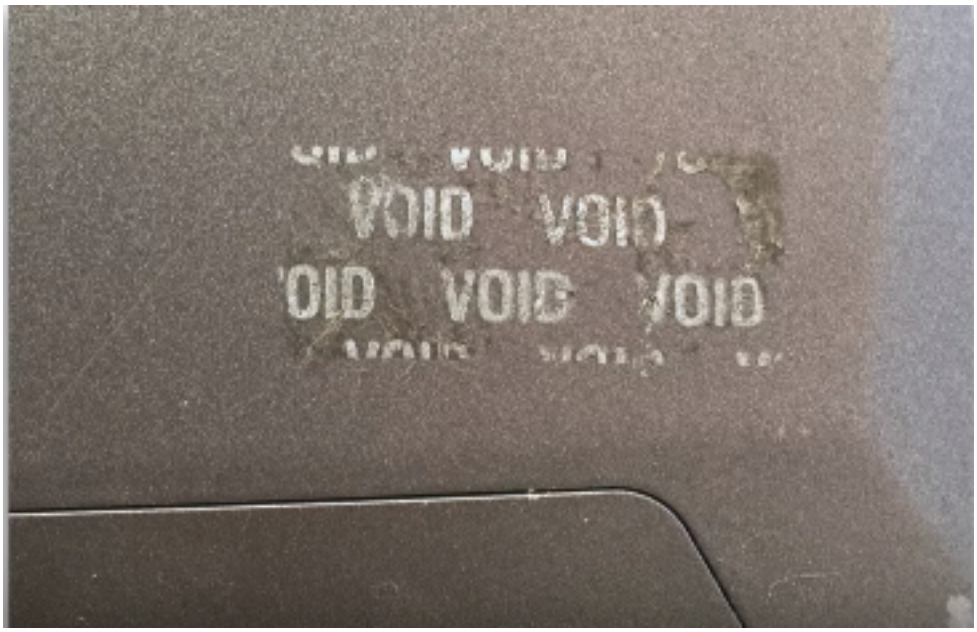
Asset Tracking Tags:

• Used for a record of every assets (devices such as routers, switches, cables, fiber modules, CSU/DSUs, etc)
• With assets tags, you can have a database of the exact make & models of the devices in your organization & where they might be located
• The asset tag may have a number on it as well as a barcode (the barcode can be useful for checking in or checking out the device).

Tamper Detection

Tamper Detection:

• Since you cannot watch all of your equipment all the time, you can have your systems monitor themselves with tamper detection
• Devices such as servers, PCs, routers, etc have case sensors which detect if someone removes the case of the device (indicating they may want to steal some hardware from it), then an alarm is immediately sent from a BIOS.
• If an item has an asset tag or identification tag, you may want foil asset tags which leave a message on the device if the tag is removed (see image)



Identification Badges

Identification Badges:

• ID badges are 1 way to keep track of who may be authorized to be allowed into a particular area
• ID badge can contain:
  ■ Picture of individual
  ■ name of individual
  ■ other details regarding individual's employment w/organization
• The ID badge may also be integrated with door access or a smart card (certain doors can be unlocked with ID badge while other doors cannot be unlocked w/ID badge)

Biometrics

Biometrics:

• used in authentication
• can include but aren't limited to: fingerprint, iris, voiceprint
• System usually stores a matematical representation (AKA a hash) of your biometrics instead of storing your actual fingerprint
• Biometrics are difficult to change, you can't change your fingerprint
• Biometrics are only used in certain situations & are usually mixed in with other authentication methods as it isn't foolproof

Tokens & Cards

Tokens & Cards:

• Smart cards:
  ■ Integrates with devices (door locks, desktops, etc)
  ■ May require a PIN
• USB Token:
  ■ Certificate is usually stored on USB drive & you plug it inside device to authenticate

• Hardware or software tokens/key fobs:
    ■ Generates pseudo-random authentication codes.

Authorization, Authentication, & Accounting

AAA Framework

AAA Framework:

• If you're logging into a network, connecting to a VPN, or gaining command line access to a switch, you're probably using the AAA framework to authenticate which is described as:
• Identification:
    ■ This is who you claim to be
    ■ usually your username
• Authentication:
    ■ Proves you are who you say you are
    ■ usually authenticated by password & other authentication factors
• Authorization:
    ■ Based on your identification & authentication, what access do you have?
• Accounting:
    ■ Tracking what information was accessed, login time, data sent & received, & log out time

RADIUS

RADIUS (Remote Authentication Dial-in User Service):

• One of the more common AAA protocols (commonly used with WPA2 Enterprise)
    ■ RADIUS is supported on a wide variety of platforms & devices, not just for dial-in
• Centralize authentication for users using RADIUS:
    ■ Same credentials to login to routers, switches, firewalls, remote VPN access, or 802.1x network access if RADIUS was used
• 1 reason RADIUS has grown so popular is because you can find RADIUS services available on almost any operating system

TACACS

TACACS:

• Terminal Access Controller Access-Control System
• An alternative remote authentication protocol
• TACACS was created to control access to dial-up lines on the older ARPANET
• Extention of TACACS is XTACACS (Extended TACACS):
    ■ A Cisco-created (proprietary) version of TACACS
    ■ Provides additional support for accounting & auditing
• These days, if you're using TACACS for authentication, it's likely you're using TACACS+ which is the latest version of TACACS
    ■ TACACS+ provides more authentication requests & response codes
    ■ TACACS+ was released as an open standard in 1993
• You can find TACACS+ services for many operating systems that work across many different services

Kerberos

Kerberos:

• If you're managing a group of switches or routers & using RADIUS or TACACS for authentication, you have to provide a username & password each time you login to a separate device, but there's a way to login once & automatically have access to all resources associated w/login (what that account is authorized to access)
• Kerberos is a network authentication protocol
    ■ Authenticate once, trusted by the system until you log out (single sign on)
    ■ No need to re-authenticate to everything
    ■ Mutual authentication - You authenticate to the server & the server authenticates to you
• Kerberos was the standard since the 1980s
• When you login to a Windows domain, it's Kerberos that's providing the single sign on in the background

SSO with Kerberos:

• Enabled using cryptographic tickets, the ticket is granted to someone who is logged on properly & this ticket can be shown to other resources on the network to gain access
• Authentication credentials are provided once
• Only works with devices that are able to communicate using Kerberos protocols

LDAP (Lightweight Directory Access Protocol)

LDAP (Lightweight Directory Access Protocol):

• Protocol for reading & writing directories over an IP network
    ■ Directories are an organized set of records, like a phone directory
• LDAP uses X.500 standard which was written by International Telecommunications Union (ITU)
    ■ if you create an LDAP database then other devices can use this standard X.500 to be able to read & write info
• LDAP uses TCP/389 & UDP/389
• If you have a directory in Windows Active Directory, Apple OpenDirectory, or OpenLDAP then you can use this standard to communciate to any of these directory types

X.500 Distinguished Names:

• LDAP pairs together an **attribute** & a **value** & uses multiples of those attributes to be able to define an object in a database

Attribute	Field	Usage
CN	Common Name	Identifies the person or object.
OU	Organizational Unit	A unit or department within the organization.
O	Organization	The name of the organization.
L	Locality	Usually a city or area.
ST	State	A state, province, or county within a country.
C	Country	The country's 2-character ISO code (such as c=US or c=GB).
DC	Domain Component	Components of the object's domain.

Local Authentication

Local Authentication:

• There may be times where you do not want to authenticate to a centralized database, in these cases you want to use local authentication
• If you're logging in to a device such as a switch, a router, server, etc then you want to use a set of credentials that are stored on that device
• Most devices include an initial local account (default accounts) & good devices will force a password change.
• Most people are using local accounts to be able to gain access to devices if the AAA server is no longer accessible

Certificate-based Authentication

Certificate-based Authentication:

• With public & private keys, we can create a certificate that would be private to you & you'd use this to authenticate
• Many people will put these certificates on a smart card so they can authenticate with the smart card
• PIV (Personal Identity Verification) Card:
    ■ Used by US Federal Government, it's their “smart card”
    ■ Contains picture & identification information
• CAC (Common Access Card):
    ■ Used by US Department of Defense, it's their “smart card”
    ■ Contains picture & identification
• Smart cards aren't the only way to store these certificates, they can also be stored on a laptop or a USB drive (plus more)
    ■ This is done with IEEE 802.1X
    ■ Storing the certificate on-device storage or separate physical devices

Auditing

Auditing:

• With these centralized authentication functions, we gain lots of info regarding whose using the network & when they're using it. We have info regarding where they're logging in from, what resources they're accessing, etc. We can log all these access details which may include details pertaining to OS logins, VPN logins, device access, etc
• With all of this info logged, we can then go back & provide audits of this info to be sure people are logging in from the correct locations & people are accessing the appropriate resources for their particular login
• We can even create rules for our AAA server that are based on the time-of-day (time-of-day restrictions) (**EX**: If there is a particular lab that no one should be accessing after normal working hours, we can create a rule in our AAA server that prevents access to those resources after a particular time of day)

Access Control

Network Access Control (NAC)

Network Access Control (NAC):

• NAC uses IEEE 802.1X which is port-based & basically makes it so people can't access the network until they've authenticated.
    ■ When we refer to port-based in this case, we are referring to physical ports & physical access to the network
• If you're using 802.1X for NAC, then you're probably using a type of EAP to provide the authentication (EAP = Extensible Authentication Protocol & there is a AAA server that's either running TACACS or RADIUS that usually verifies that authentication)
• It's good to use NAC but remember to disable unused ports on your switches
• Enable MAC address checking functions in switch to ensure that nobody can get around some of the functionality of NAC by spoofing a MAC address

Port Security

Port Security:

• Another function to control access
• Prevents unauthorized users from connecting to a switch interface (set it to disable port or alert you if someone connects)
• Port security is based on MAC address of the device connecting (even if the MAC address is being forwarded from another switch then it still looks at the MAC address to make the decision)
• You can set up each port on a switch to have unique rules in terms of allowing/disallowing certain MAC addresses on the network

Port Security Operation:

• You configure your switch with a max number of MAC addresses allowed on an interface
    ■ You decide how many MAC addresses are too many
    ■ You can also configure specific MAC addresses
• The switch then monitors the number of MAC addresses connected to the interface & maintains a list of every MAC address & once you exceed the maximum then port security activates & the default option is to disable the interface that exceeded the threshold

Captive Portals

Captive Portals:

• Another good way to provide access to networks
• Captive portals are common on wireless networks
• When connecting to a network your device is checked against a list of devices that are allowed access to the network & if you aren't in the list then you're presented with a captive portal login prompt
• Once authentication via captive portals is accepted your session begins until either you're automatically logged out or you log out yourself.

Wireless Network Security

Wireless Encryption

Wireless Encryption:

• Wireless communication goes through air waves (every device on wireless network is a radio receiver & wireless transmitter)
• If someone is listening in on these frequencies they can listen in on all of the traffic going in & coming out of a wireless network
• To combat this, we use encryption where either everyone gets their own password to use on the wireless network or everyone uses the same password. This makes it so only people who have the correct credentials can transmit & listen for data on the network.
• One of the most common methods of encrypting data on wireless network is through the use of WPA2, but if you have older equipment you can use WPA.

WPA

WPA:

• WIFI Protected Access
• Created in 2002 to replace WEP (Wired Equivalent Privacy had serious cryptographic vulnerabilities)
    ■ The cryptographic vulnerability allowed all traffic to be decrypted.
• WPA used security protocol TKIP (Temporal Key Integrity Protocol) which used the RC4 stream cipher.
    ■ Initialization Vector (IV) is larger in WPA than it was in WEP & uses an encrypted hash
    ■ Every packet with WPA gets a unique 128-bit encryption key

TKIP:

• The info about the encryption key sent across the network with TKIP would change constantly since it combined the secret root key with the Initialization Vector (IV)
• There was also a sequence counter added onto TKIP to prevent relay attacks
• TKIP also implements a 64-bit Message Integrity Checker to prevent against tampering of packets that were traveling through the wireless network
• TKIP has its own set of vulnerabilities & was deprecated from the 802.11 standard

WPA2 & CCMP

WPA2 & CCMP:

• WPA2 uses CCMP (Counter Mode Cipher Block Chaining message Authentication Protocol - encryption protocol) to encrypt the traffic going through the wireless network
• WPA2 uses AES (Advanced Encryption Standard instead of RC4
• CCMP effectively replaced TKIP
• Provides data confidentiality (through AES), authentication, & access control

CCMP Block Cipher Mode:

• Uses AES for data confidentiality
• Uses 128-bit keys and a 128-bit block size
• Requires additional computing resoures to generate keys

EAP

EAP:

• An authentication framework used to authenticate onto the network
• **EAP** - Extensible Authentication Protocol
• Contains many different ways to authenticate based on RFC standards
• WPA & WPA2 uses 5 EAP types as authentication mechanisms

EAP Types

EAP Types:

• **EAP-FAST**
    ■ EAP Flexible Authentication via Secure Tunneling
    ■ Provided light weight authentication method while also increasing the security needed for wireless networks
• **EAP-TLS (EAP Transport Layer Security)**
    ■ Same TLS used for web servers used for wireless authentication
    ■ Provides strong security & has had wide adoption
    ■ EAP-TLS has support from most of the industry
• **EAP-TTLS (EAP Tunneled Transport Layer Security)**
    ■ Allows us to tunnel other types of authentication methods through existing encrypted EAP communication so you can use any authentication you can support & you maintain the security with TLS
• **PEAP (Protected Extensible Authentication Protocol)**
    ■ Created by Cisco, Microsoft, & RSA Security to provide EAP within a TLS tunnel
    ■ Commonly implemented on Microsoft devices as PEAPv0/EAP-MSCHAPv2 (MSCHAP since it authenticated to the Microsoft's MS-CHAPv2 databases)
    ■ PEAP combines a secure channel & EAP

Wireless Security Modes

Wireless Security Modes:

• These are the configuration options you have to choose from on a wireless access point/wireless router
• **Open System:**
    ■ No authentication password is required.
    ■ Anyone can access network
• **WPA2-Personal/WPA2-PSK:**
    ■ WPA2 with a pre-shared key
    ■ Everyone uses the same 256-bit key to authenticate & access network
• **WPA2-Enterprise/WPA2-802.1X:**
    ■ Authenticates users individually (with registered accounts) with an authentication server (**EX**: RADIUS)
    ■ Uses 802.1X to provide access control to wireless network
    ■ You login with normal user & password & the system authenticates these credentials to a backend AAA server & you gain access to the wireless network

MAC Filtering

MAC Filtering:

• Can be performed on both wired & wireless networks
• You define the allowed MAC addresses on your access point & it sets up an **implicit deny** rule (like with firewalls) which means that if the MAC address isn't on the allowed list, it automatically rejects it
• You can easily find the MAC addresses on a wireless network through LAN analysis which would lead to someone spoofing their MAC address to MAC addresses that may be allowed onto the network & connecting.
    ■ This is one reason why MAC filtering is often referred to as security through obscurity

Geofencing

Geofencing:

• Some MDMs (Mobile Device Managers) allow for Geofencing which can restrict or allow features when a device is in a particular area. (**EX**: Disabling camera functionality of phones & tablets if the device is inside the facility)
• Geofencing can also be used for authentication:
    ■ It can be used to only allow logins when the device is located in a particular area.

Wardriving

Wardriving:

• Wardriving is combining a WIFI monitoring system & a GPS and driving around gathering information about the wireless networks that are located inside of organizations
• Wardriving has also been extended to Warflying, Warbiking, etc

Device Hardening

Changing Default Credentials

Changing Default Credentials:

• Most network devices have default usernames & passwords, change them
    ■ These default credentials can be found on routerpasswords.com
    ■ These default credentials will provide admin access

Upgrading Firmware

Upgrading Firmware:

• Many network devices don't use traditional operating systems (windows, linux, etc) & if you need upgrade these systems then you are normally looking to perform an upgrade to the firmware of the system
• If you're upgrading to a firmware version, make sure to clarify that there are no known security vulnerabilities associated with the version you're upgrading to.
• Although you may be upgrading the firmware in an effort to solve problems you are encountering, the upgrade may introduce new problems so be prepared to have a rollback plan just in case.

Patch Management

Patch Management:

• For the network devices that are running Windows, Linux, etc you want to ensure these devices have the latest patches which can provide:
    ■ System stability
    ■ Security fixes
    ■ But be wary, patches can introduce new vulnerabilities and/or problems so be prepared to rollback to the previous version.
• Sometimes for example in Windows, they offer a large amount of patches in a bundle called a service pack that is available to download.
• There can also be emergency updates that are sent out that address zero-day vulnerabilities and/or exploits or address important security discoveries, so be sure to be aware these exist.

File Hashing

File Hashing:

• Hashing produces a message digest of the text/data ran through it
• Hashes allow us to provide integrity checks against files we download (to be sure the file hasn't been corrupted or maliciously modified)

Watching The Network

Watching The Network:

• It's easy to gain a wealth of information just by simply using a packet analyzer against a network, this can be done nearly everywhere.
    ■ This is why it's good practice to use encrypted protocols & technologies

Secure Protocols

Secure Protocols:

• If a VPN connection is unavailable & you want to be sure all traffic is going to be encrypted, make sure all your applications are using secure protocols (**EX**: SSH instead of Telnet, HTTPs instead of HTTP, SFTP or FTPs instead of FTP, etc)
• Setting up a VPN is always a good option as well, you can have your VPN using TLS but it can also use IPSec (Internet Protocol Security which encrypts at the IP packet level, AKA the **network** layer)

Generating New Keys

Generating New Keys:

• There is always an encryption key that's used when sending traffic over these encrypted mediums
• These encryption keys are usually managed on the device (**EX**: The TLS encryption keys for HTTPs are usually stored on the web server itself)
    ■ This is why it's important to protect these keys, anyone that gains access to them can potentially decrypt info they may have gathered with packet captures
• Sometimes these infrastructure devices & web services may ship to you with a default key, so you want to be sure to change it.
    ■ It's useful to have a formal policy to outline processes & procedures that must be followed in order to be sure that every device has its own unique key.

Disable Unused Interfaces

Disable Unused Interfaces:

• Disabling unused interfaces is useful to provide security, if there are any rooms that should not have access/do not need access to the switch, disable the interface connecting it to that location
• Disabling unused interfaces means that you may have to do research in order to determine what interfaces on that switch should be enabled & which should be disabled. If new devices are added, you need to be sure the disabled interfaces are also transfer over to the new device.
• **Network Access Control (NAC)** can also be used to provide additional security for unused interfaces
    ■ This will force individuals to provide additional authentication (username & password, etc) before they can interact/connect to the interface

Mitigation

Mitigation Techniques

IPS Signature Manager

IPS Signature Manager:

• With a IPS Signature Manager, you determine what happens to any traffic if it matches the signatures while going through your network
    ■ You can block it, allow it, send an alert, etc
• There are thousands of different rules in an IPS & you have to determine what the outcome is for every single rule
• Rules can grouped together by different functions & define what happens with the larger group

Device Hardening

Device Hardening:

• No system is secure with default configurations
• Manufacturers of network devices often provide a hardening guide
• There are also other general-purpose guides that show how to harden network devices available online

Native VLAN

Native VLAN:

• This is different from the “Default VLAN" which is the VLAN assigned to an interface by default
• This is used when trunking different switches together
• If you're sending traffic across a trunk & the traffic belongs to the Native VLAN (it's coming from the Native VLAN) then an 802.1Q header won't be added. These are often referred to as non-trunked frames
• To separate out any user traffic from network management traffic, you may want to change the Native VLAN value to be some other value (EX: Changing Native VLAN to VLAN 999)
    ■ This is helpful as some Cisco management protocols use VLAN 1 & Native VLAN defaults to VLAN

Privileged Accounts

Privileged Accounts:

• Administrator/Root access gives complete access to the system so the user can manage hardware, drivers, & install software
• Who has access to these administrator logins would need to be controlled tightly & be highly secured which can be accomplished through:
    ■ Strong passwords & 2FA implemented
    ■ Scheduled password changes (related to password expiration dates)
• Regular user accounts have limited control, these accounts should have different access rights when compared to administrative accounts

File Integrity Monitoring (FIM)

File Integrity Monitoring (FIM):

• Some files change all the time (**EX**: Log files) but there are files that should never change (**EX**: OS files, internal files, etc)
• Many security breaches begin by someone changing one of these files that shouldn't be changed, so you may want to enable **FIM**:
    ■ Enabling **FIM** gives you the ability to scan in real time or on demand to detect if any of the files

have been changed
• In Windows there is **SFC (System File Checker)**:
    ■ Looks at Windows's files to be sure they havent been changed
• In Linux, there's an agent from **Tripwire**:
    ■ If any system files change, you will be alerted via the tripwire agent
• There's also lots of host-based IPS options which can monitor individual systems & send out alerts if any important files change

Restricting Access via ACLs

Restricting Access via ACLs:

• There should only be certain people allowed to login to network devices, this can be ensured via ACLs
• Use device ACLs to limit access to important infrastructure devices
• ACLs can be configured so only people on network management/network security subnets would have access to infrastructure devices & all other traffic inbound to those devices would be dropped
• This is a bit different than setting up an ACL for application access:
    ■ This is used mostly for access to management interfaces for networking devices
    ■ Traffic from unauthorized users is dropped

Switch Port Protection

Loop Protection

Loop Protection:

• Connect 2 switches to each other & they'll send traffic back & forth forever due to there being no “counting” mechanism at the MAC layer
• As more traffic is added to the network, more traffic begins to flow into this loop making it easy to bring down a network.
    ■ Loops are somewhat difficult to troubleshoot but they are easy to resolve if the loop's location is known
• IEEE Standard 802.1D is the standard to prevent loops in bridged (switched) networks
    ■ AKA **Spanning Tree Protocol (STP)**
    ■ Created in 1990
    ■ Used practically everywhere on all switching devices
    ■ **Spanning Tree Protocol (STP)** makes certain ports block ports if it suspects that enabling the port would cause a loop
    ■ STP recognizes any changes in the network infrastructure (**EX**: In the case of a particular connection experiencing problems which would lead to network A not being able to communicate through a certain switch, STP would recognize there was a change & examine & determine if there is a need to remove any blocked ports to allow a network to communicate to another network)

BDPU Guard

BDPU Guard:

• STP can take a while for the network convergence (if there is a problem with the connection & a switch/bridged network's only route to communicate with another switch/bridged network is cut off) to occur

■ On some switches you have the option to bypass the listening & learning states of the switch so devices can immediately begin communicating (this is listening & learning the network infrastructure), this bypass is called **BDPU (Bridge Protocol Data Unit) Guard.**

■ This bypass of the listening & learning state is called **PortFast** on Cisco switches

• **BDPU (Bridge Protocol Data Unit)** is the protocol Spanning Tree uses to communicate between all the different switches

■ An end user device (laptop, PC, etc) will never send BDPU frames

■ BDPU frames are only sent to & from switches that are participating in Spanning Tree

■ If a BDPU frame is detected on a PortFast configured interface (i.e., a workstation), the interface is automatically shutdown as workstations shouldn't be sending BDPUs so this indicates that there must be a switch on that end that can cause a potential loop.

• This BDPU guard should only be enabled on interfaces that you are 100% sure are only going to be used by end station devices

Root Guard

Root Guard:

• Another method of protecting switch interfaces

• On any spanning tree network, there is going to be 1 switch that is considered the root switch or root bridge & you can manually determine which device this is by setting the root bridge priority to 0 in the configuration of the switch

■ But this doesn't always guarantee root, if any other device also happens to have a root bridge priority of 0 then Spanning Tree will choose the device with the lowest MAC Address to be the root switch/ bridge

• **Root guard** allows you to pick the root bridge & prevents rogue root bridges

■ Lets say someone decided to connect a bridge that has a lower MAC address with the bridge priority of 0 to the network, without root guard, it would choose this new device as the new root bridge but with root guard, it prevents this from happening.

Flood Guard

Flood Guard:

• A method to limit the number of devices that can communicate through any particular switch interface

• Flood guard's default is to disable the interface if the number of MAC addresses on a switch exceeds the maximum

• Flood guard also prevents a DoS attack where an attacker would flood the network w/a number of different MAC addresses in order to overflow the number of MAC addresses on a switch

DHCP Snooping

DHCP Snooping:

• One way of causing problems on a network is installing & launching your own rogue DHCP server that then begins handing out IPs that are different from the official DHCP server

■ To prevent this we can enable DHCP snooping on your switch, the switch effectively becomes a firewall. This allows you to configure certain interfaces on your switch to be considered trusted, (**EX**: Routers, switches, DHCP servers) & you could then define other interfaces as untrusted

■ This allows your switch to begin “watching/listening” for DHCP conversations & it “learns” & adds a list of untrusted devices to an internal table of the switch

■ If the switch sees static IP addresses, rogue DHCP server responses or other invalid traffic, it can filter that info from those untrusted interfaces.

Network Segmentation

Segmenting the Network

Segmenting the Network:

• Physical, logical, or virtual segmentation
    ■ Devices, VLANs, virtual networks
• Segmenting the network may be attractive due to performance reasons
    ■ If we divide the network into smaller chunks, we have the opportunity to increase the bandwidth of high-bandwidth applications
• Segmenting the network may be attractive due to security reasons
    ■ You may want to be sure that certain users aren't able to communicate to certain servers or certain applications should only be able to communicate w/each other
• Segmenting the network may be attractive due to compliance
    ■ You may want to be sure that PII or CC info is segmented from other parts of the network

Physical Segmentation

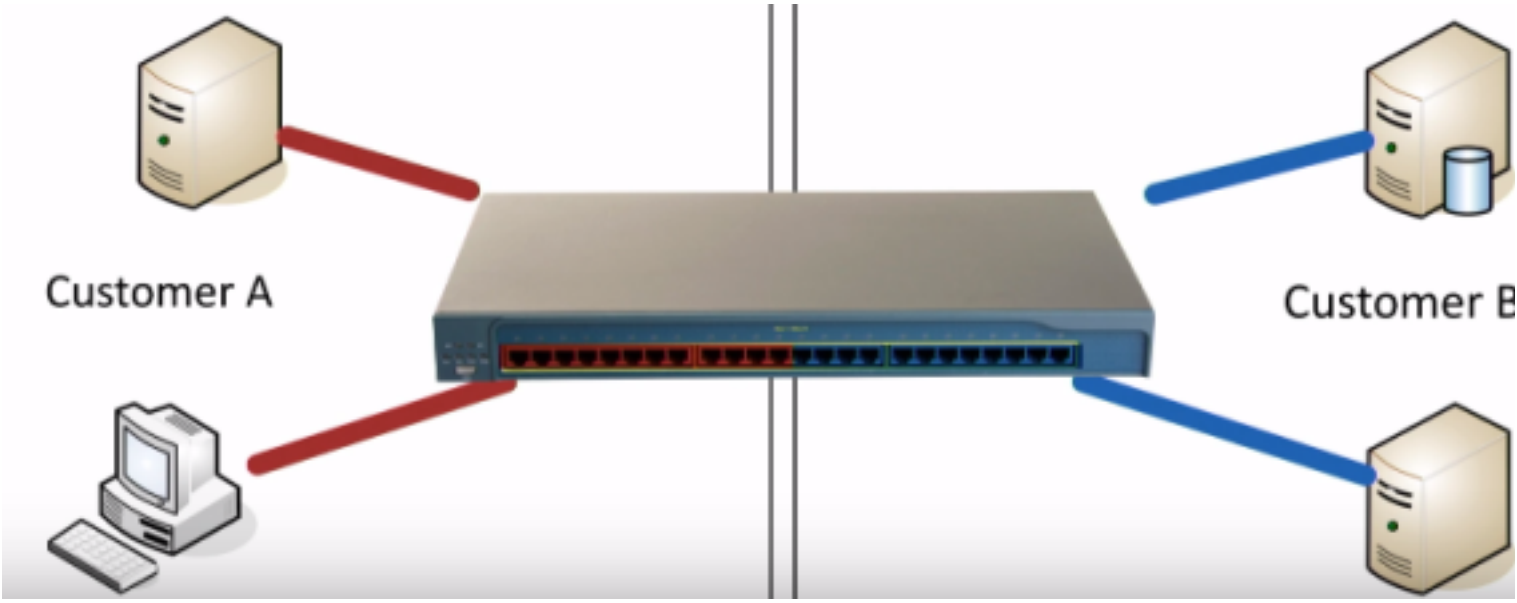
Physical Segmentation:

• Devices are physically separate
• The only way that the two physically segmented devices would be able to communciate is if they were connected in some way:
    ■ Through a direct connection
    ■ Through another switch or router
• You may use physical segmentation with web servers in one rack while database servers are in another rack & these servers would communicate to their respective switches.
• Physical segmentation can also be based on applications, you can have Application A servers in one rack with its own switch while Application B's servers are on another rack with a completely different switch.

Logical Separation with VLANs

Logical Separation with VLANs:

• Separation via VLAN maintains the separation aspect of physical separation (the aspect that the 2 devices cannot communciate w/each other & be mixed up with each other) but in the logical sense & it is more efficient with the devices used (specifically switches)
    ■ With physical separation, lets say you were physically separating customer data, you'd have to use a different switche for each new customer & this switch will likely only have 2-3 cconnected devices which leaves wasted port real estate. This separation can be accomplished via VLANs except without the waste of port real estate (you only need 1 switch, see photo)



- In a VLAN, if you need to communicate between VLANs, you would need a Layer 3 device (such as a router or a firewall in a high security environment)

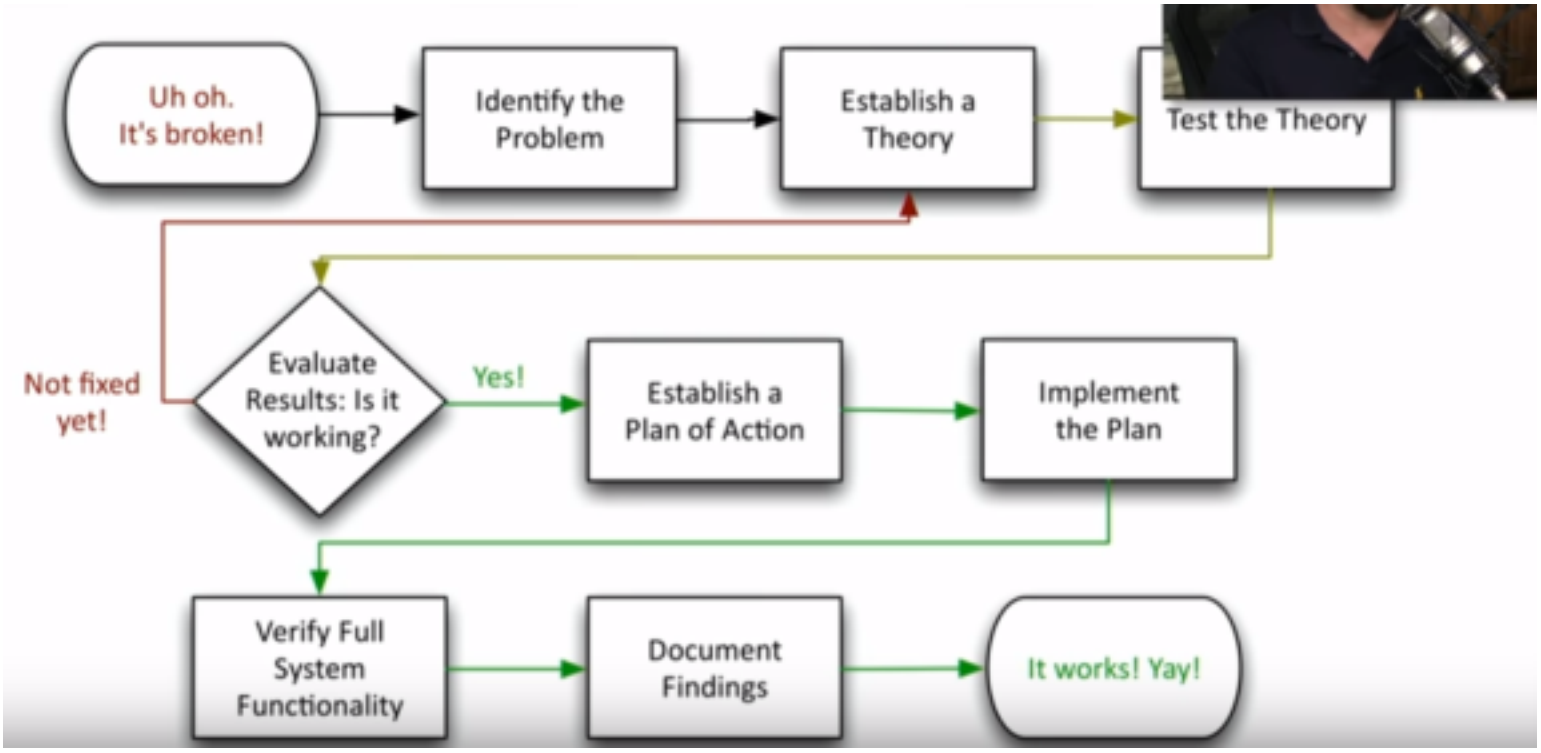
DMZ

DMZ:

- An additional layer of security between the Internet & you.
- Used when you have some resources that you want people to be able to access from the Internet (**EX**: Web server) but you still want to protect the internal network from being accessed from the Internet.
    - DMZ is commonly paired with a firewall
    - Rules would be created in the firewall to redirect IPs to the DMZ where the resource you want to be accessed from the Internet would be located but prevent any access from the Internet to the internal network

Network Troubleshooting & Tools

Network Troubleshooting Methodology



• Above is the flow chart for the methodology

Identify the Problem

Identify the Problem:

• Gather as much info about the issue that's occurring
• Duplicate the issue, if possible
• Identify & document any symptoms that may be occurring from the problem, even if the symptom doesn't seem as if it could be occurring due to the problem
• Some issues may be identified by the end users, question them to gather valuable info
• Determine if anything has changed (change control comes in handy here)
• There may be multiple problems that may not have anything to do w/each other, it's important to approach these multiple problems individually & break them into smaller pieces

Establish a Theory

Establish a Theory:

• Once you've gathered as much info as possible, you can examine these details & establish a theory of what you think is likely going wrong
• Consider everything that may be causing this issue
    ■ Consider even the not-so-obvious
    ■ Examine the problem from the top of the OSI model to hte bottom or from the bottom of the OSI model to the top
• Make a list of all possible cause
    ■ Start with easy theories
    ■ Include the complex theories when moving up the list

Test the Theory

Test The Theory:

• Confirm the theory
• If you're able to recreate the problem in a lab, you can now apply each theory till you find the one that resolves the issue
    ■ After each theory is tested, you want to reset the lab

Create a Plan of Action

Create a Plan of Action:

• Once the theory is tested & it's determined the theory will resolve the issue, building & documenting a plan is the next step
    ■ Correct the problem with a minimum of impact on the production network
    ■ Some issues won't be able to be resolved during production hours
• Identify potential effects (**EX**: you may run into problems if the soluton is upgrading software in network devices, having a backup plan for safety is a good idea)
    ■ Have a plan B
    ■ And a plan C

Implement the Solution

Implement the Solution:

• After the plan is documented, you can take it to your change control team & they can give you an available window when that change could be implemented
• The available change window may be small so it's appropriate to bring in assistance from a 3rd party

Verify Full System Functionality

Verify Full System Functionality:

• Once you have implemented the changes, your job isn't done
    ■ Now you have to test the system to be sure that those changes actually fixed the problem
    ■ You can verify full system functionality by bringing in the users who originally experienced the problem & having them test the system
• This may be a good stage to implement preventive measures
    ■ To ensure that the appropriate people are alerted if the problem occurs again
    ■ Or to ensure that there are alternative options to use if the problem occurs again

Document Findings

Document Findings:

• Once it's all resolved, it's time to document findings
    ■ Here you will document the entire process from the beginning to the end.
    ■ You want to provide as much info as possible so that if anyone runs into the same problem again, they can simply search your “knowledge base” & find a solution

Network tools

Command Line Tools

Flavors of Traceroute

Flavors of Traceroute:

• Not all traceroutes are the same, there are minor differences in the transmitted payload
• Windows commonly sends ICMP echo requests (same requests used in ping):
    ■ receives ICMP time exceeded messages (AKA TTL down to 0)
    ■ And an ICMP echo reply once it reaches the final destination
    ■ But outgoing ICMP is commonly filtered via firewalls
• Some operating systems allow you to specify the protocol used:
    ■ Linux, Unix, Mac OS, etc
• IOS mobile devices send UDP datagrams over port 3343
    ■ With some extendable options in IOS, you can change the port number
• Regardless of the OS being used, the basic operation of traceroute will be the same across all OSes

nslookup & dig

nslookup & dig:

• both commands allow a user to lookup info from DNS servers
    ■ Grabs canonical names, IP addresses, cache timers, etc
• **nslookup**:
    ■ Used in Windows, Mac OS, Linux, etc
    ■ Lookup names & IP addresses from DNS server
    ■ Deprecated now (use dig instead)
• **dig** (Domain Information Groper):
    ■ Provides more advanced info but also the same info nslookup is capable of providing
    ■ Not native to Windows distros but you can download a version for Windows

IPtables

IPtables:

• Stateful firewall:
    ■ Linux iptables - Filters packets in the kernal
    ■ Usually placed on a device or server
• Firewall functions:
    ■ IPtables offers advanced filtering by IP adresses, ports, applications, content of packets
    ■ Some linux distros prefer **firewalld** or similar host-based firewalls over iptables
    ■ The IPtables firewall is usually located on the ingress/egress of a network (Entrance/exit of a network)

Netstat

Netstat:

• Available on Windows, Linux, Mac OS, etc
• Provides many different views of what the statistics are of network communications on a particular device
• **netstat -a**
    ■ shows all active connections
• **netstat -b**
    ■ shows all active connections + the Windows binary that was used to create that connection across the network
• **netstat -n**
    ■ do not resolve names

tcpdump

tcpdump:

• Captures packets from the command line
• tcpdump is included in many linux & unix distros
    ■ There is a version for Windows called WinDump
• You can apply filters, view packets go by in real-time
• You can even save all the packets collected into a pcap formatted file (file format that is easily readable by packet analyzers such as wireshark)
    ■ useful if you want to view the packets in another application

pathping

pathping:

• Native to Windows, combines ping & traceroute functionality
    ■ Included with Windows NT & later
• There are 2 phases to pathping
    ■ **Phase 1** - runs a traceroute & builds a map between your device & another device
    ■ **Phase 2** - begins to measure round trip time on every link along the way & also measures packet loss at each hop. Takes a little bit of time to run but is useful

Route

Route:

• Another important piece of info when troubleshooting a device is knowing where traffic will be routed based on what the destination IP address is:
    ■ In Windows, we can view this with the **route print** command

Address Resolution Protocol (APR)

Address Resolution Protocol (APR):

• You can determine a MAC address based on an IP address of a device
• **arp -a**
    ■ Shows ARP table in Windows' devices
    ■ If there is no MAC address associated with an IP address, you can ping the IP to gain the MAC address

Software Tools

Protocol Analyzer

Protocol Analyzer:

• Used to solve complex application issues
    ■ Allows user to get into the details. Captures every frame that goes between devices in the network (whether that be wireless or via wired connections)
• Protocol analyzers can be software or built into router or switches in your network
• With a protocol analyzer you can view traffic patterns
    ■ You gain the ability to identify unknown traffic
    ■ You can verify packet filtering & security controls are working properly

Wireless Packet Analysis

Wireless Packet Analysis:

• Troubleshooting wireless networks can be challenging as wireless sends signals to whoever is in range & any device that wants to listen can do so if they want since everything is sent via the airwaves
• If you're using software that's listening in on the network then the software needs to disable the transmission function of the wireless card because if you're transmitting, you won't be able to hear anything else on the wireless network.
• You also want to be sure you have the correct wireless interface card to perform the analysis functions:
    ■ Some network drivers won't capture wireless information
    ■ You need specialized adapters (wireless adapters, etc)/chipsets & drivers to put the card into this wireless analysis mode (AKA **promiscuous mode**)
• With wireless packet analysis you ca nview wireless-specific info such as:
    ■ signal-to-noise ratio, channel info, etc
• Wireshark is a good wireless packet analyzer

Hardware Tools

Cable Crimpers

Cable Crimpers:

• Allows user to fasten the RJ45 connector to the end of the wire
• Some crimpers also provide other connections so you can crimp RJ11 or coaxial connections on the

same crimper 

Crimping Best-Practices

Crimping Best-Practices:

• Get a good crimper
    ■ And get a good pair of electrician's scissors/cable snips in order to work easily with small cables
    ■ And get a good wire stripper (useful if you're working with coaxial cables) (**NOTE**: A number of crimpers will actually include a wire stripper on the crimper itself)
• Make sure you're using the correct modular connectors for the type of cable being used
    ■ There are differences between wire types (**EX**: The type of connectors that go on a CAT5 cable are slightly different than the ones that go on a CAT6 cable)

Cable Testers

Cable Testers:

• After you've performed this crimp, how do you know the crimp is actually working?
    ■ 1 way to tell is to put a cable tester on the wire
    ■ The cable tester performs a continuity test on the wire to see if pin 1 is connected to pin 1, pin 2 is connected to pin 2, etc.
    ■ The cable test can identify missing pins or if there are any wires that may have crossed between any of the pins
• Cable testers aren't used for frequency testing
    ■ If you wish to test things like cross talk, signal loss, etc you likely want to bring in a **TDR (Time Domain Reflectometer)**

TDR & OTDR

TDR & OTDR:

• **TDR** = Time Domain Reflectometer
• **OTDR** = Optical Time Domain Reflectometer
    ■ Used when working with Fiber
• These can provide lots of info about copper or fiber cable
    ■ Once plugged into connection, it can estimate cable lengths
    ■ It can identify splices/cuts/breaks & identify how far down the cable that particular problem exists
    ■ If you're simply attempting to figure out the type of cable, it can tell you this info as well
    ■ These devices are commonly used when first installing a cable infrastructure due to them being able to detect the amount of signal loss from one end of the cable to the other end
    ■ These devices often work with software which allows you to log every cable you're testing so you can create a report that everything on the network is functioning as expected

The TDR

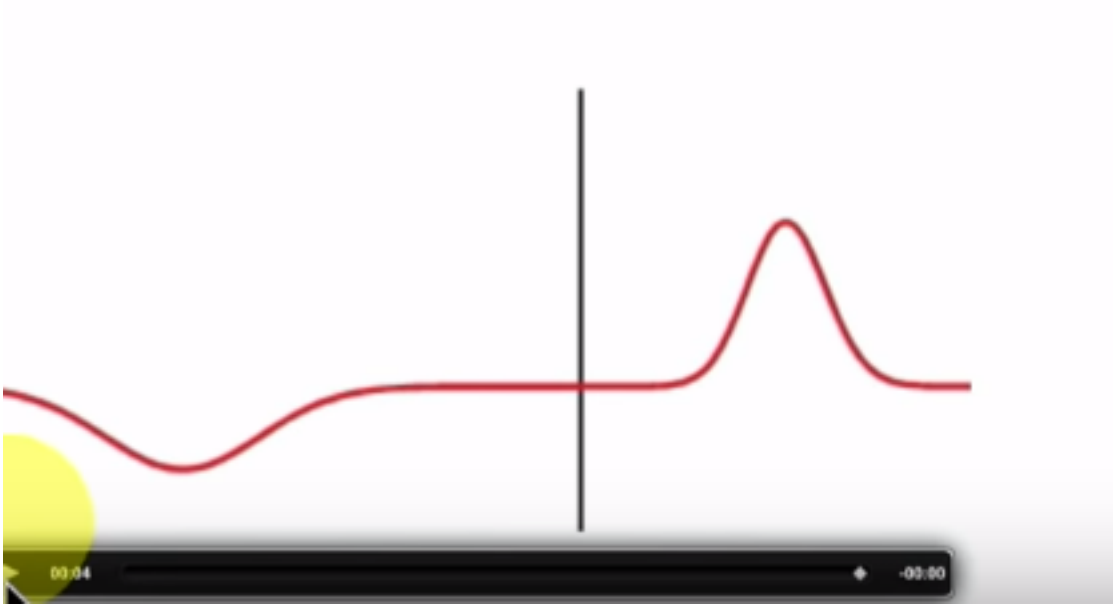
The TDR:

• TDR is able to determine where these breaks are by sending an **electrical pulse** down the cable (like a radar “ping”) & then it listens for any **reflections** that are coming from any problems, the TDR then calculates the time it took to send that signal & the time it took to hear the reflection & tells you the distance between those 2

- **Impedance discontinuities cause a reflection** which is why the TDR listens to these

• The OTDR does the same except with light instead of electrical pulses:

- It then watches for any reflections to come back



• Notice how how the small “pot hole” on the left is being reflected back, this is the reflection & it indicates there is a problem

Using a TDR/OTDR

Using a TDR/OTDR:

• An expensive tool & may require additional training to actually operate the hardware since there are many features & many metrics to be read & be able to understand results its providing
    ■ Costly tools, especially for fiber
• If you want some way to certify that your cables & fibers are working as expected then this would be the tool you want to use
    ■ You can validate everything about your installation & certify that your network connections are working exactly as expected

Punch-Down Tools

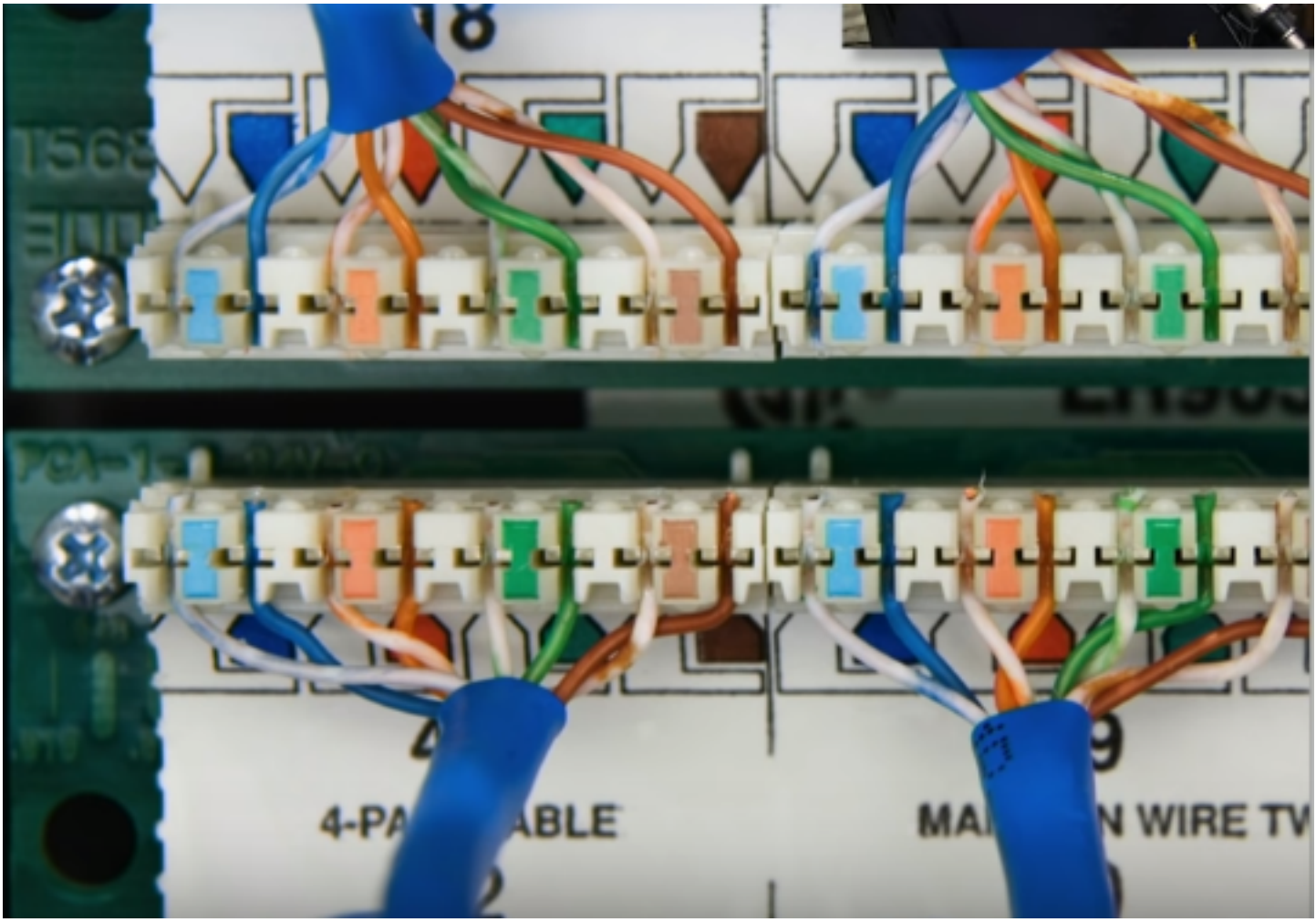
Punch-Down Tools:

• If you're working with patch panels, you'd probably be using a punch-down tool:
    ■ It pushes the cable into sharp connections on punch down block (AKA wiring block) & locks those wires in place
    ■ It also trims off excess of the wires during the punch
• You effectively “punch” a wire into a wiring block:
    ■ You would use this with a 66 block or a 110 block most commonly on today's network.

Punch-down Best Practices

Punch-down Best Practices:

• When you're working with patch panels & punch-down tools you want to be sure you're organized:
    ■ There are a lot of wires in a small space
    ■ Cable management is key

■ **EX**: 

■ This patch panel numbers each connectors & shows you exactly where the wires go while punching them down

• On today's high speed ethernet network, you want to be sure to maintain the twists in the wire as close as possible to where it enters the punch down block

• Once you've connected the patch panels document everything

■ Which interfaces is connecting w/which desk out on the floor or which workstation

Light Meter

Light Meter:

• When you're working with RJ45 connectors & crimping your own cables, it's common to use cable testers to test if there is continuity for all 8 of those pins

• If you're running fiber, you want similar tests

■ **You won't be testing continuity with fiber** though, you simply see how much light is making it's way from one end of the fiber to the other end.

■ To test the amount of light getting through the fiber, you use a light meter (this is simply seeing how much signal is making it through that fiber run)

• The light meter will send a light (either laser or LED depending on the type of light meter being used) from one side & have another device which measures how much light is received on the other end of the fiber

• If you have a long fiber run & you're concerned about not all of the light coming through, it's useful to use this tool to see what the results once you connect the production equipment

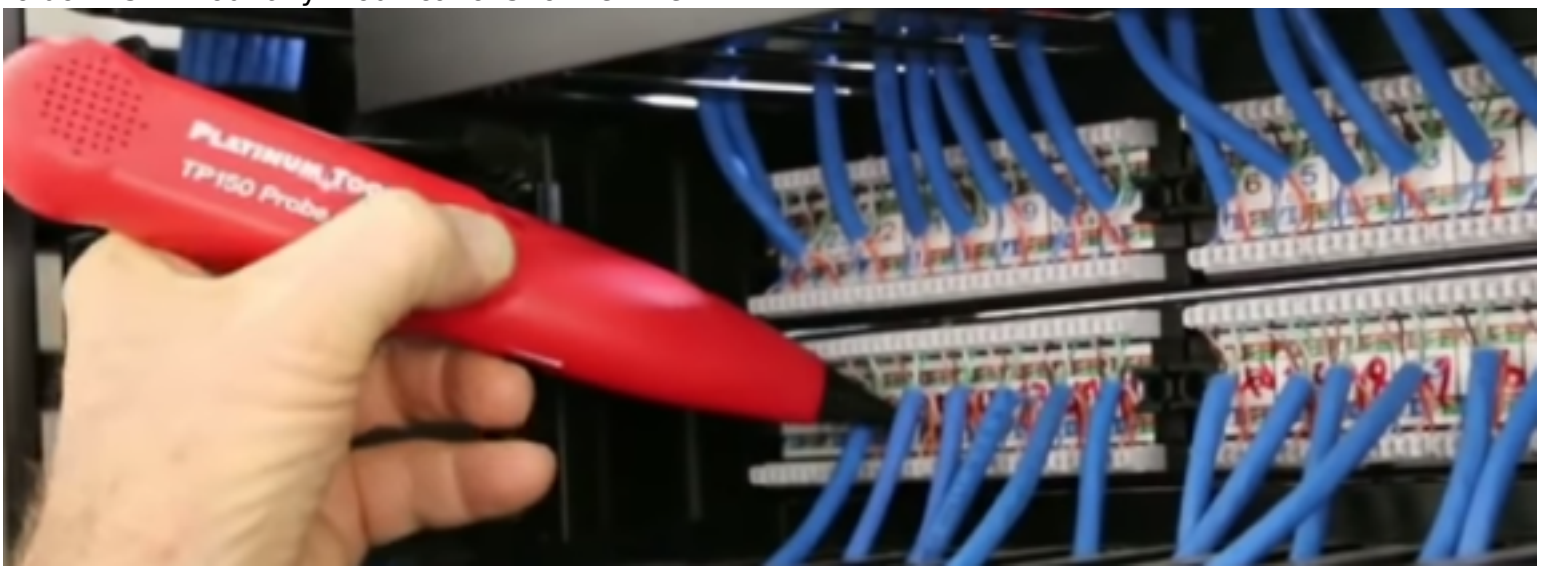
Tone Generator

Tone Generator:

• If you're working with a patch panel or you're simply working with lots of wires in a room & you're attempting to figure out where the other end of a wire is, you want to use a **tone generator**:

■ The tone generator puts an analog sound on the wire & then you use a separate inductive probe to determine where the other end of the wire happens to be (you hook up the tone generator with one end of the cable & the generator has differnet modular jacks that can fit onto any cable & you simply use the inductive probe by touching it on the other ends of the cables & the probe will mimic the sound the tone generator generates once it's found)

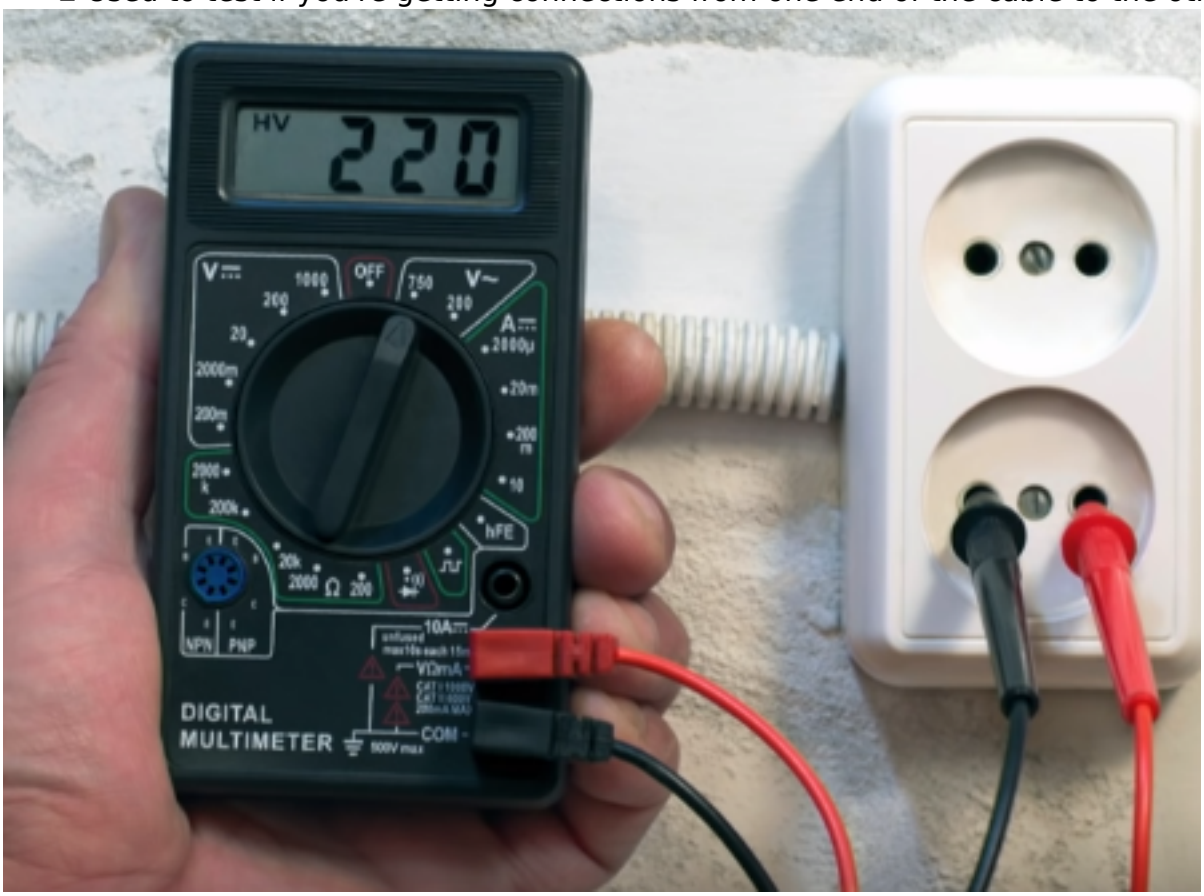
■ With this, you don't need to break the wire open or touch any copper, the inductive probe allows us to do this without any modifications to the wire



Multimeters

Multimeters:

• Tools that allow you to test AC voltage
  ■ Allows you to see if you're getting power out of an outlet
• Also allow you to check DC voltage
  ■ To check the voltage on the inside of network devices
• Multimeters even have continuity tests
  ■ Used to test if you're getting connections from one end of the cable to the other end



Spectrum Analyzer

Spectrum Analyzer:

• Good for wireless networks
• Allows you to examine all the different frequencies that happen to be in a particular range
• If you're connecting a Wireless Access Point & wondering if there is anything that is operating on the same frequency that may be of interference, a spectrum analyzer will be able to detect that
• The spectrum analyzer views everything across a particular set of frequencies so if there are other devices that are causing interference on the same frequency it will show up on the spectrum analyzer

Wired Network Troubleshooting

Signal Loss

Signal Loss:

• Whether you're using fiber or copper, the signal will begin to degrade as it goes farther & farther in distance
• This signal loss is referred to as Attenuation
    ■ This is the loss of strength as the signal moves through a medium (the medium being either copper fiber cabling, & even wireless)

Decibels (dB)

Decibels (dB):

• This is 1 way to numerically quantify the strength of a signal is with Decibels
• 1 decibel = 1/10 of a bel
• If you were to measure twice the amount of signal across a line, you would say it increased 3 decibels
    ■ This is due to decibels being measured on a logarithmic scale

dB Loss Symptoms:

• 1 of the most common symptoms is no signal
• This is where it'd be useful to have a TDR or an OTDR to test how much signal you're able to put through a particular medium

Latency

Latency:

• the difference between the request & the response
    ■ The waiting time
• Some latency is acceptable & considered normal
    ■ There is latency due to electrical signals having to go down the wire & for them to come back
    ■ But it's when the delay begins to become excessive that problems begin to occur.
• It's common to use packet capturing tools when troubleshooting latency to see specific time stamps of when you send a request & when you get a response

Jitter

Jitter:

• Since there are lots of real-time applications, the delays that are experienced in these applications is known as jitter
• Real-time applications are very sensitive to delay/jitter as if you miss a packet, most of the time there isn't any retranmission (due to UDP being used)
    ■ Even if the application isn't using UDP & provides retransmission, for some applications, there is no time for retransmission of data (**EX**: In a VOIP call, retransmitted data would cause confusion in phone calls)
• Jitter measurements are the time between frames

• The first line is a normal transmission of frames & below is where frames begin to experienc excessive jitter & frames begin to fail to transmit

Troubleshoot Excessive Jitter:

• The first thing you may want to look at the amount of used bandwidth & compare it to the amount that you have according to agreements w/your ISP
    ■ If excessive bandwidth is being used, receiving real-time info/data (or any data for that matter) will be challenging
• Switches & routers can also contribute to jitter:
    ■ Be sure your switches & routers aren't queuing up information or have excessive congestion & that they aren't dropping any frames as the frames come into the network
• Many times, QoS (Quality of Service) is being applied in networks:
    ■ This is where you prioritize real-time communciation services

Crosstalk

Crosstalk (XT):

- When signal that's crossing 1 pair of wires interferes the signal on another pair of wires
  - Can affect the overall performance of a connection
- TDRs can measure the amount of crosstalk that is occurring on a particular set of wires
- **Near End Crosstalk (NEXT)**:
  - One of the types of crosstalks that may be occurring
  - This is the amount of crosstalk that occurs at the transmitting end (AKA the near end)
- **Fair End Crosstalk (FEXT)**:
  - This is crosstalk that occurs as it goes through the network at the other side (The destination)
  - Both these measurements mean you can measure the amount of crosstalk when the signal was at its strongest (the near end) as well as the amount of crosstalk that occurs as the signal went through the cable (the far end)

Troubleshooting Crosstalk:

- There is always going to be a little bit of cross talk in copper cabled networks but an excessive amount is when further investigation would be required
- The first place to look should be the crimp that was added to the cable
  - Make sure the twists are maintained as they go into the RJ45 connector
- You may also consider using a differnet cable:
  - Perhaps using an STP
  - Or a category 6A cable which has an increased cable diameter which means there will be an increased distance between pairs which minimizes crosstalk
- It's important to perform an analysis of each connection before you plug in any devices in order to solve any issues before dealing with an actual productive network experiencing problems

Avoiding EMI & Interference

Avoiding EMI & Interferences:

- Proper cable handling:
  - No twisting - don't pull or stretch the cables
  - Each cable documents the maximum bend radius allowed, don't extend over this radius
  - Don't use staples or cable ties as these can affect the cables inside the cable
- Potential places to find EMI & interference with copper cables:
  - Avoid power cords, fluorescent lights, electrical systems, & fire prevention components
- A good way to test for EMI is to use a TDR & see exactly how much signal & noise appear on that cable
  - Test after installation so you can find most of your problems before use

Open & Shorts

Open & Shorts:

- A short circuit:
  - When 2 connections are touching each other (two wires inside an ethernet cable for example)
  - If someone has bent an ethernet cable, a short may occur
  - Can cause intermittent connectivity
- An open circuit:
  - The wire is completely open, there is basically a break in the connection
  - Causes complete interruption

Troubleshooting Opens & Shorts:

• Since these opens & shorts may be inside the cable, it's difficult to find exactly where they may be
    ■ In some cases, the wire has to be moved just the right way in order for connection to pass through
• These are also difficult or sometimes impossible to repair, it's easier to simply replace the cable
• A TDR can assist in finding exactly where the open or short in the cable happens to be
    ■ The TDR can tell you exactly how many feet away from the TDR the open or short in the cable happens to be

Troubleshooting Pin-outs

Troubleshooting Pin-outs:

• If you're someone who crimps your own RJ45 connectors onto ethernet cables then you know it's easy to switch cables around & have the incorrect pin-outs on these wires
    ■ When you plug in the wire, you may experience slowed speeds or simply no connection at all
• Visually inspecting the wire to see if you did punch things down in the correct order can be difficult since many connectors look alike
    ■ It may be useful to get a cable tester to see the pinouts between 1 side & another

T568A & T568B Termination

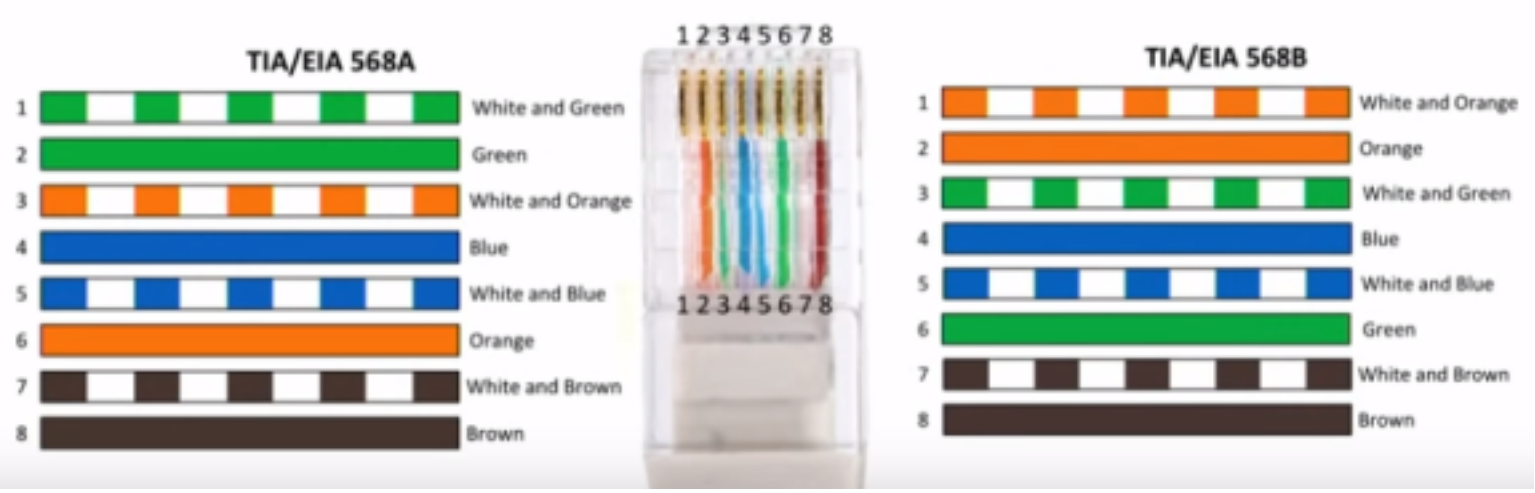
T568A & T568B Termination:

• The pin outs used for ethernet networks are an international standard
    ■ They come from the EIA/TIA-568-B standard
    ■ This specifies 8 conductor 100-ohm balanced twisted pair cabling

    ■
• There are 2 popular ways of performing pin outs on an ethernet cable:
    ■ The T568A & the T568B
    ■ You may even see that on certain connectors and/or punch blocks that there may be different colors that tell you which are for T568A & which are for T568B
    ■ These standards will show that most people will use T568A pin-outs for horizontal cabling (cabling that is on the same floor). But many organizations traditioanlly use 568B. As long as you choose one or

the other & stay consistent, you won't run into any problems
• If you punch down one side of a cable with a 568A standard & the other standard w/the 568B, you aren't going to have a straight through cable

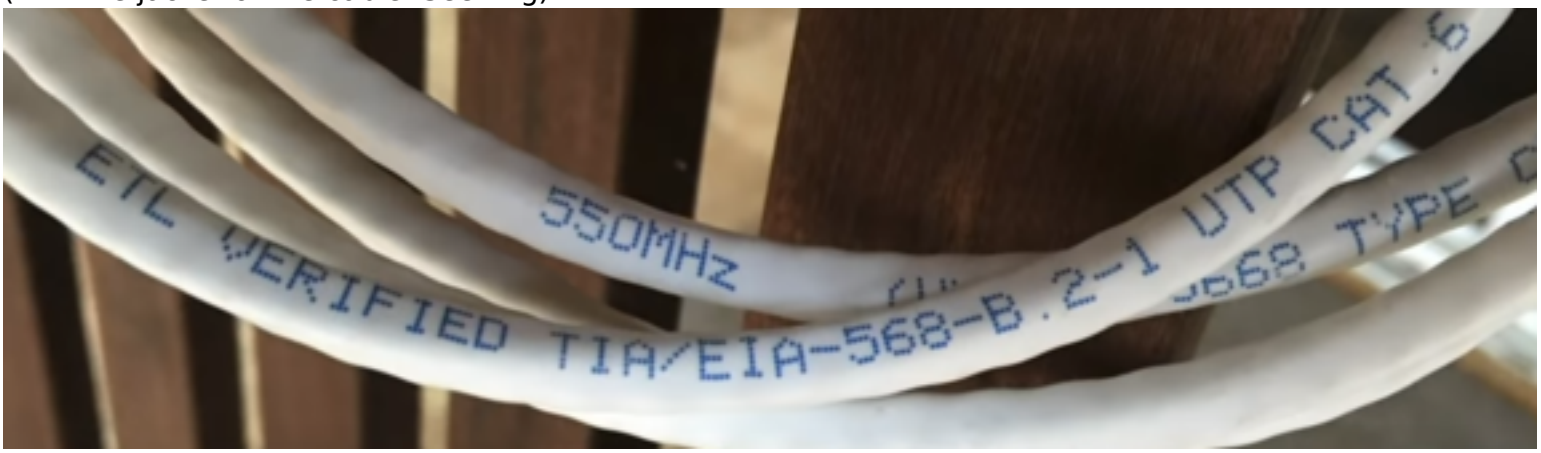
Visual Difference Between T568A & T568B



Incorrect Cable Type

Incorrect Cable Type:

• If you look at the statistics for your ethernet interface & see lots of CRC errors or physical errors:
    ■ You may want to check to confirm the correct type of cable is in use. One way to tell is to simply look at the outside of the cable & there may be info regarding the cable type printed on the sheath itself (AKA the jacket of the cable. See img)



    ■ You may want to confirm that the info printed on the sheath of the cable match with the actual specifications of the cable by using a TDR

Troubleshooting Interfaces

Troubleshooting Interfaces:

• If you're having issues with a cable or fiber & believe there are issues with it at the physical layer, you

will see errors appear on the interface that's connected to the cable
    ■ **EX**: You can look at the interface & see if there are any frame check sequence errors, oversized packets or late collisions
    ■ You may also look at the ethernet adapter configurations (the speed, duplex, VLAN to see if both devices are configured to be on the same VLAN, etc) on both sides of the connection & verify they match.
    ■ It's common to send traffic back & forth to these devices to see if any of these physical level errors are going to increase as more traffic is sent over the connection

Transceiver Match

Transceiver Match:

• If transceivers are in use, you should verify that the transceivers are matching the fiber or the connection that's being plugged into them
    ■ **EX**: If you're plugging fiber into a transceiver, the transceiver needs to match the wavelength of the fiber
• You also should verify that you're using the correct transceivers & optical fiber across the entire link
    ■ If you don't use the correct transceivers or optical fiber, you can experience signal loss, dropped frames, missing frames, or other problems at the physical layer.

• These transceivers look the same but notice that one (the above) is designed for a 1310 nanometer connection while the other (bottom) is designed for an 850 nanometer connection

Bottlenecks

Bottlenecks:

• Whenever someone says the network is slow, what they're really saying is that anyone of the many devices that are plugged into the network may be experiencing some type of problem inside of them
    ■ There is never a single performance metric that needs to be examined, you need to look at every step along the path as it is a series of technologies working together.
    ■ This means you may have to look at the CPU speed, storage access speeds, network bandwidth to

really get an understanding of the performance of the traffic going across the network
    ■ You must monitor the performance for nearly all network devices in order to find the slowest one. It also helps if you have a baseline of what the “normal” network performance is.

Interface Configuration Problems

Interface Configuration Problems:

• If you have problems with the configurations of the interfaces used on your network, you may symptoms such as:
    ■ Poor throughput which is very consistent & easily reproducible
    ■ Or you may find some devices have no connectivity (link lights aren't lighting up to indicate a successful connection)
    ■ Or you may find that there is a link light lighting up but no activity light on the adapter
    ■ All of these may easily be resolved by simply checking the interface configuration of the ethernet adapters

Interface Configuration

Interface Configuration:

• On many networks, the ethernet cards are configured to autoconfigure when they connect to the network. They determine what's on the other end & make sure both configurations match on both sides.
    ■ Although this isn't fool proof, some network admins prefer to set up their network configurations manually so they know that both sides of the connection will match.
• The first thing to check for is a link light to ensure that the devices are indeed successfully connected
    ■ If there is no light then it may be a cabling problem or an interface configuration issue
• The speed of the ethernet connection needs to match on both sides:
    ■ A mismatch will result in no connectivity across the network
    ■ If one side there is 100 MB/s then on the other side there also needs to be 100 MB/s
• Another thing that needs to match is the duplex configuration of both sides of the connection:
    ■ If there is a mismatch, it's difficult to troubleshoot since there is indeed connectivity but the connection will suffer problems
    ■ If mismatched, speed will suffer & there will be an increase in late collision counter (this 2nd symptom can also give you an indication that there is a duplex mismatch)

VLAN Mismatch

VLAN Mismatch:

• When configuring interfaces on switch, you assign each interface w/a VLAN
    ■ if the wrong VLAN is entered, problems will occur. EX: The link light may be lighting up but surfing the internet or connecting to other devices may not be possible. Or there may be an IP address assigned via DHCP (auto assignment protocol) but the IP isn't on the correct subnet you should be on. And if you manually configure the IP, you still aren't able to connect to devices on the network
• The best way to check for a VLAN configuration is on the switch itself:
    ■ You would SSH or connect to the switch & see what the VLAN setting is for the interface that's connected to that device. VLAN 1 is usually the default for the switch but check documentation to see what VLAN that device should be a member of.

Wireless Network Troubleshooting

Reflection

Reflection:

• 1 challenge when designing wireless networks is dealing w/reflection:
    ■ Reflection is when a wireless signal bounces off objects. Some objects may bounce the signal better and the signal may bounce differently at 2.4GHZ when compared to 5GHZ
    ■ If there is too much reflection then the signal may be weaker than expected
    ■ A little bit of reflection can actually be useful if you're taking advantage of multipath interference with MIMO <--- **Research further**
• Excessive reflection can be avoided by fixing the position of antennas
    ■ Reflection may not be a problem for MIMO in 802.11n or multiuser MIMO in 802.11ac

Refraction

Refraction:

• Wireless signals can also suffer from refraction:
    ■ Refraction occurs when the signal passes through an object & exits that object at a different angle. This might affect data rates.

Absorption

Absorption:

• If a wireless signal isn't reflecting off an object, then it may be absorbed by the object:
    ■ This is when signal passes through an object & loses signal strength (this occurs especially through walls & windows)
• Different objects absorb differently as frequencies change:
    ■ 2.4 GHz has a different absorption rate than 5 GHz
• This is one of the reasons antennas are placed on the ceiling:
    ■ To avoid going through walls

Latency & Jitter

Latency & Jitter:

• Latency:
    ■ Delay from transmitting info & receiving a response.
• Jitter:
    ■ A deviation from a predictable data stream (very common with real-time applications such as VOIP)
• On wireless networks, there are many opportunities for wireless interference & signal issues since anything can be conflicting w/that wireless signal.
    ■ These interferences can result in slower data rates & loss of data which then results in retransmission of data.
• If the network is very busy, you may also run challenges with latency & jitter:
    ■ If your network is overcapacity & have many different devices communicating, there may be slow downs as more & more people join the wireless network.

Attenuation

Attenuation:

• Just like on copper or fiber, it occurs on wireless networks:
    ■ As you move farther & farther away from the access point, the signal weakens. This can be measured via a **wifi analyzer** or viewing the signal strengths on a device
• To avoid excessive attenuation, you may be able to boost the signal on the access point itself
    ■ Not all access points have this option though.
    ■ If it does, this allows for a greater range
    ■ If the device you're on has the ability to add on an antenna, you may be able to use one with a higher gain which allows for greater signal capturing
• The closer you are to the access point, the less attenuation you experience

Interference

Interference:

• On a wireless network means that something else is using the same frequencies that we're trying to communicate on the wireless network
    ■ Sometimes it's predictable interference such as a microwave oven, florescent lights, cordless telephones, high-power sources. These all can be easily solved via turning off the light or microwave or disabling the high-power source
    ■ Sometimes the interference is unpredictable
• One way to view interference statistics is via netstat:
    ■ netstat -e
    ■ Performance monitor can also be used via Windows to monitor those statistics over time

Incorrect Antenna Type

Incorrect Antenna Type:

• The type of wireless antenna you use depends on the reach & scope of your network
    ■ If you're trying to cover wireless networks on a single floor of a building, you'd be using a different antenna when compared to trying to connect 2 buildings together
• We can use **omnidirectional antenna**:
    ■ We hook it up to the ceiling, the signal is equally distributed in every direction
    ■ Not very useful between buildings
• **Directional Antenna**:
    ■ If you're attempting to connect 2 buildings, this would be the preference
    ■ All the wireless signal is directed in 1 single direction

Incorrect Antenna Placement

Incorrect Antenna Placement:

• You also want to be sure the antennas are placed in the right place
    ■ If access points are too close to each other, the frequencies may interfere with each other
    ■ If your antennas are too far away from users & there are other electrical devices causing interference, you may find slower bandwidth than what's expected

■ You may also want to check to confirm that the access points are using the frequencies and the channels that you're expecting to be used
■ It may also be a problem with 2.4 GHz channels as there are only so many non-overlapping channels available which means that there may be some interference

Overcapacity

Overcapacity:

• There is only so much capacity (only so many devices can be communicating over these very narrow frequency ranges we have for wireless networks)
■ If there are too many devices connected to the same wireless network you may have problems with **device saturation**.
■ If you have the option of using 5 GHz, use it since there will be a wider range of frequency & overcapacity isn't as big of a problem with 5 GHz
• You may also run into **bandwidth saturation**:
■ This is when too many people are attempting to use data at once, **EX**: too many people attempting to transfer files at once.

Frequency Mismatch

Frequency Mismatch:

• Since we have a number of different 802.11 standards, there are chances that some standards may use different frequencies when compared to another standard
■ One thing we have to be sure, the devices we are using have to match the frequencies that will be used on that access point
• You may run into problems where a client on the network is communicating over a slightly different frequency/channel to the access point
■ Check to see if someone manually configured a channel on their wireless device instead of having it set to the default (automatching what's on the access point)
• Mixing different standards on the wireless network may cause the network to not be as efficient as possible:
■ Older standards may slow down the newer network

Wrong SSID

Wrong SSID:

• Every access point has at least one SSID configured:
■ this designates the name of the wireless network we'd connect to

Signal to Noise Ratio

Signal to Noise Ratio:

• This is a good statistic to view how much interference is occurring on your wireless network
• The signal is the normal communication you would want from your wireless network
• The noise is the interference:
■ Might be from other devices or other wireless networks
• You want a very large ratio, much more signal when compared to noise:

    ■ The same amount of signal to noise (aka 1:1) is bad

Network Service Troubleshooting

Names not resolving

Names not resolving:

• If DNS isn't working, it'll be difficult to resolve an IP address from a FQDN or vice versa:
    ■ This means browsing the web wouldn't work
• Try pinging IP addresses:
    ■ This will confirm you at least have connectivity to the network

Troubleshooting DNS Issues

Troubleshooting DNS Issues:

• The first thing to check is the IP address of your local device:
    ■ If you're able to ping an IP address on another subnet mask then you know your local device has the correct IP address, subnet mask, & default gateway
    ■ But you may want to check the configuration on your DNS servers, make sure IP addresses are listed on your configuration & make sure there the correct IP addresses for your DNS servers
• Use **nslookup** or **dig**:
    ■ This queries the DNS server & will see if you're able to receive responses for the services you would like to access.
• If those DNS servers aren't responding, try using a different DNS server:
    ■ Google's DNS server: 8.8.8.8 & 8.8.4.4
    ■ Quad9's DNS server: 9.9.9.9

IP Configuration Issues

IP Configuration Issues:

• If the IP configuration on your device isn't correct, there may be a number of different symptoms that occur such as:
    ■ You can communicate to local IP addresses but you cannot communicate with different IP addresses on a different subnet mask
    ■ Or there is no IP communication at all, you cannot communicate with IP addresses on the local subnet or IP addresses on a different subnet mask
    ■ Or you can communicate to some local IP addresses but others aren't accessible/communicable from your machine

Troubleshoot IP Configuration

Troubleshoot IP Configuration:

• The first thing to do is check the documentation to confirm that you have the correct IP address for

your subnet mask
    ■ Also check your device's IP address, subnet mask, & default gateway & make sure it matches your documentation
• If you suspect your switch is configured on the wrong VLAN & you're on the wrong IP subnet, you should be able to capture packets & determine what subnet you're connected to.
• If you're not on your network or don't have access to the documentation, check the devices around you to confirm that these devices's IP address, subnet mask, & default gateway match yours
• Try using ping & traceroute:
    ■ The issue might be your infrastructure
    ■ Ping local IP, default gateway, & outside addresses & perform traceroute on outside addresses to see how far you're able to get outside your local subnet

Duplicate IP Addresses

Duplicate IP Addresses:

• Some network admins like to manually configure IP addresses on all their devices:
    ■ There is no DHCP server
    ■ They have to be very careful they aren't duplicating IP addresses between devices
• DHCP doesn't guarantee you aren't going to have duplicate IP addresses
    ■ There might be multiple DHCP servers & you've accidentally configured duplicate IP addresses both of those servers
    ■ Someone could've even turned on their own IP addresss & now their server is handing out IP addresses
• If 2 devices on the same network have the same IP address, you'll run into major problems:
    ■ Both devices will suffer intermittent connectivity. 1 device will have connectivity for a period of time & then the other device will take over that connectivity for a period of time. This cycle will repeat
• But on most modern OSes, a check on the IP address is performed by the OS before it connects to the network:
    ■ If the OS finds that the OS is already in use, it blocks your system from creating a duplicate IP address

Troubleshooting Duplicate IP addresses

Troubleshooting Duplicate IP addresses:

• You can start with the devices that are being manually configured:
    ■ Check the IP address, subnet mask, & default gateway & confirm it matches your documentation
• Before bringing a workstation online, ping its IP address & see if another (different) device responds:
    ■ If a another device does respond, you know that IP address shouldn't be manually configured on that device
• If you're manually configuring the IP address & you know it's the right address but some other device is already using it, you can use that 3rd party device to ping the IP address & find the MAC address of the device already using the IP address & then locate the MAC address in the switch:
    ■ The switch's MAC table should be able to tell you what interface the MAC address belongs to
• If you believe you're getting the duplicate IP Address from a DHCP server:
    ■ You may want to capture the packets associated w/the DHCP process to tell exactly what DHCP server is providing you with that duplicate IP address. This would be done by determining which DHCP server is responding to requests.

Duplicate MAC Address

Duplicate MAC Address:

• This doesn't occur very often
• MAC addresses are burned into the Network Interface Card (NIC) & it's very uncommon to see 2 NICs with the same MAC address
• If you do see a duplicate MAC address it could be unintentional like someone misconfigured a manual MAC address configuration
• Man-in-the-Middle attacks can often involve spoofed MAC addresses as well so you want to be sure there aren't any security concerns on your network
• It may also simply be a manufacturing error where 2 different NICs have the same burned in MAC addresss
• If there are duplicates of the same MAC address on your network those devices will experience intermittent connectivity:
    ■ The switch will be confused about where that MAC address is on the network
• If you're trying to confirm the MAC address of a device then you may want to ping the IP address of the device then look at the ARP cache (using the ARP commands) to see what MAC address is associated with that IP address

Expired IP Address

Expired IP Address:

• If you're using DHCP, you know that most devices are able to renew their IP address halfway through the lease time
    ■ But if you find that an IP address assigned by the DHCP server is expiring, this may indicate a problem with the DHCP server
    ■ If the DHCP server isn't available to renew that IP address then the client will release that IP address at the end of a DHCP lease
    ■ If you find an IP address starting with 169.254.*.* then you know that this is an automatic IP address assignment & the client wasn't able to retrieve a DHCP assigned address.
• Check the status of your DHCP server:
    ■ Confirm you have available addresses in the pool & the DHCP server is working normally.

Rogue DHCP Server

Rogue DHCP Server:

• If someone starts up their own DHCP server & begins handing out IP addresses to anyone who might need them, this is a rogue DHCP server
    ■ Since there isn't much security attached to DHCP, this may be easy for someone to put on your network
• Rogue DHCP servers can cause many problems:
    ■ People can be assigned invalid or duplicate IP addresses, this can prevent many clients from communicating to other devices (intermittent connectivity or even no connectivity in some cases)
• One way to disable this rogue DHCP communication:
    ■ Enable security on your switch. More specifically enable DHCP snooping on your switch which attempts to identify rogue DHCP devices & allows you to authorize DHCP devices in Microsoft's Active Directory & only those devices would be allowed to hand out DHCP addresses.
    ■ Once the rogue DHCP server is disabled, you would need to find the devices that got an IP address from the rogue DHCP server & have them release that IP address & renew a new IP address lease with the authorized DHCP server.

Untrusted SSL Certificate

Untrusted SSL/TLS Certificate:

• If you're communicating to a web server over an encrypted channel & get a popup stating the certificate isn't trusted by your computer's OS, then you may have a problem communicating securely to that web server
    ■ This means your browser received the certificate from the web server but the certificate authority that signed the certificate isn't in the browser's configuration so the browser doesn't trust the certificate
• This can be the result of the certificate itself not being signed by a certificate authority
• This can also be the result of the certificate being signed by a certificate authority that isn't listed as a trusted certificate authorities in your browser config
• Check the certificate details yourself which will tell you the certificate authority that issued the certificate:
    ■ Compare the certificate authority to the list of trusted certificate authorities in your browser
• If you're communicating to an internal web server on your company's network then you might need to add your company's certificate authority to your browser
    ■ Normally this certificate is added by your workstation administration team but it can manually be added

Incorrect Time

Incorrect Time:

• Configuring the date/time on all devices on your network becomes very important when trying to implement security
    ■ **EX**: The default tolerance for Kerberos is a 5 minute Window so it's important to have very tight tolerances on the time & date on all your devices. The reason being is that Kerberos assigns you a ticket & that ticket has a time stamp with it & if the time stamp is too old, kerberos considers that ticket to be invalid which results in your client not being able to login. This is why when a user experiences a problem with attempting to login with Kerberos is to check the time stamp on the device that's attempting to login to the network
• The easiest thing to do is to configure NTP on all devices which automates the clock setting
    ■ Now the devices would be in sync in regards to time with one another

Exhausted DHCP Scope

Exhausted DHCP Scope:

• When you manage a DHCP server you create a pool of a certain number IP addresses that are available but what if you run out of addresses?
    ■ In these situations you'll find that those devices aren't able to get an IP address from the DHCP server & will assign themselves an **APIPA address** which allows for local subnet communicaiton only.
    ■ If you find that your DHCP server is assigning APIPA addresses, you want to check your DHCP server & make sure there are IP addresses available for use & add more IP addresses if possible
• Exhausting the amount of IPs in a DHCP pool may sneak up on you:
    ■ Which is why it's good to implement **IP Address Management (IPAM)** which allows you to monitor & be alerted if the DHCP pool gets low
• If there are lots of transient users (users who move into the network & remain in the network for a brief period of time) then you might want to lower your lease time
    ■ This is going to allow for more IP addresses to be released faster & will provide a larger pool for other users that might need them

Blocked TCP/UDP Ports

Blocked TCP/UDP Ports:

• Certain application flows may be blocked due to filters installed on a firewall:
    ■ This would result in an application not working & may cause slowdowns with other applications
    ■ This could also be configured as an ACL on a router & it would still be restricting access for an application to travel through that network device
• These security checkpoints are usually configured with very conservative rules (think least privilege) & it's not uncommon for these rules to prevent new applications from working on the network
• Perform a packet capture & confirm that there are indeed application requests & no response being received:
    ■ This will confirm communication is the problem
• From there you may want to run a TCP- or UDP-based traceroute tool (this traceroute tool should allow you to customize the TCP or UDP port number that's used)
    ■ This would allow you to see just how far the traffic is able to go & then you can provide that traceroute info to a network admin who can then decide where the filtering is occurring

Incorrect Host-Based Firewall Setting

Incorrect Host-Based Firewall Setting:

• A similar problem to blocked TCP/UDP ports may occur if the application is being filtered out by your host based firewall
    ■ A firewall admin may also be able to filter the traffic out based on far more than the protocol & port number, specifically filtering by the application name
• In environments where the host-based firewall is managed centrally, you may not have access to view firewall info
    ■ So you may need to document exactly what application(s) you wish to use & provide this info to the firewall admin
• In this case, you want to perform a packet capture from an external device (not the device you want the application to run on) to see exactly the traffic that's leaving that computer & the traffic that's returning
    ■ The returning traffic may never make it to the network which indicates a network-based firewall is filtering it
    ■ Or the returning traffic may be dropped by the OS which indicates a host-bsaed firewall

Incorrect ACL Setting

Incorrect ACL Setting:

• With ACLs, there are many options to filter by:
    ■ IP address, port numbers, & other parameters
    ■ Can allow or deny traffic by filtering packets based on a combination of this criteria
• If you're trying to determine if an ACL is blocking your traffic:
    ■ You can perform a packet capture & be able to see what traffic you're trying to send & what traffic is being received
    ■ You may also want to use a traceroute utility that allows you to customize the port number that's used which would allow you to send traffic into the network & you'd be able to tell at exactly what hop the traffic is stopping

Unresponsive Service

Unresponsive Service:

• If you're attempting to communicate to a server & you're not getting any response & you know the problem isn't related to a filter or an ACL:
    ■ Then there may be a service that's simply not responding to your request & you may want to be sure you're accessing that service over the correct TCP or UDP port number.
    ■ Confirm the device itself is up & running, run a ping or traceroute on the device & confirm you're able to communicate to that server successfully
    ■ Try telnetting or sshing to the port number & see if there's a response. If there's no response you may need to restart the application or restart the server where that application exists

Hardware Failure

Hardware Failure:

• If the server that's hosting the application is experiencing problems, the issue may be similar to the service itself not responding:
    ■ First confirm connectivity, if there really is a hardware failure than you're likely not going to receive a response to the ping
    ■ You can also confirm if there is a hardware failure via traceroute, you can see what hops are being performed to get to the server & see if it responds. This is also used to see if you're being filtered which would confirm it isn't a hardware filter (if you are being filtered)
    ■ Check the physical server & confirm why it isn't responding

Python Networking

Socket Commands

Socket Commands:

• socket.socket() = creates a socket connection
• s.bind(host,port) = bings a socket to a host & port
• s.send() = sends data over a socket connection
• s.listen() = listens for any data
• s.recv() = recieves data
• s.close() = closes socket connection

Basic Port Scanner (Scans 1 port only)

```
#!/usr/bin/python3

#scans for open ports

import socket

s = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
#Assigns variable to make calling it later down the line easier.Inside parenthesis we call "socket.AF_INET" which specifies we will be using IPv4 & "SOCK_STREAM" specifies the type of transport layer connection. If yo uwanted TCP, you would call "socket.SOCK_DGRAM" for UDP datagrams
#s.settimeout(5)
# ^ sets the default connect to stop attempting to connect & assume it's closed after 10 seconds, this may not be the best idea for all ports since some may take some time but it's for the sake of being quick
```

```
host = "#Enter Target IP Here"
port = "#Enter specific port here"



def portscanner(port):
    if s.connect_ex(host, port):
        print("The port is closed")
    else:
        print("The port is open")



portscanner(port)
```

Basic Port Scanner (Scans multiple ports in 1 run)

```
#!/usr/bin/python3
#scans for open ports
import socket

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
#Assigns variable to make calling it later down the line easier.Inside parenthesis we call "socket.AF_INET" which specifies we will be using IPv4 & "SOCK_STREAM" specifies the type of transport layer connection. If yo uwanted TCP, you would call "socket.SOCK_DGRAM" for UDP datagrams

ports = [20, 21, 22, 443, 80]
host = "137.74.187.100"
for i in ports:
  if s.connect_ex((host, i)):
    print("Port", i, "is closed\n")
  else:
    print("Port", i, "is open\n")
```

Direct & Reverse Connection

Direct Connection:

• Requires IP address of your own & remote computer you wish to connect to as well as a port to bind the socket to & connect to

Problems w/Direct Connection:

• If the IP address is dynamic so it changes so it's difficult to maintain the connection
• Even if we could maintain persistence with the connection, it computer will likely have a firewall which makes it difficult to access the computer remotely

Reverse Connection:

• Instead of an attacker attempting to intiate a connection from an attacker's computer, it's the victim initating the connection from their computer
    ■ This mitigates most of the problems that are faced with direct connections
    ■ But the problem of the hacker's IP address being dynamic still occurs since the IP address that the victim's computer calls back to/connects to won't be valid for long. Attackers solve this by hosting a server with a static IP address.