Welcome to the Fourth Chapter.

Domain 4: What we will be covering.

- **This is a GIANT domain.**

- Network Basics and Definitions.
- The OSI and TCP/IP model.
- IP Addresses, Port Numbers, and MAC Addresses.
- Wi-Fi and other wireless networks.
- Virtualization, Cloud, and Distributed Computing.
- Fault tolerance and resiliency.
- Data centers.
- Attacks and Attackers.

Network Basics and Definitions:

- **What is networking?**
  - A computer network is a set of computers sharing resources or data.

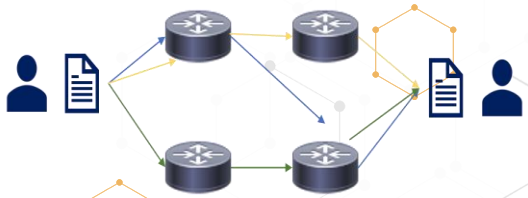
We use defense-in-depth on our internal network and when our data traverses the internet.

- We do this by ensuring all our network devices, protocols, and traffic are as secure as possible.
- **Simplex** is a one-way communication (One system transmits, the other listens).
- **Half-duplex** communication sends or receives at one time only (Only one system can transmit at a time).
- **Full-duplex** communication sends and receives simultaneously. (Both systems can transmit/receive simultaneously).
- **Baseband** networks have one channel and can only send one signal at a time.
  - Ethernet is baseband: “1000base-T” STP cable is a 1000-megabit, baseband, Shielded Twisted Pair cable.
- **Broadband** networks have multiple channels and can send and receive multiple signals at a time.
- The **Internet** is a global collection of peered WAN networks, it really is a patchwork of ISPs.
- An **Intranet** is an organization's privately owned network, most larger organizations have them.
- An **Extranet** is a connection between private Intranets, often connecting business partners' Intranets.

- **Circuit Switching -** Expensive, but always available, used less often.
  - A dedicated communications channel through the network.
  - The circuit guarantees the full bandwidth.
  - The circuit functions as if the nodes were physically connected by a cable.
- **Packet Switching -** Cheap, but no capacity guarantee, very widely used today.
  - Data is sent in packets but take multiple different paths to the destination.
  - The packets are reassembled at the destination.
  - **QoS (Quality of Service)** gives specific traffic priority over other traffic.
    - Most commonly VOIP (Voice over IP) or other UDP traffic needing close to real time communication.
    - Other non-real time traffic is down prioritized, the 0.25 second delay won't be noticed.

Circuit Switching Network

Packet Switching Network

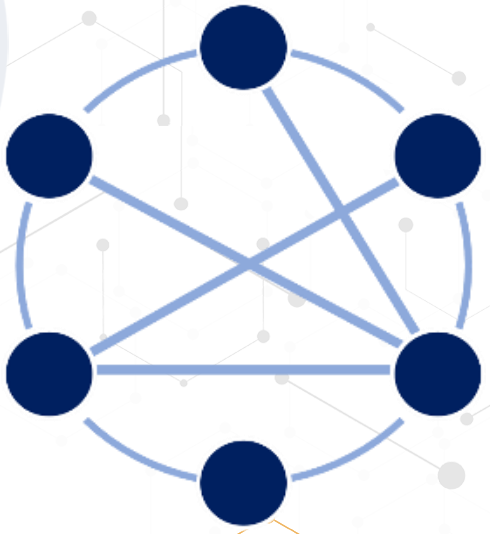


- **PAN (Personal Area Network)** - A personal area network is a computer network used for communication among computers and other information technological devices close to one person (PCs, printers, scanners, consoles …).
  - Can include wired (USB and FireWire) and wireless devices (Bluetooth and infrared).
- **LAN (Local Area Network)** - A network that connects computers and devices in a limited geographical area such as a home, school, office building or campus.
  - Each computer or device on the network is a node, wired LANs are most likely based on Ethernet technology.
- **MAN (Metropolitan Area Network)** – A large computer network that usually spans a city or a large campus.
- **WAN (Wide Area Network)** - A computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances. Combines many types of media such as telephone lines, cables, and air waves.
- **GAN (Global Area Network)** - A global area network, is a network used for supporting mobile users across a number of wireless LANs, satellite coverage areas, … the transition from one to the next can be seamless.
- **VPN (Virtual Private Network)** - A VPN network sends private data over an insecure network, most often the Internet.
  - Your data is sent across a public network, but looks and feels private.

The OSI Model:

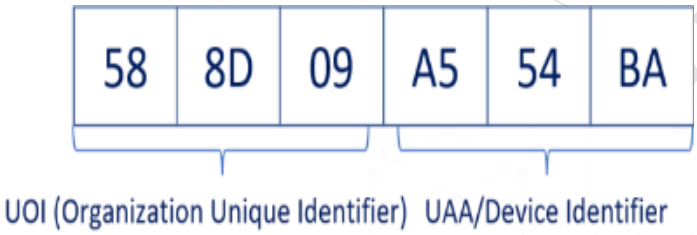
- **The OSI Model (Open Systems Interconnect):**
  - A layered network model that standardizes the communication functions of a telecommunication or computing system regardless of their underlying internal structure and technology.
  - The model partitions a communication system into abstraction layers, the model has 7 layers.
    1. Physical
    2. Data Link
    3. Network
    4. Transport
    5. Session
    6. Presentation
    7. Application.
       - 7-1 **A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing.
       - 1-7 **P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way.
  - Know the PDUs (Data, Segments, Packets, Frames, Bits).

- **Layer 1 - Physical Layer:**
  - Wires, Fiber, Radio waves, hub, part of NIC, connectors (wireless).
  - **Cable types:**
    - Copper TP (Twisted Pair) Least secure, eavesdropping, interference, easy tap into, but also cheap.
    - Fiber is more secure, not susceptible to eavesdropping, harder to use, can break, higher cost.
  - **Topologies:**
    - Bus, Star, Ring, Mesh partial/full.
  - **Threats:**
    - Data emanation, theft, eavesdropping, sniffing, interference.



Partial Mesh Topology

- **Layer 2 - Data Link Layer:**
  - Transports data between 2 nodes connected to same network.
  - LLC – Logical Link Control – error detection.
  - MAC address (BIA) – a unique identifier on the network card.

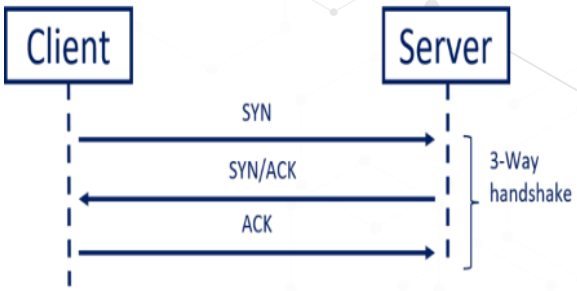


    - Can be spoofed very easily, both for good and not so good reasons.
    - 48-bit hexadecimal first 24 manufacturer identifier, last 24 unique.
    - 64-bit hexadecimal first 24 manufacturer identifier, last 40 unique.
    - **Threats** - MAC Spoofing, MAC Flooding.
  - **ARP (Address Resolution Protocol)** Layer 2/3.
  - **CSMA/CD** – Ethernet – minimized with switches vs. hubs.
  - **CSMA/CA** – Wireless.
  - **Token passing** – Similar to the talking stick, not really used anymore.

- **Layer 3 - Network Layer:**
  - Expands to many different nodes (IP) – The Internet is IP based.
  - Isolates traffic into broadcast domains.
  - **Protocols:**
    - IP, ICMP, IPSEC, IGMP, IGRP, IKE, ISAKMP, IPX.
  - **Threats:**
    - Ping of Death, Ping Floods, Smurf – spoof source and directed broadcast, IP modifications, DHCP attacks, …

- **Layer 4: Transport Layer:**
  - **SSL/TLS Layer 4 to 7.**
  - **UDP (User Datagram Protocol):**
    - Connectionless protocol, unreliable, VOIP, Live video, gaming, “real time’’.
    - Timing is more important than delivery confirmation.
    - Sends message, doesn’t care if it arrives or in which order.

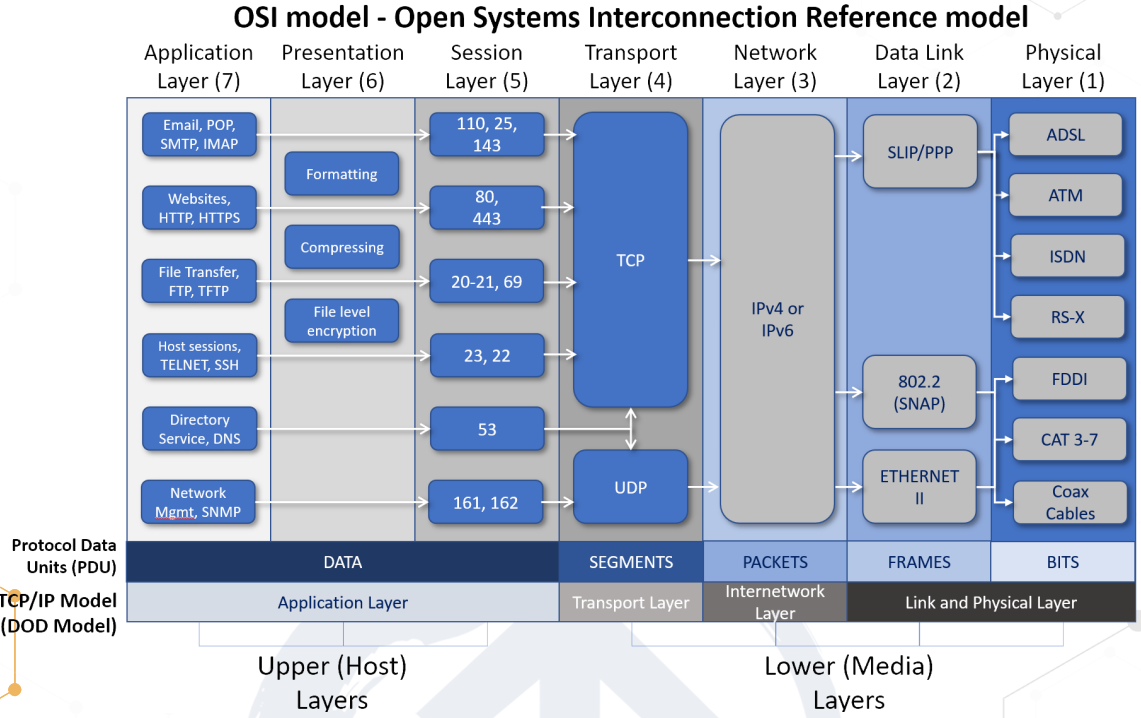
- **Attack: Fraggle attack** – works the same way as smurf but may be more successful since it uses UDP and not ICMP.



- **TCP (Transmission Control Protocol):**
  - Reliable, Connection orientated, Guaranteed delivery, 3-way handshake, slower/more overhead, data reassembled.
  - **Attacks: SYN floods** – half open TCP sessions, client sends 1,000s of SYN requests, but never the ACK.

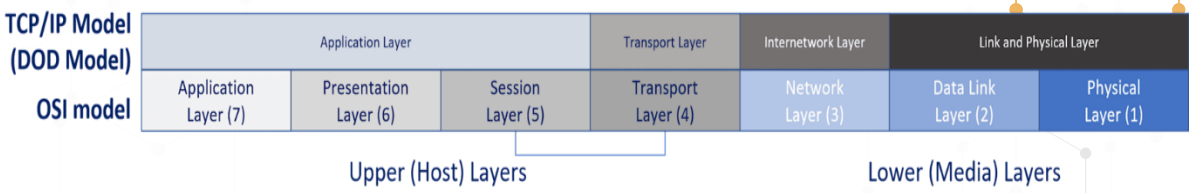
- **Layer 5 – Session Layer:**
  - Establishes connection between 2 applications: Setup > Maintenance > Tear Down.
- **Layer 6 - Presentation Layer:**
  - Only layer with no protocols.
  - Formatting, compressing, encryption (file level).
- **Layer 7 - Application Layer:**
  - Presents data to user (applications/websites).
  - HTTP, HTTPS, FTP, SNMP, IMAP, POP, and many more.
  - Non-Repudiation, certificates, application proxies, deep packet inspection, content inspection, AD integration.

- The higher you go up the layers, the slower it is. Speed is traded for intelligence.
- **Threats to Level 5-7:** Virus, worms, trojans, buffer overflow, application, or OS vulnerabilities.



The TCP/IP Model:

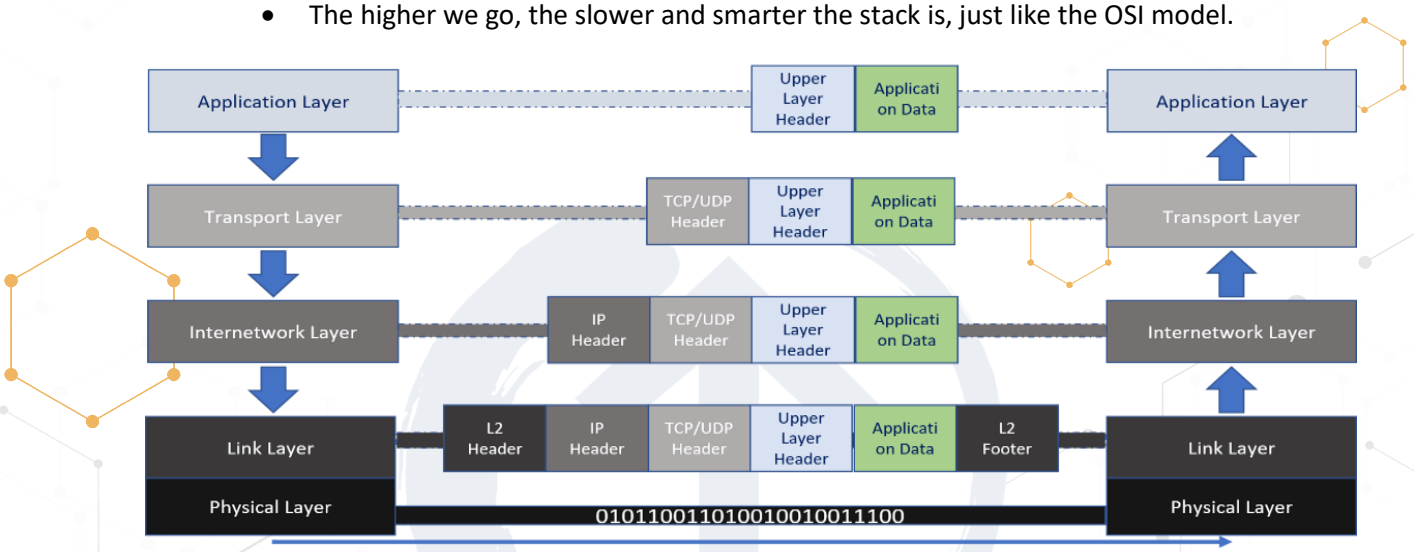
- **The TCP/IP Model** (Internet Protocol Suite):
  - A conceptual model that provides end-to-end data communication.
  - Specifying how data should be packetized, addressed, transmitted, routed, and received.
  - It has four layers which are used to sort all related protocols according to the scope of networking involved.
  - From lowest to highest:
    - **The link layer** containing communication methods for data that remains within a single network segment.
    - **The internet layer** connecting independent networks, thus providing internetworking.
    - **The transport layer** handling host-to-host communication.
    - **The application layer** provides process-to-process data exchange for applications.



- **The link and physical layer** have the networking scope of the local network connection to which a host is attached.
  - Used to move packets between the Internet layer interfaces of two different hosts on the same network.
  - The process of transmitting and receiving packets on a given link can be controlled both in the software device driver for the network card, as well as on firmware or specialized chipsets.
  - These perform functions such as adding a packet header to prepare it for transmission, then transmit the frame over a physical medium.
  - The TCP/IP model includes specifications of translating the network addressing methods used in the Internet Protocol to link layer addresses, such as Media Access Control (MAC) addresses.
  - The link and physical layer = OSI layer 1-2.
- **Internet/Internetwork layer** is responsible for sending packets across potentially multiple networks.
  - Requires sending data from the source network to the destination network (routing).
  - Internet/Internetwork layer = OSI layer 3.
  - The Internet Protocol performs two basic functions:
    - **Host addressing and identification:** This is done with a hierarchical IP address.
    - **Packet routing:** Sending the packets of data (datagrams) from the source to the destination by forwarding them to the next network router closer to the final destination.
- **The transport layer** establishes basic data channels that applications use for task-specific data exchange.
  - Its responsibility includes end-to-end message transfer independent of the underlying network, along with error control, segmentation, flow control, congestion control, and application addressing (port numbers).
  - Data is sent connection-oriented (TCP) or connectionless (UDP).
  - The transport layer = OSI layer 4.
- **The application layer** includes the protocols used by applications for providing user services or exchanging application data over the network (HTTP, FTP, SMTP, DHCP, IMAP).
- Data coded according to application layer protocols are encapsulated into transport layer protocol units, which then use lower layer protocols for data transfer.
- The transport layer and the lower-level layers are unconcerned with the specifics of application layer protocols.

- Routers and switches do not typically examine the encapsulated traffic, rather they just provide a conduit for it. However, some firewall and bandwidth throttling applications must interpret application data.
- The TCP/IP reference model distinguishes between **user protocols** and **support protocols.**
- The application layer = OSI layer 5, 6, and 7.

- Each layer of the model adds or removes encapsulation (encapsulation / de-capsulation).
- The higher we go, the slower and smarter the stack is, just like the OSI model.



IP Addresses, Port Numbers, and MAC Addresses:

- A unique identifier on the network card.
- Can be spoofed pretty easily, both for good and less good reasons.
- EUI/MAC-48 are 48bits (original design).
  - The first 24 are the manufacturer identifier.
  - The last 24 are unique and identify the host.
- EUI-64 Mac Addresses use 24bit for manufacturer, but 40 for unique ID.
  - The first 24 are the manufacturer identifier.
  - The last 40 are unique and identify the host.

- Both are widely used today and used by both IPv4 and IPv6.
  - For 48bit MAC's IPv6 modified it into 64bit MAC's by adding FF:FE to the device identifier.

- **IP Addresses:**
  - First deployed for production in the ARPANet in 1983, ARPANet later became the internet.
  - IP was developed in the 1970's for secure closed networks (DARPA - Defense Advanced Research Projects Agency). Security was not built in but was bolted on later.
  - IPv4 is a connectionless protocol for use on packet-switched networks.
  - It operates on a best effort delivery model, it does not guarantee delivery, it also does not assure proper sequencing or avoidance of duplicate delivery. We have added protocols on top of IP to ensure those.
  - IPv4 is the IT route's most Internet traffic today, but we are slowly moving towards IPv6.
    - The move towards IPv6 is mainly dictated by IPv4 Addresses being depleted years ago.
  - IPv4 has around 4.2 billion IP addresses and of those ~4 billion are usable internet addresses.
    - There are currently over 35 billion mobile devices on the internet, 75 billion is predicted by 2025.
    - All major cellphone carriers in the US use IPv6 for all cell phones.
    - **IPv4** has 4,294,967,296 addresses where **IPv6** has 340,282,366,920,938,463,463,374,607,431,768,211,456.

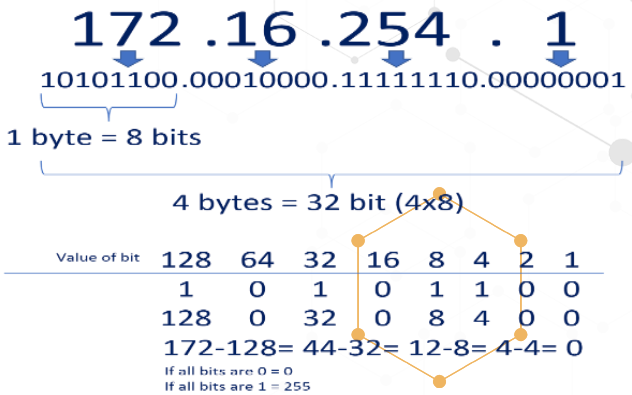
- **IP Addresses and Ports:**
  - When we send traffic, we use both the Source IP and Port as well as Destination IP and Port. This ensures we know where we are going, and when the traffic returns it knows where to return to.
  - The **IP addresses** can be seen as the number of an apartment building.
    - The **Port number** is your apartment number.
    - If you have 50 browser tabs open, each tab has its own port number(s).
  - **Well-known Ports:**
    - 0-1023 - Mostly used for protocols.

- **Registered Ports:**
  - 1024 to 49151 - Mostly used for vendor specific applications.
- **Dynamic, Private or Ephemeral Ports:**
  - 49152–65535 - Can be used by anyone for anything.

- **Common Ports:**

20	TCP	FTP data transfer.
21	TCP	FTP control.
22	TCP/UDP	Secure Shell (SSH).
23	TCP	Telnet unencrypted text communications.
25	TCP	Simple Mail Transfer Protocol (SMTP) can also use port 2525.
80	TCP/UDP	Hypertext Transfer Protocol (HTTP) can also use port 8008 and 8080.
110	TCP	Post Office Protocol, version 3 (POP3).
137	UDP	NetBIOS Name Service, used for name registration and resolution.
138	TCP/UDP	NetBIOS Datagram Service.
143	TCP	Internet Message Access Protocol (IMAP).
443	TCP	Hypertext Transfer Protocol over TLS/SSL (HTTPS).
3389	TCP/UDP	Microsoft Terminal Server (RDP).

- **IPv4 (Internet Protocol version 4)** addresses:
  - IPv4 addresses are made up of 4 octets (dotted-decimal notation) and broken further down in a 32bit integer binary.
  - We use IP addresses to make it readable to normal people, it is easier to read 4 sets of numbers than a 32 bits string of 0s and 1s.
  - Similarly, websites are really just IP addresses translated with DNS, which is then translated into binary.
  - It is easier to remember **google.com**, than it is to remember **66.102.12.231** or **2607:f8b0:4007:80b::200e**.

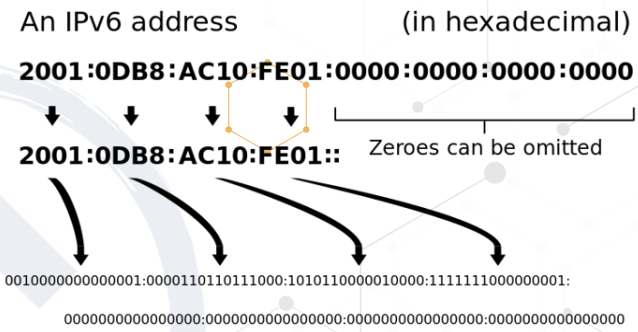


  - **Public IP Addresses** (Internet routable addresses):
    - Used to communicate over the internet between hosts.
  - **Private Addresses** (RFC 1918 – Not routable on the internet):

Other notable IP spaces:

- 10.0.0.0 10.255.255.255 16777216 127.0.0.0/8 Loopback IPs
- 172.16.0.0 172.31.255.255 1048576 169.254.0.0/16 Link-Local
- 192.168.0.0 192.168.255.255 65536 255.255.255.255 Broadcast

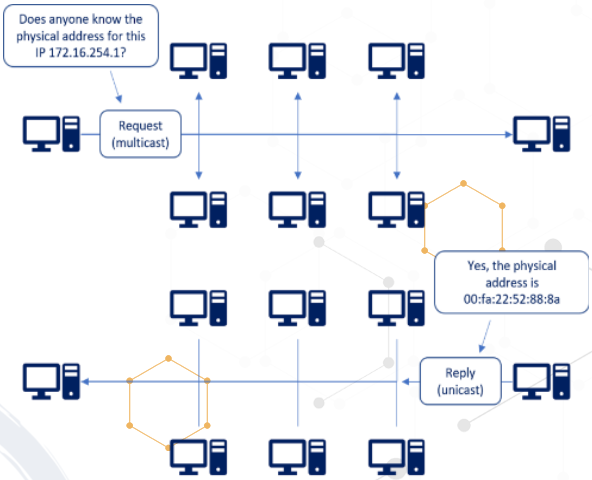
- **IPv6:**
  - IPv6 is 128bit in hexadecimal numbers (uses 0-9 and a-f).
  - 8 groups of 4 hexadecimals, making addresses look like this:
    - fd01:fe91:aa32:342d:74bb:234c:ce19:123b
  - The IPv6 address space is huge compared to IPv4.
    340,282,366,920,938,463,463,374,607,431,768,211,456 addresses.
    - 34 with 37 0s total or 79 with 27 0s as many addresses as IPv4.
    - Every square foot on the planet can have 65000 IP addresses.



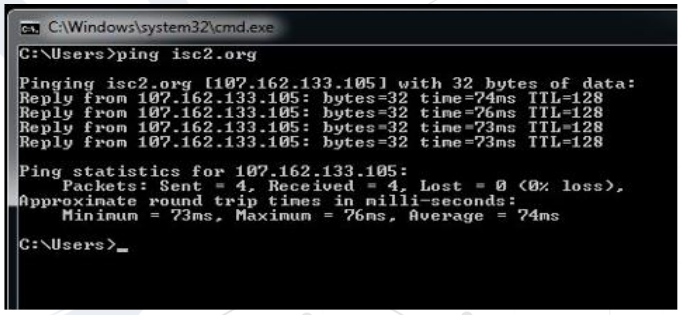
  - IPSec is built in, not bolted on like with IPv4.
  - Mostly switched behind the scenes today, many organizations do not have Dual Stack equipment in place.
  - Used by major US ISPs for cell phones (and to some extend the connection to your modem).
  - To make the address more manageable 1 set of 0s can be shortened with :: above you see the last 16 0s being shortened to 2001:0DB8:AC10:FE01::

IP Support Protocols:

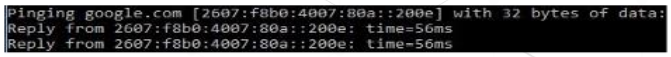
- **ARP (Address Resolution Protocol):**
  - Translates IP Addresses into MAC Addresses.
    - OSI Data/Network Layer or Network/Internet Layer.
  - ARP is a simple and trusting protocol, anyone can respond to an ARP request.
  - **ARP (cache) Poisoning:** An attacker sends fake responses to ARP requests, often done repeatedly for critical ARP entries (Default Gateway).
    - A countermeasure can be hardcoding ARP entries.
  - **RARP** (Reverse ARP) is used by diskless workstations to get IPs.



- **ICMP (Internet Control Message Protocol):**
  - Used to help IP, for Ping (Echo request/reply) and TTL Exceeds in Traceroute.
  - Often used for troubleshooting.
  - An ICMP Echo Request is sent to the IP, which then sends an ICMP reply back (or not).
  - Originally used (and still) to see if a host is up or down.
  - Today if we get an Echo reply we know the host is up, but no reply does not mean it is down.
  - Firewalls and routers can block ICMP replies.

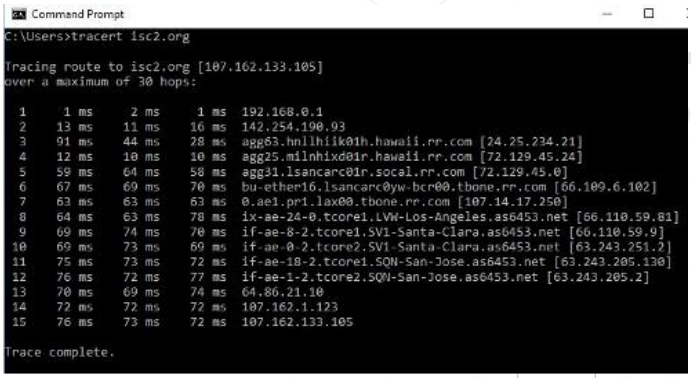


I ping isc2.org (can be name or IP if you know it).
The name is translated into the IP.
I get 4 replies from the IP, 32bytes (IPv4 ping size)
It took 73-76ms (milliseconds 1/1000th of a second)



IPv6 pings are slightly different, since they use the IPv6 headers, but the payload size is the same.

- **Traceroute:**
  - Uses ICMP to trace a network route.
  - Traceroute uses the TTL value in somewhat reverse.
  - We send a message with TTL 1.
    - The first router decrements the TTL to 0 and sends an ICMP Time Exceed message back, First Hop is now identified.

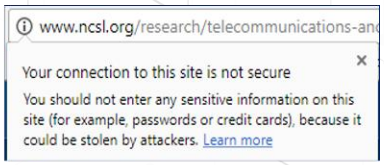


Traceroute to isc2.org (tracert on windows command line):
My local network > ISP > A few Hawaii hops > a few LA hops > 2x Santa Clara > 2x San Jose > Most likely ISC2 Firewall > and finally the actual webserver.

  - We send message 2 with TTL 2, 2nd router does the same, it is identified.
  - We do that over and over till the destination is reached (maximum 30 hops).

- **HTTP** and **HTTPS** - Transport HTML data.
  - **HTTP (Hypertext Transfer Protocol):**
    - Uses TCP port 80 (8008 and 8080), unencrypted website data sent across the internet.
- **HTTPS (HTTP Secure):**
  - Uses TCP Port 443 (8443), encrypted data sent over the internet.
- **HTML (Hypertext Markup Language):**
  - The actual language webpages are written in.
  - Not to be confused with HTTP/HTTPS.

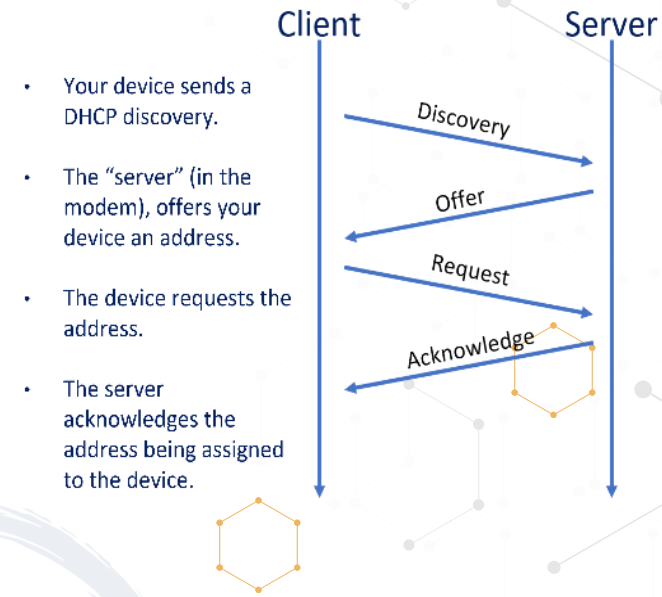
HTTPS: Connection (notice the Secure)



HTTP: Connection.

HTML: The basic building block of webpages.

- **DHCP (Dynamic Host Configuration Protocol):**
  - The common protocol we use to assign IPs. Controlled by a DHCP Server for your environment.
  - You most likely already use it on your home network, this is how when you connect a cable or connect wireless, you are online right away.
- Both BOOTP and DHCP use UDP Port 67 for the BOOTP/DHCP Server and UDP Port 68 for the Client.



Cables:

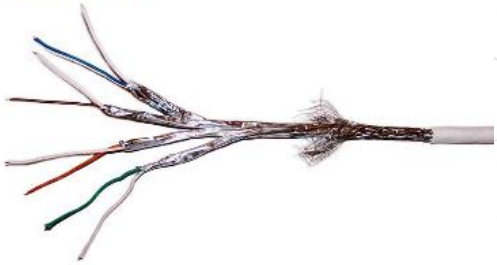
- **Networking Cables:**
  - When it comes to networking cables, most people think RJ45 Copper Ethernet cables, many more types are used though.
  - Networking cables all come with pros and cons, some are cheap, some more secure, some faster, ...
  - They can also pose different security vulnerabilities depending on the cable type and the environment.
  - **EMI (Electromagnetic Interference):**
    - Magnetism that can disrupt data availability and integrity.
  - **Crosstalk** is the signal crossing from one cable to another, this can be a confidentiality issue.
  - **Attenuation** is the signal getting weaker the farther it travels.
    - Copper lines have attenuation, with DSL the farther you are from the DSLAM (Digital Subscriber Line Access Multiplexer) the lower speed you get.


Putting a data center in a basement is a bad idea, in this case drowned DSLAMs

- **Twisted Pair Cables:**
  - **UTP (Unshielded Twisted Pair):**
  - Pairs of twisted pairs of cable.
    - Twisting them makes them less susceptible of EMI.
    - 1 cable sends and 1 receives data.
    - The tighter the cables are twisted, the less susceptible to EMI. For example, CAT3 pairs (less tight) are more susceptible to EMI than CAT6 (more tight).
  - **STP (Shielded Twisted Pair):**
    - Has extra metal mesh shielding around each pair of cables, making them less susceptible to EMI, but also making the cables thicker, stiffer, and more expensive.

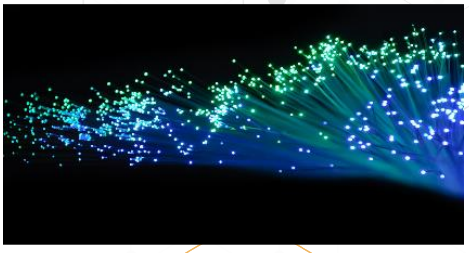
UTP Cable:

STP Cable:



- **Fiber Optic Cables** Use light to carry data (vs. electricity for copper cables)**:**
  - **Pros:** Speed 1 Petabit per second, 35miles/50 km over a single fiber.
    - Distance, it has no attenuation like copper, a single uninterrupted cable can be 150 miles+ (240km+) long.
    - Not susceptible to EMI.
    - More secure than copper since it can't be sniffed as easily as copper.
  - **Cons:** Price, more difficult to use, you can break the glass in the cable if you are not careful.
  - **Single-Mode fiber** - A Single strand of fiber carries a single mode of light (down the center), used for long distance cables (Often used in IP-Backbones).
  - **Multi-Mode fiber** - Uses multiple modes (light colors) to carry multiple data streams simultaneously, this is done with WDM (Wavelength Division Multiplexing).

Single-Mode fiber.



Light through fiber strands.

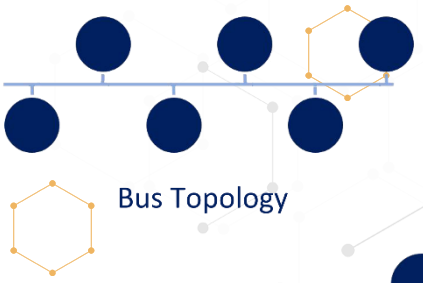
- All cable measurements are in metric system (m/km).
- Only 3 countries in the world do not use metric system (Burma (Myanmar), Liberia, and the United States).
    - **1Kbps** - Kilobits per second
        - 1,000 bps (10^3)
    - **1Mbps** - Megabit per second
        - 1,000,000 bps (10^6)
    - **1Gbps** - Gigabit per second
        - 1,000,000,000 bps (10^9)
    - **1Tbps** - Terabit per second
        - 1,000,000,000,000 bps (10^{12})
    - **1Pbps** - Petabit per second
        - 1,000,000,000,000,000 bps (10^{15})

UTP Categories – Copper Ethernet Cables				
CAT1	Up to 1Mbps		Twisted Pair	Old phone cable
CAT2	Up to 1Mbps		Twisted Pair	Token Ring network
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Ring & 10BASE T
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring network
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, Fast Ethernet, Token Ring
CAT5e	Up to 1Gbps	100m	Twisted Pair	Ethernet, Fast Ethernet, Gigabit Ethernet
CAT6/6a	Up to 10Gbps	100m	Twisted Pair	Gigabit Ethernet, 10G Ethernet (55m)
CAT7	Up to 10Gbps	100m	Twisted Pair	Gigabit Ethernet, 10G Ethernet (100m)
Multi-mode Fiber Ethernet Cables				
FDDI	160 / 500 MHz			1Gbps 220m, 10Gbps 26m
OM1	200 / 500 MHz			1Gbps 275m, 10Gbps 33m
OM2	500 / 500 MHz			1Gbps 550m, 10Gbps 82m
OM3	1500 / 2000 MHz			1Gbps 550m, 10Gbps 300m, 40/100Gbps 100m
OM4	3500 / 4700 MHz			1Gbps 550m, 10Gbps 400m, 40/100Gbps 150m
All fiber				100BASE-FX 2000m, 1000BASE-SE-LX 550m
Single-mode Fiber Cables				
				1 Pbps 50 km, 69.1Tbps 240 km

LAN Topologies:

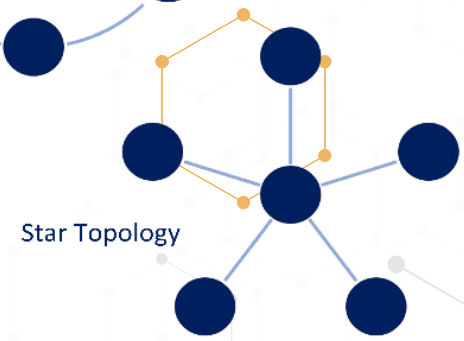
- Network topology describes the layout and topologies of interconnections between devices and network segments.
- **Ethernet** and **Wi-Fi** are the two most common transmission technologies in use for local area networks.
- At the data link layer and physical layer, a wide variety of LAN topologies have been used, including ring, bus, mesh, and star.
- At the higher layers, NetBEUI, IPX/SPX, and AppleTalk used to be common, but TCP/IP is now the de facto standard.

- **Bus:**
  - All nodes are connected in a line, each node inspects traffic and passes it along.
  - Not very stable, a single break in the cable will break the signal to all nodes past that point, including communication between nodes way past the break.
  - Faulty NICs (Network Interface Card) can also break the chain.

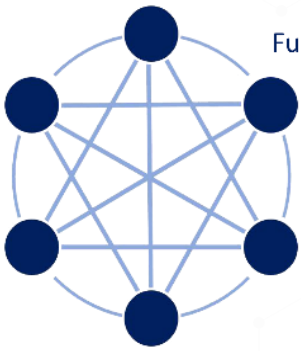


- **Tree** (Hierarchical):
  - The base of the Tree topology controls the traffic, this was often the mainframe.

- **Ring**:
  - All nodes are connected in a ring.
- **Star**:
  - All nodes are connected to a central device.
  - This is what we normally use for Ethernet, our nodes are connected to a switch.
  - Provides better fault tolerance, a break in a cable or a faulty NIC will only effect that one node.
  - If we use a switch, no token passing, or collision detection is needed since each node is on its own segment.
  - If we use hubs, collisions will still occur; but I hope none are around anymore, not just how slow they are, but more how unsecure they are now.

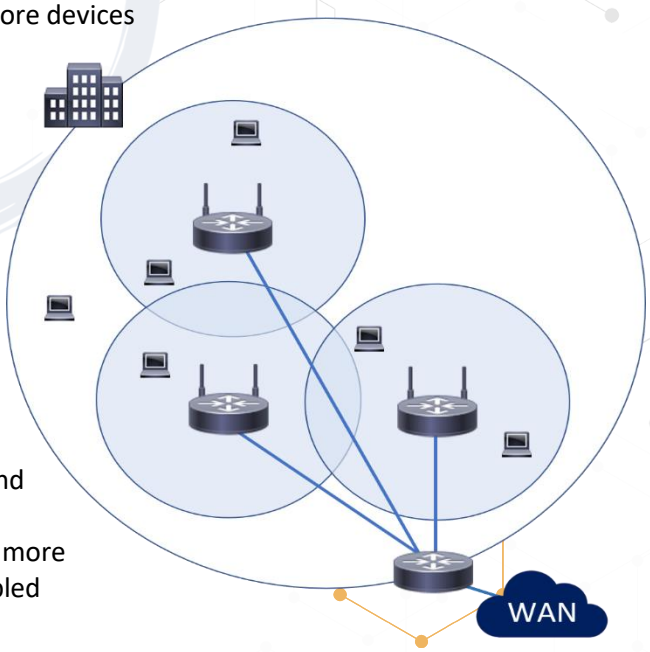


- **Mesh**:
  - Nodes are connected to each other in either a partial mesh or a full mesh.
  - **Partial Mesh**:
    - Nodes are directly connected to some other nodes.
  - **Full Mesh**:
    - All nodes are directly connected to all other nodes.
    - More redundant but requires a lot more cables and NICs.
    - Often used in HA (High Availability) environments, with cluster servers for keepalives.

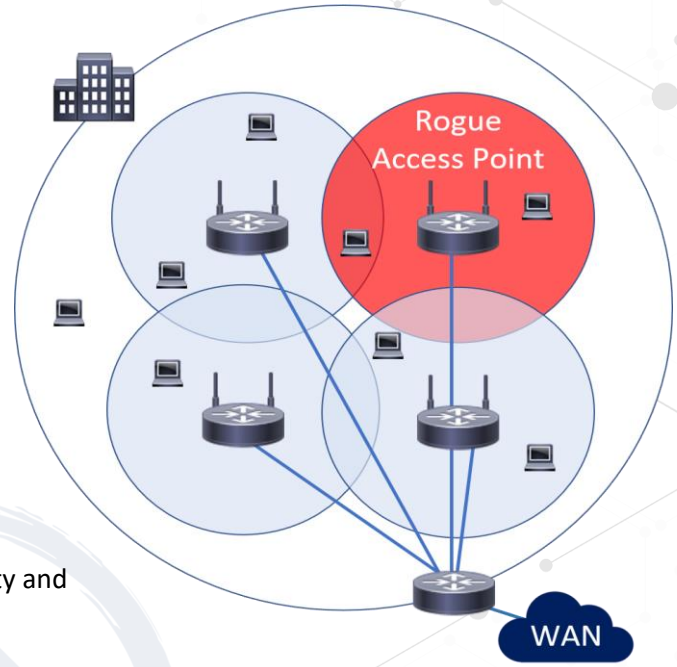


Wi-Fi:

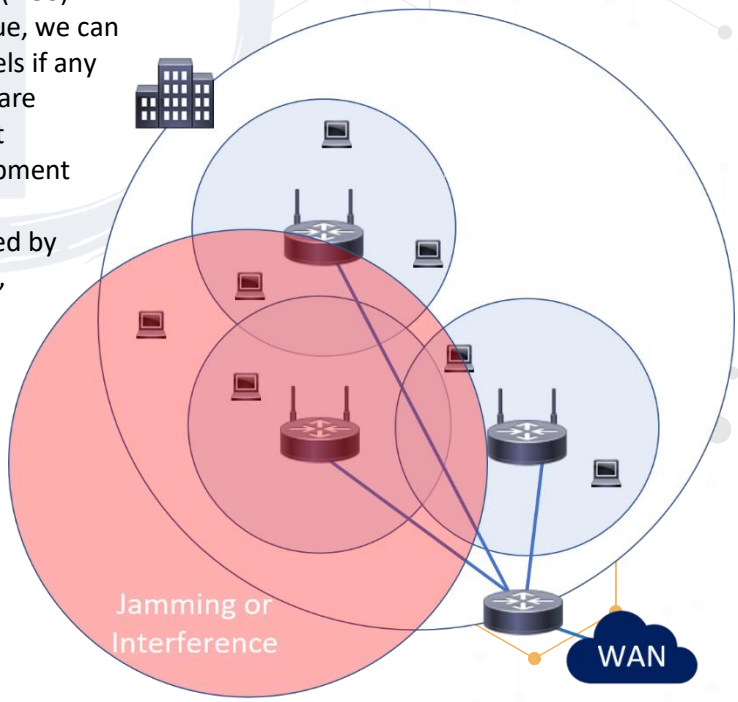
- A wireless computer network that links two or more devices using a wireless distribution method within a limited area (a home, a school, a coffee shop, or an office building).
- Gives users the ability to move around within a locally covered area and be connected to the network.
- Often multiple APs (Access Points) are set up throughout an office building to give seamless roaming coverage for the employees.
- WLAN normally also provides an Internet connection, but not always.
- Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name.
- Wi-Fi makes us more mobile and our connection more seamless, but it is easier to compromise than cabled internet connection.



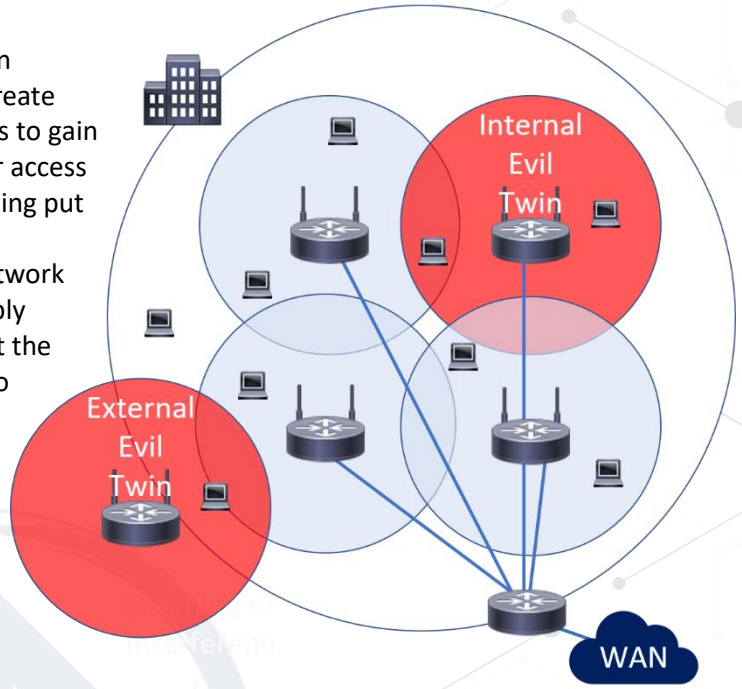
- **Wi-Fi Attacks:**
  - **Rogue Access Points:**
    - An unauthorized access point that has been added to our network without our knowledge.
    - This can be malicious by an attacker or just an employee wanting Wi-Fi somewhere with bad coverage.
    - Without our security posture, they are a very big concern.
    - Can be somewhat mitigated with Port security on the Switches and by scanning for Rogue access points.
    - Can compromise confidentiality and integrity.



  - **Jamming/Interference:**
    - This can be a lot of traffic on the Wi-Fi frequencies or done by attackers to disrupt our network (DOS).
    - If interference is an issue, we can change to other channels if any less crowded channels are available or to different frequencies if our equipment supports it.
    - The 2.4 GHz band is used by Bluetooth, microwaves, cordless phones, baby monitors, Wi-Fi,…
    - Can compromise integrity and availability.



- **Evil Twin:**
  - An evil twin is used when attackers are trying to create rogue access points so as to gain access to the network or access to information that is being put through a network.
  - Can be done on your network or not, the attacker simply names their access point the same as ours but with no security and user devices automatically connect to them.
  - Can compromise confidentiality and integrity.



Wireless Networks:

- **Bluetooth:**
  - A wireless technology standard for exchanging data over short distances using 2.4 GHz from fixed and mobile devices and building personal area networks (PANs).
  - Bluetooth has three classes of devices; while designed for short-distance networking, Class 1 can reach up to 100 meters.
  - Class 1: 100 meters, 2: 10 meters, 3: under 10 meters.
  - Bluetooth implements confidentiality, authentication, and key derivation with custom algorithms based on the SAFER+ block cipher.
  - The E0 stream cipher is used for encrypting packets, granting confidentiality, and is based on a shared cryptographic secret, namely a previously generated link key or master key.
  - Cryptanalysis of E0 has proven it to be weak, attacks show the true strength to be 38 bits or even less.
  - Bluetooth key generation is generally based on a Bluetooth PIN which must be entered on one or both devices.
  - Bluetooth security is to some extent security through obscurity, it assumes the 48-bit MAC address of the Bluetooth adapter is not known.
  - Even when disabled, Bluetooth devices may be discovered by guessing the MAC address.
  - The first 24 bits are the OUI, which can be easily guessed, the last 24 bits can be discovered with brute-force attacks.

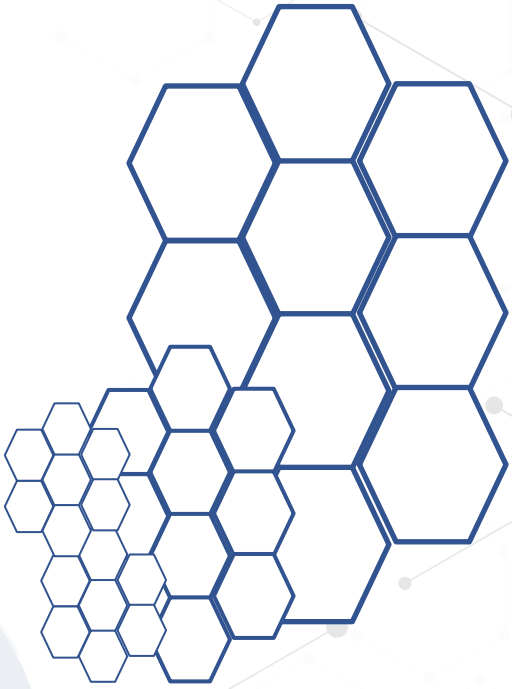
- **Attacks:**
  - **Bluejacking**: Sending unsolicited messages over Bluetooth, most often harmless but annoying.
  - **Bluesnarfing**: Unauthorized access of information from a Bluetooth device: phones, desktops, laptops,...
  - **Bluebugging**: The attacker gains total access and control of your device; it can happen when your device is left in the discoverable state.
  - Only possible on older phones with outdated OSs, newer smartphones constantly update their OS.

- **Countermeasures:**
  - Enable Bluetooth only when you needed it.
  - Enable Bluetooth discovery only when necessary and disable discovery when your devices are paired.
  - Do not enter link keys or PINs when unexpectedly prompted to do so.
  - Remove paired devices when you do not use them.
  - Regularly update firmware on all Bluetooth enabled devices.

- **Li-Fi:**
  - Uses light to transmit data and position between devices.
  - Can send high-speed data using visible light, ultraviolet, and infrared spectrums.
  - Can be used in areas prone to EMI (Electromagnetic interference), such as aircraft cabins, hospitals, and nuclear power plants.
  - Speeds (currently) up to 100 Gbit.
  - Light can reflect off walls and still reach 70 Mbit without requiring a direct line of sight.
  - Pros: Not the same capacity as Wi-Fi (radio frequency exhaustion) and can be used in places where Wi-Fi is prohibited.
  - Cons: Short-range, not always reliable, and high cost of implementation.

- **Zigbee:**
  - Mesh wireless network with low power, low data rate, and close proximity.
  - Simple and less complex compared to other WPANs (Wireless Personal Area Networks) such as Bluetooth or Wi-Fi.
  - It has a range of 10 to 100 meters, but it requires line-of-sight. Data rates vary between 20 kbit/s (868 MHz band) and 250 kbit/s (2.4 GHz band).

- **Satellite:**
  - For many years, satellite internet was a relatively slow and expensive option.
  - You have a modem, as with any other internet connection, as well as a satellite dish (2-3 ft. or 60-90 cm).
  - Typical satellite connections have had a latency of 500 ms and speeds ranging from 10 to 50 Mbps.
  - Starlink is currently testing speeds ranging from 20-200 Mbps down to 15-50 Mbps up, with latencies ranging from 15-40 ms.

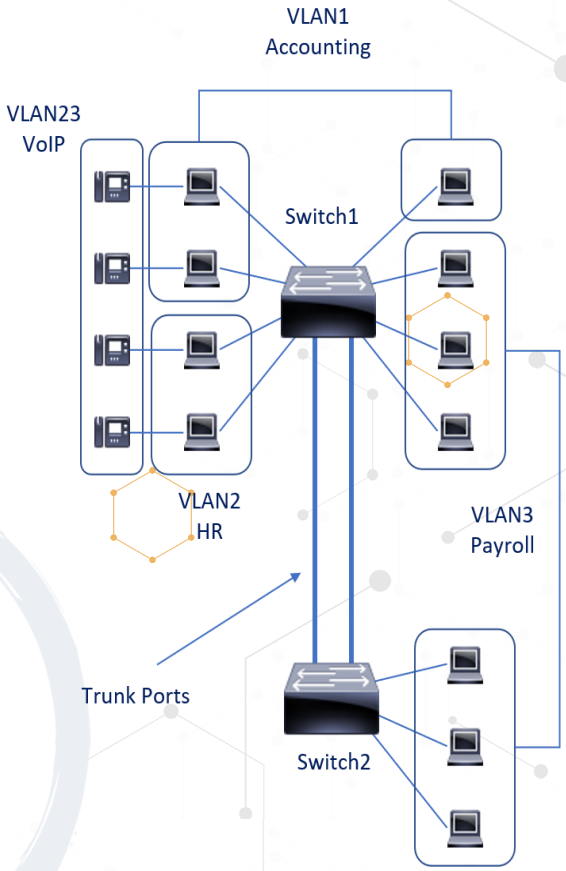


- Cellular networks/mobile networks are communication networks where the last leg is wireless.
- The network is divided into cells and distributed across areas, with each cell containing at least one fixed-location transceiver, if not more.
- These base stations provide network coverage to the cell, allowing it to transmit voice, data, and other types of content.
- To avoid interference and provide guaranteed service quality within each cell, a cell typically uses a different set of frequencies than neighboring cells.

- **3G:**
  - Bandwidth: 2 Mbps, latency: 100-500 ms, average speed 144 kbps.
- **4G:**
  - Bandwidth: 200 Mbps, latency: 20-30 ms, average speed 25 Mbps, 16km (10 miles).
- **5G:**
  - Bandwidth: 5-20 Gbps, latency: <10 ms, average speed 200-400 Mbps, 500m (1500 ft).
  - High frequency, short-range, and can be blocked by anything metal and even just solid objects.
  - A lot more 5G towers are needed to get coverage.

VLANs and Routers:

- **Layer 2 Protocols:**
- **VLAN (Virtual LAN)** is a broadcast domain that is partitioned and isolated at layer 2.
  - Specific ports on a switch are assigned to a certain VLAN.
  - The Payroll VLAN is in 2 different buildings and spans multiple switches.
  - VLANs use tags within network packets and tag handling in networking systems, replicating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks.
  - It allows networks and devices that must be kept separate to share the same physical devices without interacting, for simplicity, security, traffic management, and/or cost reduction.
  - **VLAN Trunks** - Ports connecting two switches to span VLANs across them.
  - VLANs share bandwidth, a VLAN trunk can use link aggregation, quality-of-service prioritization, or both to route data efficiently.



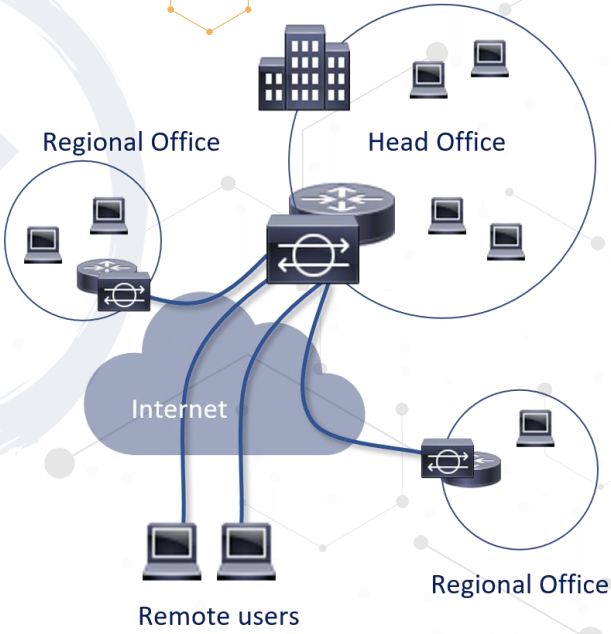
- **Virtual eXtensible Local Area Network (VXLAN):**
  - Made and widely used for cloud computing with organizations that have mass tenants. (Think AWS, Google or similar).
  - Solves the issue with only having 4094 maximum VLANs.

VLAN	VXLAN
Maximum 4094 VLANs, 12-bit VLAN ID.	Maximum 16 million VLANs, 24-bit VLAN ID.
Less flexible and not very suitable for cloud multi-tenant environment.	Very flexible and very suitable for cloud multi-tenant environment.
Uses VLAN tagging on L2 frame for encapsulation to extend VLAN across switches.	Uses MAC-in-UDP encapsulation to extend L2 segments across locations.
VLAN is any L2 partitioned and isolated broadcast domain on our network.	VXLAN is an encapsulation protocol that runs an overlay network on existing L3 infrastructure.

- **Layer 3 Devices:**
  - **Routers:**
    - Normally have a few ports vs. a lot on switches.
    - For our organizations, they are in the data centers.
    - In your home, they are often combined with a switch and wireless in one box.
    - Forward traffic based on source and destination IPs and ports.
    - Connecting our LANs to the WAN.
    - Send traffic to the most specific route in their routing table.
    - **Static route** is a preconfigured route, always sends traffic there for a certain subnet.
    - **Default gateway** sends all non-local traffic to an ISP for instance.
    - **Dynamic route** is learned from another routing via a routing protocol (OSPF, EIGRP, BGP, IS-IS).
    - **Metric** is used to determine the best route to a destination.

VPNs, NAC, and Third-party Connectivity:

- **Authentication Protocols:**
  - **VPN (Virtual Private Network):**
    - Extends a private network across a public network and users can send and receive data across shared or public networks as if they were on the private network.
    - VPNs may allow employees and satellite offices to securely access the organization's intranet.
    - They are used to securely connect.
    - Can also be used to get around geo-restrictions and censorship or to connect to proxy servers for the purpose of protecting personal identity and location.
    - Created by establishing a virtual point-to-point connection using dedicated connections, virtual tunneling protocols or traffic encryption.



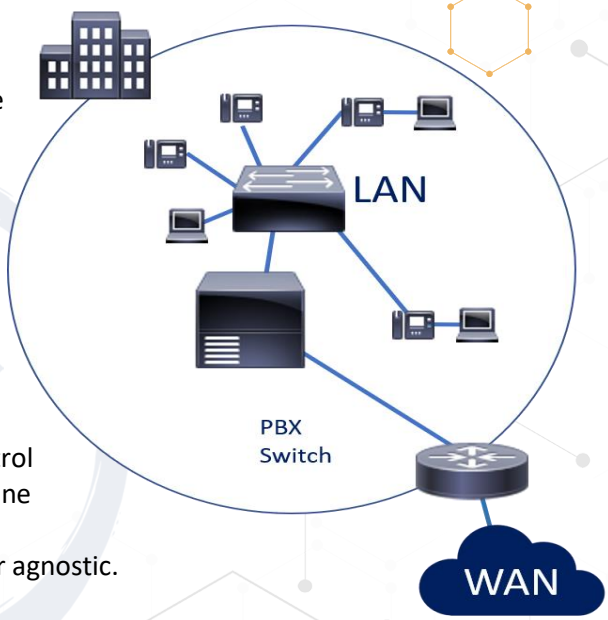
- **Third-party Connectivity:**
  - Medium size enterprises typically have 20 or more third-party providers. I believe the hospital where I worked in Hawaii had more than 200 third-party providers.
  - How do we ensure they are secure enough and conform to our policies and procedures?
  - Many never have direct contact with IT or IT-Security.

- We must conduct a thorough risk assessment to ensure that whatever they provide does not jeopardize our security posture, or we must accept the risk.
- We should have MOUs/MOAs and ISAs (Interconnection Security Agreement).

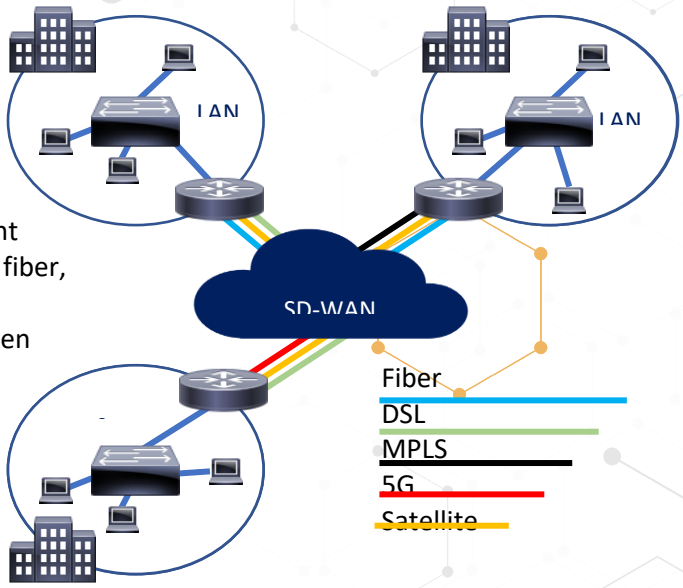
- **Network Access Control (NAC):**
  - Automatic detection and response to ensure our systems are in adherence with our security policies.
  - Can helps us with the prevention or reduction of 0-day and known attacks.
  - Along with ensuring that security policies are adhered to at all times.

SDN, SD-WAN, and SDX:

- **SDN (Software-Defined Networking):**
  - Allows network administrators via software to initialize, control, change, and manage network behavior dynamically.
  - Addresses the static architecture of traditional networks that doesn't support the dynamic, scalable computing and storage needs of more modern computing environments such as data centers.
  - This is done by separating the router's control plane from the data plane, the control plane makes routing decisions, the data plane forwards data through the router.
  - Giving us the option to be hardware vendor agnostic.



- **Software-Defined Wide Area Network (SD-WAN)**
  - 85%+ of surveyed companies have deployed or plan to deploy within 2 years (Cisco/FortiNet).
  - **Why we are seeing a move towards SD-WAN:**
    - Higher cheaper bandwidth, flexibility and scalability of bandwidth allocation, and traffic engineering.
    - Ability to utilize many different connection types (DSL, cable, fiber, satellite, 4G/5G, ...).
    - Near real-time failover between connection types.
    - Centralized easier management, better insights, reporting, and statistics.

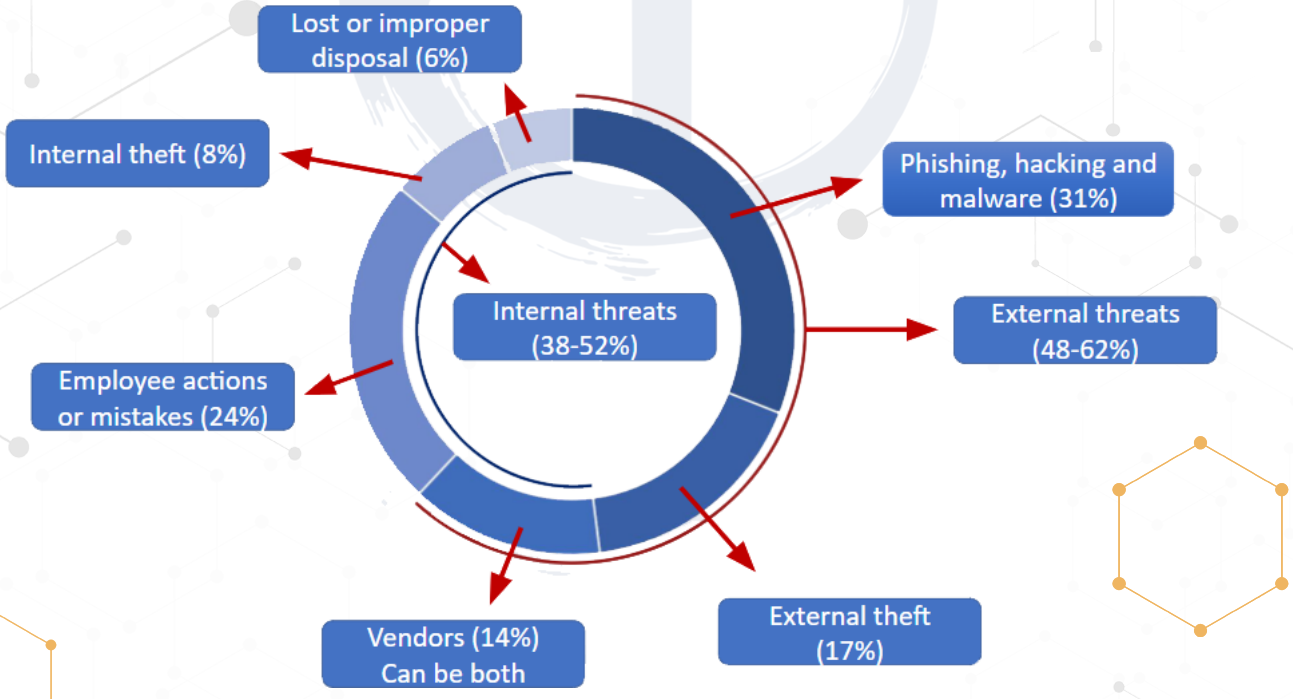


- Better performance with intelligent routing, it can choose the optimal network circuit for a given application or type of traffic.
- Rapid deployment with pre-configured appliances or virtual appliances.
- Secure connectivity - IPSec and next-generation firewall.

- **SDx (Software-Defined Everything):**
  - Any function that can be performed by or automated by software. This includes networking, storage, data center, compute, security, WAN, really anything.

Attacks and Attackers:

- **Hackers:**
  - **Now:** Anyone trying to get access to or disrupt any leg of the CIA Triad (Confidentiality, Integrity, Availability).
  - **Original use:** Someone using something in a way not intended.
  - **White Hat hackers:** Professional pen testers trying to find flaws so we can fix it (Ethical hackers).
  - **Black Hat hackers:** Malicious hackers, trying to find flaws to exploit them (Crackers – they crack the code).
  - **Gray/Grey Hat hackers:** They are somewhere between the white and black hats, they go looking for vulnerable code, systems or products.
  - **Script Kiddies:** They have little or no coding knowledge, but many sophisticated hacking tools are available and easy to use.

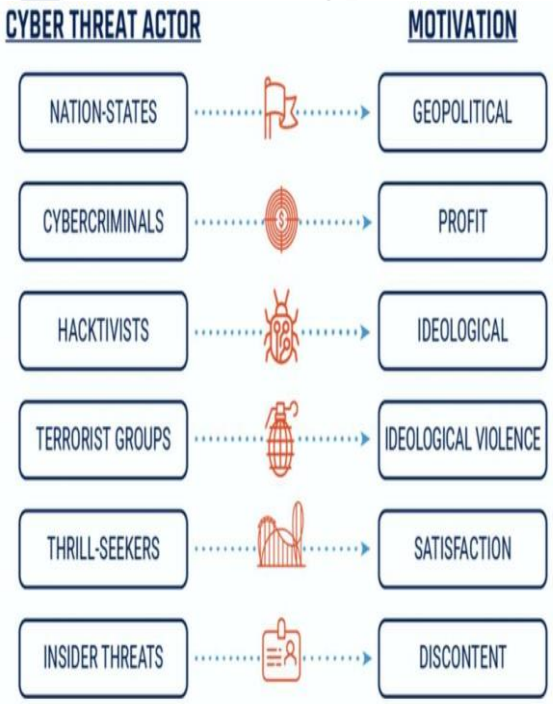


- **Outsiders:**
  - Unauthorized individuals - Trying to gain access; they launch the majority of attacks but are often mitigated if the organization has good Defense in Depth.
  - Interception, malicious code (e.g. virus, logic bomb, trojan horse), sale of personal information, system bugs, system intrusion, system sabotage or unauthorized system access.
  - 48-62% of risks are from outsiders.

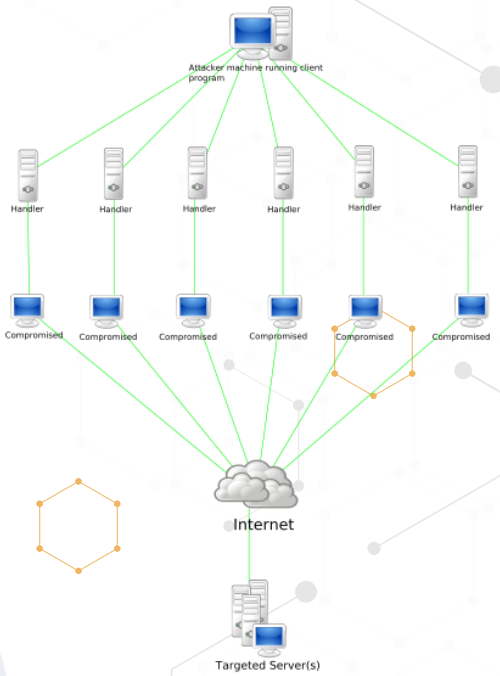
- **Insiders:**
  - Authorized individuals - Not necessarily to the compromised system, who intentionally or unintentionally compromise the system or data.
  - This could be assault on an employee, blackmail, browsing of proprietary information, computer abuse, fraud and theft, information bribery, input of falsified or corrupted data.
  - 38-52% of risks are from insiders, another reason good Authentication and Authorization controls are needed.

- **Hacktivism/Hacktivist (hacker activist):** Hacking for political or socially motivated purposes.
  - Often aimed at ensuring free speech, human rights, freedom of information movement.

- **Governments:**
  - State sponsored hacking is common; often you see the attacks happening between the hours of 9 and 5 in that time zone; this is a day job.
  - Approximately 120 countries have been developing ways to use the internet as a weapon to target financial markets, government computer systems and utilities.
  - Famous attacks: US elections (Russia), Sony websites (N. Korea), Stuxnet (US/Israel), US Office of Personnel Management (China), …



- **Bots and botnets** (short for robot):
  - **Bots** are a system with malware controlled by a botnet.
  - The system is compromised by an attack or the user installing a remote access trojan (game or application with a hidden payload).
  - They often use IRC, HTTP, or HTTPS.
  - Some are dormant until activated.
  - Others are actively sending data from the system (Credit card/bank information for instance).
  - Active bots can also be used to send spam emails.



- **Botnets** is a C&C (Command and Control) network, controlled by people (bot-herders).
  - There can often 1,000s or even 100,000s of bots in a botnet.

- **Malware:**
  - **Malware (Malicious Code) -** This is the catch-all name for any malicious software used to compromise systems or data.
    - **Viruses** - require some sort of human interaction and are often transmitted by USB sticks or other portable devices.
    - When the program is executed, it replicates itself by inserting its own code into other programs.
      - **Macro** (document) Viruses: Written in Macro Languages, embedded in other documents (Word, Outlook).
      - **Boot Sector** Viruses: Infect the boot sector or the Master Boot Record, ensuring they run every time the PC boots.
      - **Stealth** Viruses: Try to **hide themselves** from the OS and antivirus software.
      - **Polymorphic** Viruses: **Change their signature** to avoid the antivirus signature definitions.
      - **Multipart** (Multipartite) Viruses: Spread across **multiple vectors**. They are often hard to get rid of because even if you clean the file infections, the virus may still be in the boot sector and vice-versa.
  - **Worms** - spread through **self-propagation** - they need no human interaction; they do both the payload damage and replicate through aggressive network use (also makes them easier to spot).
  - **Trojans** - malicious code **embedded** in a program that is normal. This can be games, attachments, website clicks, etc.

- **RAT** (Remote Access Trojan): A malware program that gives the attacker admin control over the target system.

- **Antivirus Software** - tries to protect us against malware.
  - **Signature** based - looks for known malware signatures - MUST be updated constantly.
  - **Heuristic** (Behavioral) based - looks for abnormal behavior - can result in a lot of false positives.

Intrusion Detection and Prevention Systems (IDS/IPS):

- **IDS's and IPS's:**
  - We use both IDS's (Intrusion Detection Systems) and IPS's (Intrusion Prevention Systems) on our network to capture and alert or block traffic seen as malicious.
  - They can be categorized into 2 types and with 2 different approaches toward identifying malicious traffic.
    - **Network-Based**, placed on a network segment (a switch port in promiscuous mode).
    - **Host-Based**, on a client, normally a server or workstation.
    - **Signature (Pattern) Matching**, similar to anti-virus, it matches traffic against a long list of known malicious traffic patterns.
    - **Heuristic-Based (Behavioral)**), uses a normal traffic pattern baseline to monitor for abnormal traffic.
  - Just like firewalls, routers, servers, switches, and everything else in our environment they just see part of the larger picture, for full picture views and data correlation we use a **SIEM** (Security Information and Event Management) system or even better a SOAR (Security Orchestration, Automation, and Response) system.

- **IDS (Intrusion Detection System):**
  - They are passive, they monitor, but they take no action other than sending out alerts.
  - Events trigger alerts: Emails/text message to administrators or an alert on a monitoring tool, but if not monitored right this can take hours before noticed.
- **IPS (Intrusion Prevention System):**
  - Similar to IDS, but they also take action to malicious traffic, what they do with the traffic is determined by configuration.
  - Events trigger an action, drop/redirect traffic, often combined with the trigger monitoring/administrator warnings, emails, or text messages.
- **IDS/IPS:**
  - Part of our layered defense.
  - Basically, they are packet sniffers with analysis engines.
- **Network-Based**, placed on a network segment (a switch port in promiscuous mode).
  - Looks at a segment of our network, normally a switch, but can aggregate multiple switches.

- Inspects Host/destination ports, IP's, protocols, content of traffic, but can obviously not look in encrypted traffic.
- Can protect against DDOS, Port scans, brute force attacks, policy violations, …
- Deployed on one switch, port and NIC must be promiscuous, and port must be a span port.

- **Host-Based**, on a client, normally a server or workstation.
  - We only look at a single system.
  - Who is using the system, the resource usage, traffic, ...
  - It can be application specific; it doesn't have to be the entire system we monitor.
  - If we do choose to do traffic analysis it will impact the host by slowing it down.
  - Certain attacks can turn off HIDS/HIPS.
  - Can look at the actual data (it is decrypted at the end device), NIDS/NIPS can't look at encrypted packets.
- **Signature-Based:**
  - Looks for known malware signatures.
  - Faster since they just check traffic against malicious signatures.
  - Easier to set up and manage, someone else does the signatures for us.
  - They are completely vulnerable to 0-day attacks and have to be updated constantly to keep up with new vulnerability patterns.
- **Heuristic-Based (Behavioral):**
  - Looks for abnormal behavior - can produce a lot of false positives.
  - We build a baseline of what normal network traffic looks like and all traffic is matched to that baseline.
  - Traffic not matching the baseline is handled depending on settings, they can take a lot of tweaking.
  - Can detect 'out of the ordinary' activity, not just attacks.
  - Takes much more work and skills.
- **Hybrid-Based:**
  - Systems combining both are more used now and check for both signatures and abnormalities.

- **Intrusion Events and Masking:**
  - IDS/IPS obviously then prompt attackers to develop attacks that try to avoid detection.
    - **Fragmentation:** Sending fragmented packets, the attack can avoid the detection system's ability to detect the attack signature.
    - **Avoiding Defaults:** The TCP port utilized by a protocol does not always provide an indication to the protocol which is being transported. Attackers can send malware over an unexpected port.
    - **Low-Bandwidth Coordinated Attacks:** A number of attackers (or agents) allocate different ports or hosts to different attackers making it difficult for the IDS to correlate the captured packets and deduce that a network scan is in progress.

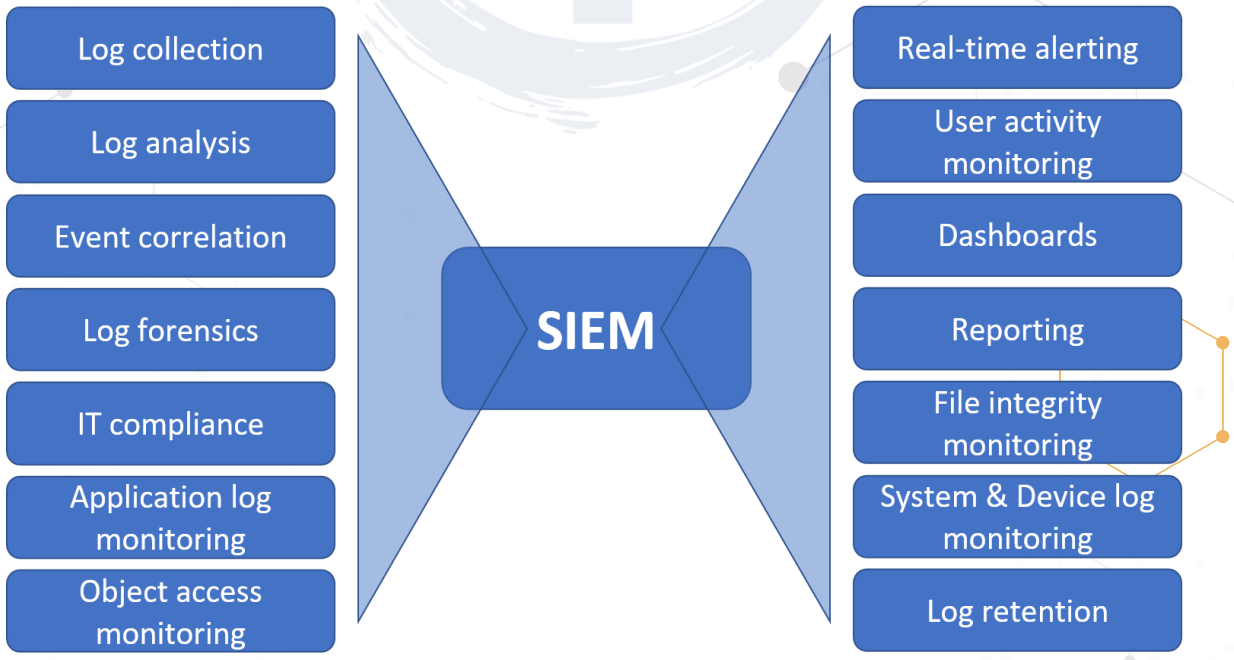
- **Alerts on IDS's/IPS's can, like biometrics, be one of 4 categories:**
  - **True Positive:** An attack is happening, and the system detects it and acts.
  - **True Negative:** Normal traffic on the network and the system detects it and does nothing.
  - **False Positive:** Normal traffic and the system detects it and acts.
  - **False Negative:** An attack is happening the system does not detect it and does nothing.

	TRUE	FALSE
POSITIVE	True-Positive Rule matched Attack	False-Positive Rule matched No attack
NEGATIVE	True-Negative No rule matched No attack	False-Negative No rule matched Attack

- We rarely talk about the "true" states since things are happening like they are supposed to, we are interested in when it doesn't, and we prevent authorized traffic or allow malicious traffic.

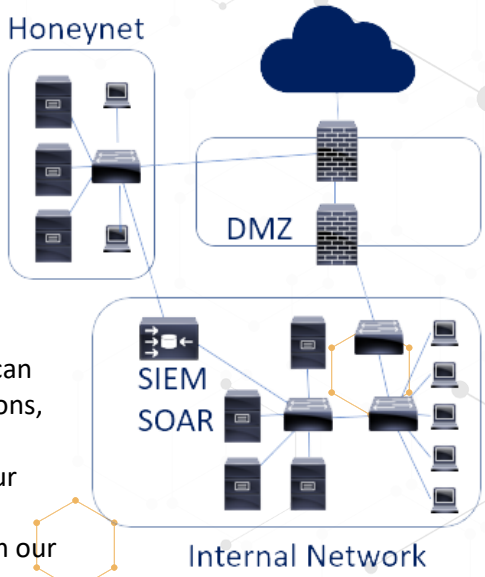
SIEM and SOAR systems:

- **SIEM (Security information and event management):**
  - Provides a holistic view of our organization's events and incidents.
  - Gathers from all our systems and looks at everything.
- **SOAR (Security Orchestration, Automation, and Response):**
  - A software solution that uses AI to allows us to respond to some security incidents automatically.
  - SOAR will also react to some events.



Honeypots and Honeynets:

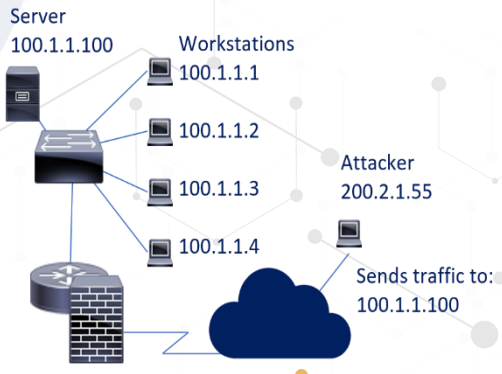
- **Honeypots and Honeynets:**
  - **Honeypots:**
  - System looking like a real system, but with the sole purpose of attracting attackers.
  - They are used to learn about our vulnerabilities and how attackers would circumvent our security measures.



  - **Honeynets:**
    - A network (real or simulated) of honeypots, can be a full server farm simulated with applications, OSs, and fake data.
    - Best practice segments the honeynet from our actual network by a DMZ/firewall.
    - The SIEM/SOAR systems collect the data from our internal systems as well as the honeynet.

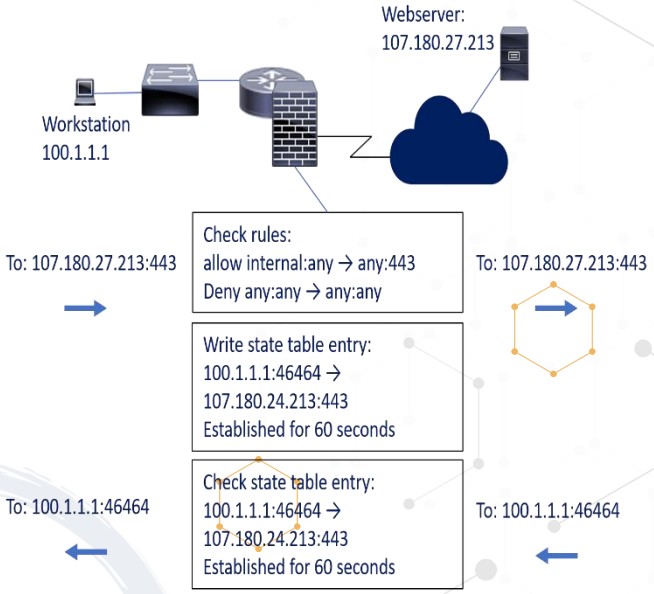
Firewalls:

- **Firewalls:** A firewall typically establishes a barrier between a trusted, secure internal network, and another outside network, like the Internet.
  - **Packet filtering firewalls**, OSI Layer 1-3.
    - Packet filters act by inspecting the "packets" which are transferred between clients.
    - If a packet does not match the packet filter's set of filtering rules, the packet filter will drop the packet or reject it and send error responses to the source.
    - Any packet that matches one of the Permits is allowed to pass.
    - Rules are checked in order; the attacker's traffic is dropped on the 3rd filter rule. Drop anything trying to access 100.1.1.100.
    - The internal machines can access the server since their IPs are whitelisted in the first rule.

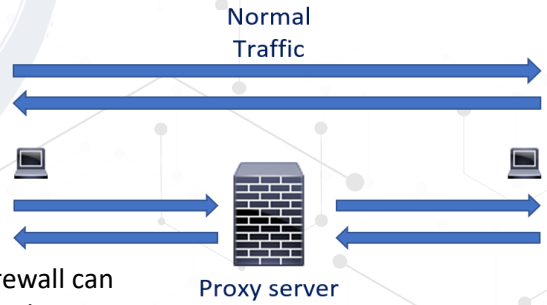


Source	Destination	Action
100.1.1.0/24	100.1.1.0/24	Permit
100.1.1.0/24	Any	Permit
Any	100.1.1.100	Deny
Any	Any	Deny

- **Stateful filtering firewalls**, OSI Layer 1-4.
  - Records all connections passing through and determines whether a packet is the start of a new connection, a part of an existing connection or not part of any connection.
  - Static rules are still used, these rules can now contain connection state as one of their criteria.
  - Some DOS attacks bombard the firewall with thousands of fake connection packets trying to overwhelm the firewall by filling its connection state memory.



- **A proxy server** can act as a firewall by responding to input packets in the manner of an application while blocking other packets.
  - A proxy server is a gateway from one network to another for a specific network application in the sense that it functions as a proxy on behalf of the network user.
- **Application layer firewalls**, OSI Layer 7.
  - The key benefit of application layer firewalls is that they can understand certain applications and protocols.
  - They see the entire packet, the packet isn't decrypted until layer 6, any other firewall can only inspect the packet but not the payload.
  - They can detect if an unwanted application or service is attempting to bypass the firewall using a protocol on an allowed port or detect if a protocol is being used any malicious way.

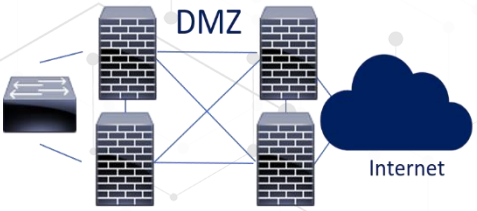


- **Network firewalls** filter traffic between two or more networks, either software appliances running on general purpose hardware or hardware-based firewall.
- **Host-based firewalls** provide a layer of software security on one host that controls network traffic in and out of that single machine.

- **Next-generation firewall (NGFW)**
  - NGFW combines traditional firewall technologies with deep packet inspection (DPI) and network security systems (IDS/IPS, malware filtering and antivirus).
  - Packet inspection in traditional firewalls only looks at the protocol header of the packet DPI also looks at the actual data the packet is carrying.
  - Next-generation firewalls tries to include more layers of the OSI model, improving filtering of network traffic that is dependent on the packet contents.
  - DPI firewalls track the progress of web browsing sessions and can tell if a packet payload, when assembled with other packets in an HTTP server reply, is actually a legitimate HTML-formatted response.

- **Firewalls Design:**
  - **DMZs:**
    - Normal DMZs use 2 firewalls in a screened subnet, but they can also be three-legged DMZs which only use 1 firewall.
    - Physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, like the Internet.
    - It adds an additional layer of security to our organization's LAN, an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled.
    - Firewalls are designed to fail closed, if they crash, get flooded with traffic or are shut down, they block all traffic.
    - To get some redundancy we often use firewall pairs and have the firewall in a mesh topology, this way one firewall failure will just shift the traffic paths.

3-legged DMZ



Firewall pair

0-day Attacks and Exploits:

- **0-day Vulnerabilities:**
  - Vulnerabilities not generally known or discovered, the first time an attack is seen is considered day 0, hence the name.
  - From when a vulnerability is discovered it is now only a short timespan before patches or signatures are released on major software.
  - With millions of lines of code in a lot of software and the 1% errors we talked about there will always be new attack surfaces and vulnerabilities to discover. The only real defense against the 0-day exploits is defense in depth and when discovered immediate patching as soon as it is available, and we have tested it in our test environments. Most signatures in IDS/IPS and anti-virus auto update as soon as new signatures are available.
  - **0-day Vulnerability:** The vulnerability that has not been widely discovered and published.
  - **0-day Exploit:** Code that uses the 0-day vulnerability.
  - **0-day Attack:** The actual attack using the code.

  - **Stuxnet has three modules:**
    - A **worm** that executes all routines related to the main payload of the attack.
    - A **link** file that automatically executes the propagated copies of the worm.
    - A **rootkit** responsible for hiding all malicious files and processes, preventing detection of Stuxnet.
    - It is introduced to the target environment by an infected USB flash drive.
    - The worm then propagates across the network, scanning for Siemens Step7 software on computers controlling a PLC, If both are not present, Stuxnet becomes dormant inside the computer, it will still replicate the worm.
    - If both are present, Stuxnet introduces the infected rootkit onto the PLC and Step7 software, modifying the codes and giving unexpected commands to the PLC while returning a loop of normal operations system values feedback to the users.

Vulnerability Scanning/Testing:

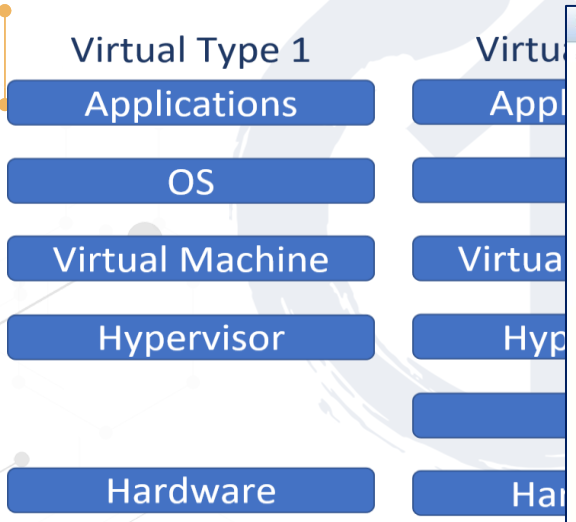
- **Vulnerability Scanning/Testing:**
  - A vulnerability scanning tool is used to scan a network or system for a list of predefined vulnerabilities such as system misconfiguration, outdated software, or a lack of patching.
  - It is very important to understand the output from a vulnerability scan, they can be 100's of pages for some systems, and how do the vulnerabilities map to Threats and Risks (Risk = Threat x Vulnerability).
  - When we understand the true Risk, we can then plan our mitigation.

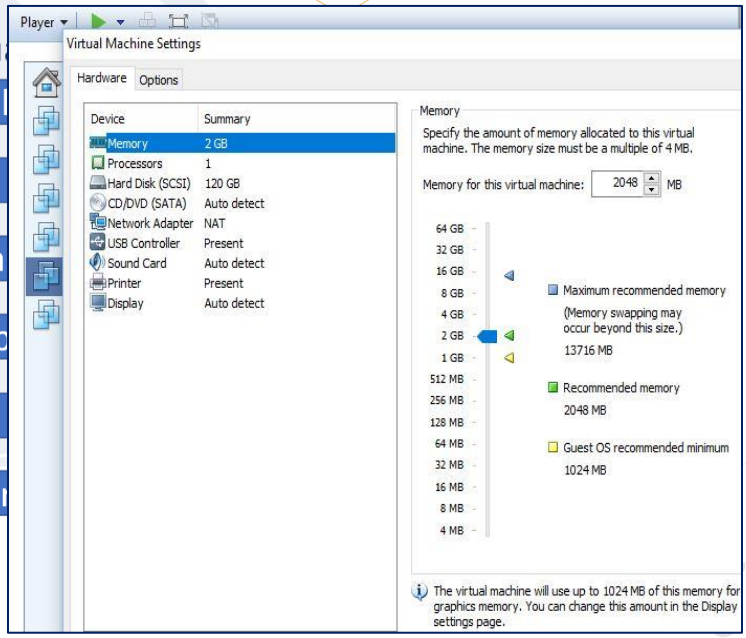
Virtualization, Cloud, and Distributed Computing:

- **Virtualization:**
  - **Virtualization** poses a whole new set of standards, best practices, and security concerns.
  - With Virtualization we have many servers (clients) on the same hardware platform (host).
  - Virtualization is software running under the OS and above the Hardware (Ring -1).
  - Traffic between the clients on the host doesn't have to traverse our network.
  - Common Virtualization software could be VMWare, Hyper-V, or Xen.
  - With Distributed Computing we use either multiple local or remote clients for our needs, most commonly cloud computing. How do we ensure the cloud Data Center meets our security posture, how do they segment their network?

- **Virtualization holds a ton of benefits:**
  - Virtualized environments cost a lot less than all physical servers.
  - It is much easier to stand up new servers (don't need to buy hardware, wait 2 weeks, rack it, run power/internet).
  - You can easily back up servers with snapshots; server builds can be done with images.
  - You can instantly reallocate resources.
  - They have lower power and cooling costs, a much smaller rack footprint (50-100 servers in the space of 5-8).

- **Hypervisor** - Controls the access between the virtual guest/clients and the host hardware.
  - Type 1 hypervisor (Bare Metal) is a part of a Virtualization OS that runs on top of the host hardware (Think Data Center).
  - Type 2 hypervisor runs on top of a regular OS like Windows 10 - (Think your PC).



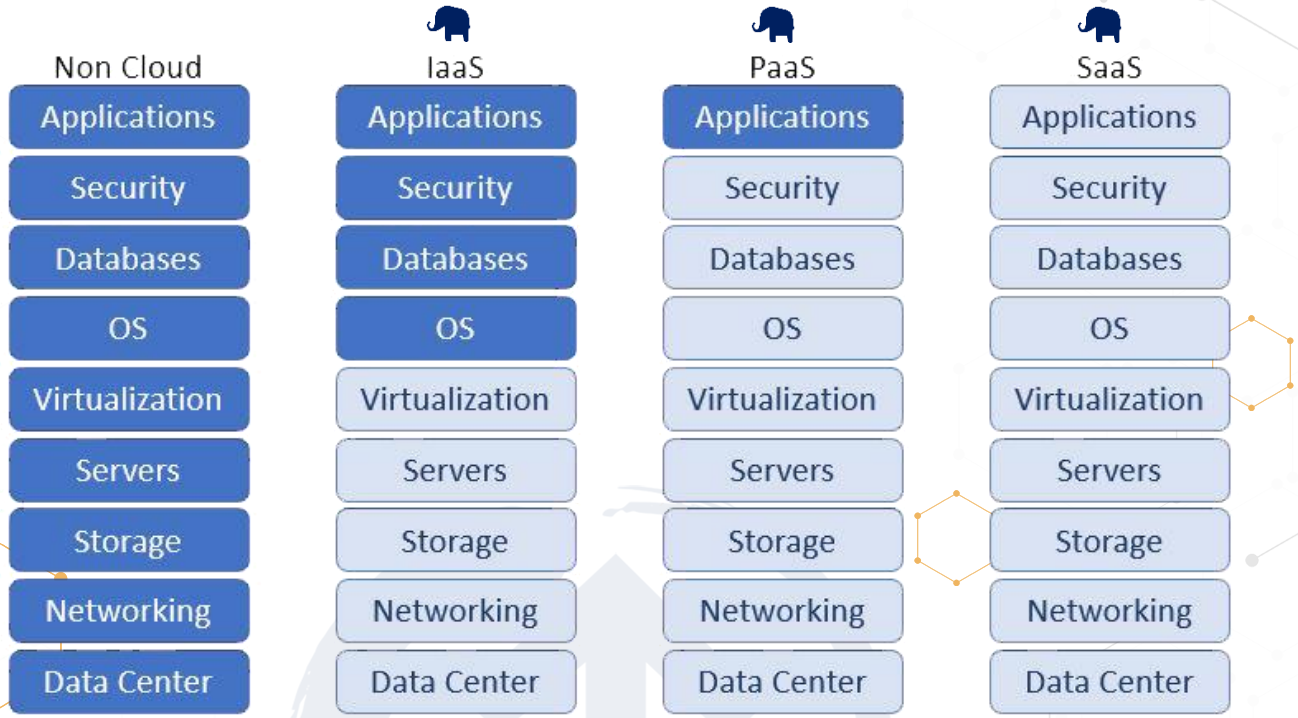


- Virtualization also poses new vulnerabilities because the technology is new-ish and very complex.
- Clients on the same host should be on the same network segment (Internal/DMZ). A host should never house both zones.
- Clients should be logically separated on the network like physical servers would be (HR, Accounting, IT VLANs).
- **VM Escape** (Virtualization escape) is when an attacker can jump from the host or a client to another client, this can be even more of a concern if you have different Trust Level Clients on the same host. They should ideally be on separate hosts.
- **Hypervisor Security** - If an attacker can get access to the hypervisor, they may be able to gain access to the clients.

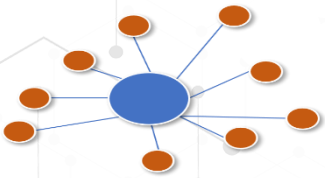
- **Resource Exhaustion** - Admins oversubscribe the CPU/Memory and do not realize more is needed (availability).

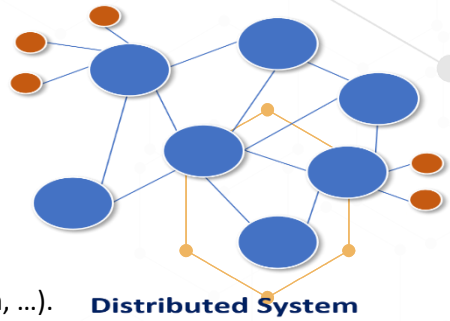
- **Cloud Computing:**
  - **Cloud Computing** - (There is no 'Cloud', it is just another computer somewhere else).
    - When we use cloud computing we build or outsources some part of our IT Infrastructure, storage, applications.
    - This can be done for many good reasons, but most are cost related.
    - Cloud Computing can be divided into 4 main types:
      - **Private Cloud Computing** - Organizations build and run their own cloud infrastructure (or they pay someone to do it for them).
      - **Public Cloud Computing** - Shared tenancy – A company builds massive infrastructures and rents it out to anyone who wants it. (Amazon AWS, Microsoft, Google, IBM).
      - **Hybrid Cloud Computing** – A mix of Private and Public Cloud Computing. An organization can choose to use Private Cloud for sensitive information and Public Cloud for non-sensitive data.
      - **Community Cloud Computing** – Only for use by a specific community of consumers from organizations that have shared concerns. (Mission, policy, security requirements, and/or compliance considerations.)
  - As with any other outsourcing, make sure you have the right to audit, pen test (clearly agreed upon criteria), conduct vulnerability assessment, and check that the vendor is compliant with your industry and the standards you adhere to.

- **Cloud Computing Public Cloud Computing:**
  - Platforms are normally offered as:
    - **IaaS** - (Infrastructure as a Service) The vendor provides infrastructure up to the OS; the customer adds the OS and up.
    - **PaaS** - (Platform as a Service) The vendor provides pre-configured OSs, then the customer adds all programs and applications.
    - **SaaS** - (Software as a Service) The vendor provides the OS and applications/programs. Either the customer interacts with the software manually by entering data on the SaaS page, or data is automatically pushed from your other applications to the SaaS application (Gmail, Office 365, Dropbox, Payroll,…).

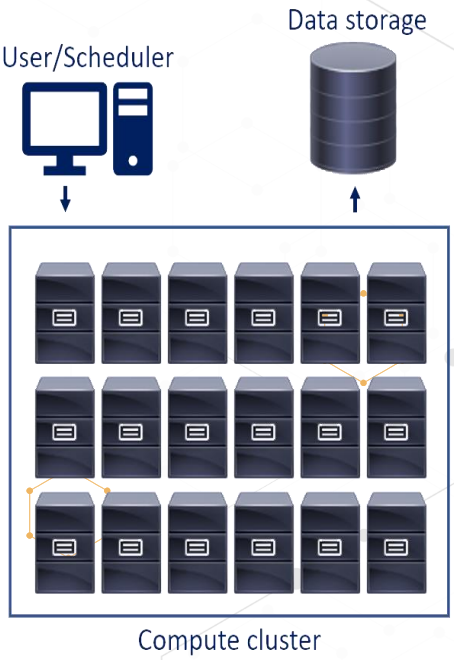


- **Distributed Systems:**
  - **Can also be referred to as:**
    - Distributed computing environment (DCE), concurrent computing, parallel computing, and distributed computing.
  - A collection of individual systems that work together to support a resource or provide a service.
  - Most end-users see the DCE as a single entity and not as multiple systems.
  - **Why do we use DCEs?**
    - They can give us horizontal scaling (size, geography, and administration), modular growth, fault tolerance, cost-effectiveness, low latency (users connect to the closest node).
  - **Where do we use DCEs?**
    - All over the place (The internet, websites, cell networks, research, P2P networks, blockchain, …).


Centralized System


Distributed System

- **High-Performance Computing (HPC) Systems:**
  - Most often aggregates of compute nodes in a system designed to solve complex calculations or manipulate data at very high speeds.
  - HPCs have 3 components. Compute, network, and storage.
  - All 3 must have enough resources to not become a bottleneck.
  - Most well-known versions are super computers.
- **Edge Computing Systems:**
  - The processing of data is done as close as possible to where it is needed, we do that by moving the data and compute resources.
  - This will optimize bandwidth use and lower latency.
  - CDN's are one of the most common types of edge computing.
  - 80%+ of large enterprises have already implemented or are in the process of implementing an edge computing strategy.



The Internet of Things (IoT):

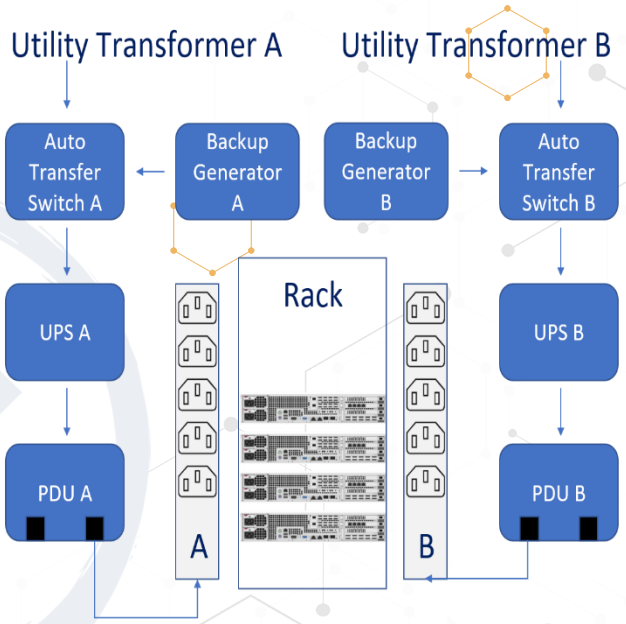
- It is really anything "Smart": Smart TVs, Thermostats, Lightbulbs, Cars, anything that connects to the internet in some way (that didn't before).
- They can be an easy way into your smart device, as most are never patched (many don't even have the option).

Asset Tracking and Hardware Hardening:

- **Asset Tracking:**
  - Keeping an accurate inventory of all our assets is important; we can't protect what we don't know we have.
  - We covered this a little in our risk analysis section, but other than identifying the assets, we also should have it as part of our technology refresh cycle to record the Asset Serial Number, Model Number, and often an internal Asset ID.
- **Hardware Hardening:**
  - On our servers - we harden the server.
    - Apply all patches, block ports not needed, delete default users, … most places are good about this.
  - Workstations are often overlooked.
- **Disabling the USB Ports**, CD drives and any other port that can introduce malware to our network:
  - Physically: Disabled on motherboard or port itself blocked, easy to bypass - not very secure.
  - Logically: Locked in Windows services or through AD (Active Directory) is not easy to bypass (if done right) - more secure.

Electricity:

- **Electricity:**
  - **Electricity** - It is important to have clean, reliable power for our servers, disk arrays, network equipment.
  - Loss of power can affect our availability and the Integrity of our data.
    - Nothing can be accessed, and power fluctuations can damage hardware and corrupt data.
  - **Power Fluctuation** Terms:
    - **Blackout** - Long loss of power.
    - **Fault** - Short loss of power.
    - **Brownout** - Long low voltage.
    - **Sag** - Short low voltage.
    - **Surge** - Long high voltage.
    - **Spike** - Short high voltage.



  - **Surge Protectors**, **UPSs** and Generators are used to get clean power.
    - **Surge Protectors** - Protect equipment from high voltage.
    - **UPSs (Uninterruptible Power Supplies):**
      - Ensure constant clean power to the systems.
      - Have large battery banks that take over in the event of a power outage, they also act as surge protectors.
    - **Generator:**
      - Fueled generators are programmed to kick in during a power outage event manually or automatically (preferred).
      - Will run as long as they have fuel, must be maintained.
    - **PDU (Power Distribution Unit)** can be in rack or not.

Backups:

- **Fault Tolerance:**
  - To ensure our internal SLAs and provide as high availability as possible we use as high degree of redundancy and resiliency as makes sense to that particular system and data set.
  - **Backups:**
    - One of the first things that comes to mind when talking about fault tolerance is backups of our data, while it is very important it is often like log reviews an afterthought and treated with "Set it and forget it" mentality.
    - For backups we use Full, Incremental, Differential and Copy backups, and how we use them is determined on what we need from our backups.
    - How much data we can stand to lose and how fast we want the backup and restore process to be.
    - In our backup solution we make backup policies of what to back up, what to exclude, how long to keep the data of the Full, Incremental and Differential backups.
    - All these values are assigned dependent on what we back up, and normal organizations would have different backup policies and apply those to the appropriate data.
    - This could be Full 3, 6, 12, 36, 84 months and infinity, the retention is often mandated by our policies and the regulations in our field of business.
    - It is preferable to run backups outside of business hours, but if the backup solution is a little older it can be required to run around the clock, in that case we put the smaller and less important backups in the daytime and the important larger ones after hours.
    - We often want to exclude parts of the system we are backing up, this could be the OS, the trashcan, certain program folders, ... we just backup what is important and rarely everything.
    - If a system is compromised and the issue is a rootkit, the rootkit would persist on the backup if we did a full mirror restore, by eliminating some of the system data we not only backup a lot less data, we also may avoid the infection we are trying to remedy.
    - For very important data we may do hourly incremental or use another form of data loss prevention (covered later in this chapter).

      Full Backup:
      - This backs everything up, the entire database (most often), or the system.
      - A full backup clears all archive bits.
      - Dependent on the size of the data we may do infrequent full backups, with large datasets it can take many hours for a full backup.
      - **IF we need to restore on Thursday:**

→ Restore with a single Wednesday full backup tape.
→ 1 tape.

Full Backup:

- Everything in the backup policy is backed up.

- **Incremental Backup:**
  - Backs up everything that has changed since the last backup.
  - Clears the archive bits.
  - Incremental are often fast to do, they only backup what has changed since the last incremental or full.
  - The downside to them is if we do a monthly full backup and daily incremental, we have to get a full restore and could have to use up to 30 tapes, this would take a lot longer than with 1 Full and 1 Differential.
  - **IF we need to restore on Thursday:**
    → Restore with the full Sunday backup and Monday, Tuesday, and Wednesday's incremental tapes.
    → 4 tapes.

Incremental Backup:

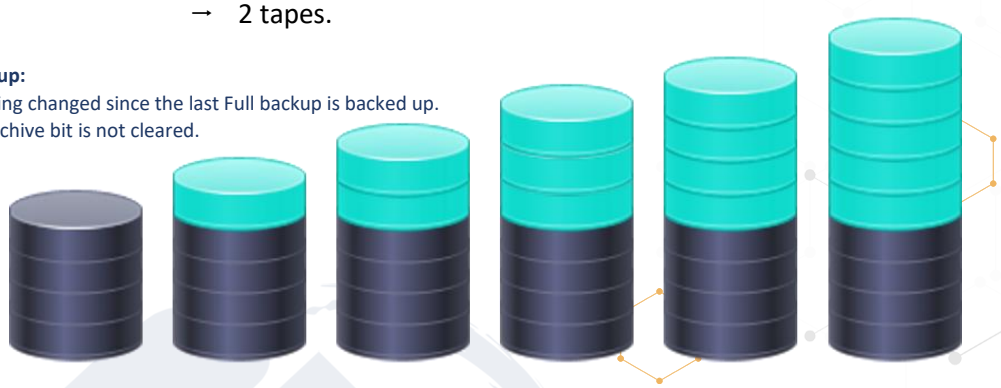
- Anything changed since the last backup is backed up.
- The archive bit is cleared.

- **Differential Backup:**
  - Backs up everything since the last Full backup.
  - Does not clear the archive bit.
  - Faster to restore since we just need 2 tapes for a full restore, the full and the differential.
  - Backups take longer than the incremental, we are backing everything since the last full.

- Never use both incremental and differential on the same data, it is fine on the same backup solution, different data has different needs.
- **IF we need to restore on Thursday:**
  - → Restore with the Sunday full backup and Wednesday's incremental tapes.
  - → 2 tapes.

Differential Backup:

- Anything changed since the last Full backup is backed up.
- The archive bit is not cleared.



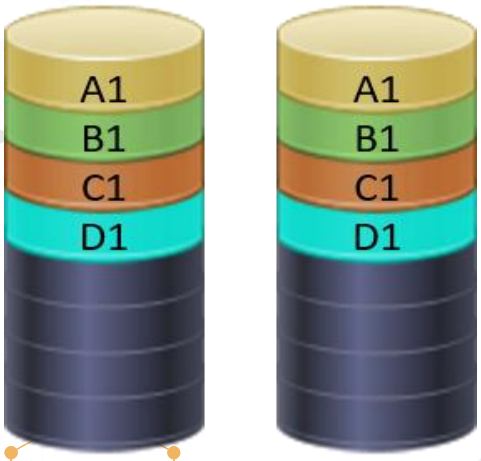
- **Copy Backup:**
  - This is a full backup with one important difference, it does not clear the archive bit.
  - Often used before we do system updates, patches, and similar upgrades.
  - We do not want to mess up the backup cycle, but we want to be able to revert to a previous good copy if something goes wrong.

- **Archive Bit:**
  - For Windows the NTFS has an archive bit on file, it is a flag that indicates if the file was changed since the last Full or Incremental backup.

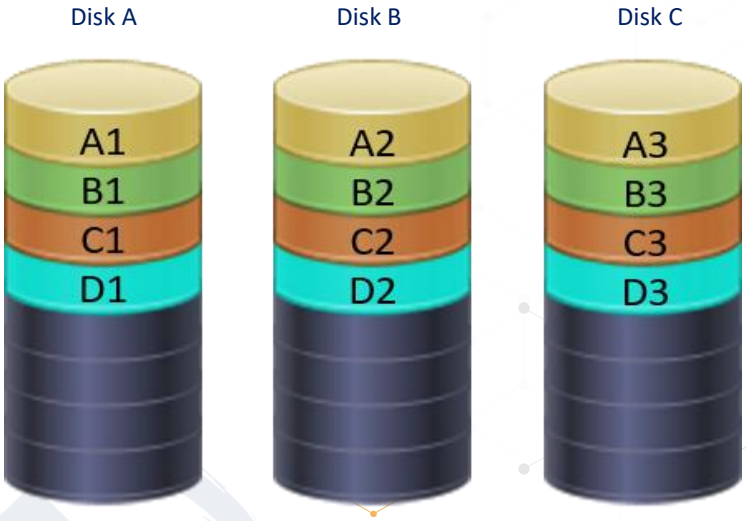
Fault Tolerance, Redundancy, and Resiliency:

- **RAID (Redundant Array of Independent/Inexpensive Disks):**
  - Comes in 2 basic forms, disk mirroring and disk striping.
    - **Disk Mirroring:**
      - Writing the same data across multiple hard disks, this is slower, the RAID controller has to write all data twice.
      - Uses at least 2 times as many disks for the same data storage, needs at least 2 disks.
    - **Disk Striping:**
      - Writing the data simultaneously across multiple disks providing higher write speed.
      - Uses at least 2 disks, and in itself does not provide redundancy.
      - We use parity with striping for the redundancy, often by XOR, if we use parity for redundancy, we need at least 3 disks.

Disk Mirroring:

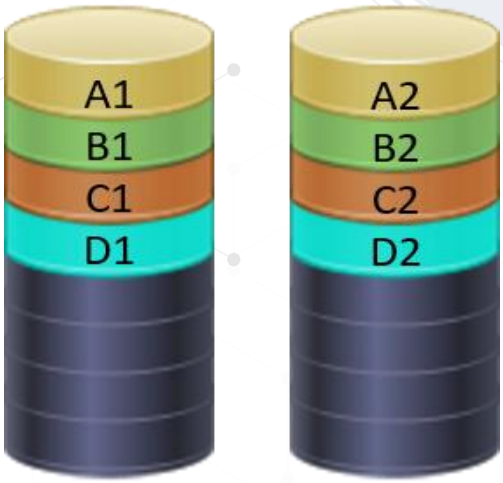


Disk Striping, no parity:

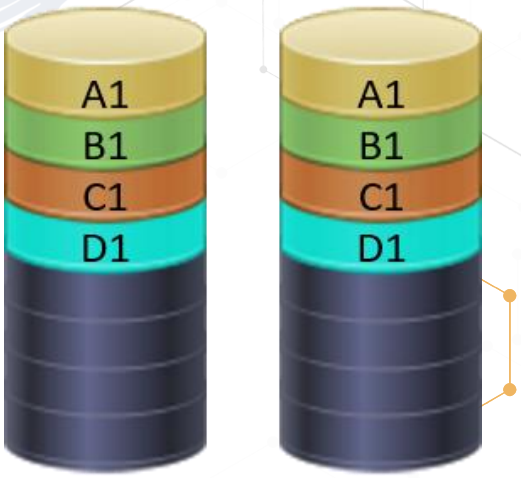


- There are many different types of RAID, for the exam I would know the above terms and how RAID 0, 1 and 5 works.
- **RAID 0:**
  - Striping with no mirroring or parity, no fault tolerance, only provides faster read write speed, requires at least 2 disks
- **RAID 1:**
  - Mirror set, 2 disks with identical data, and write function is written to both disks simultaneously.

RAID 0

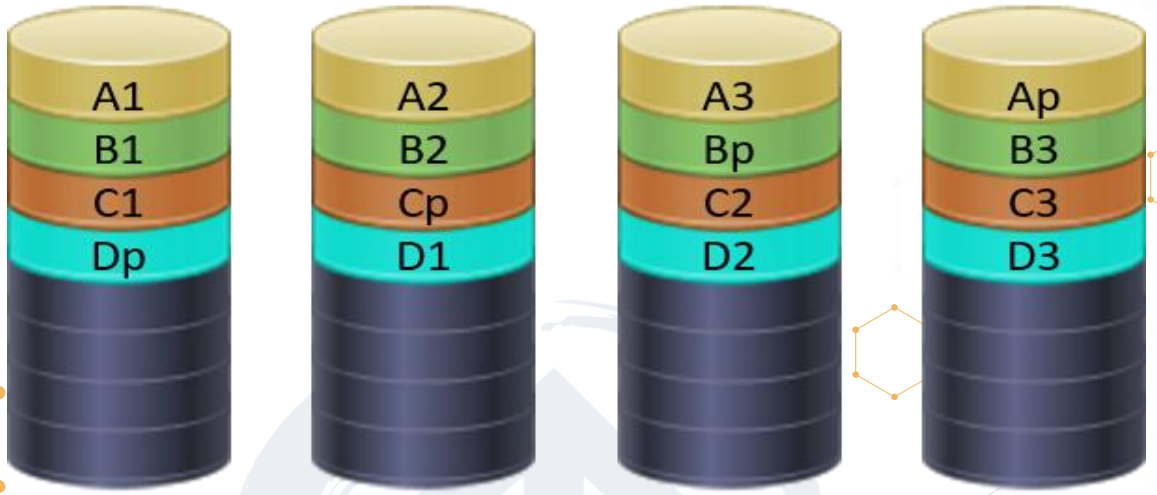


RAID 1



- **RAID 5:**
  - Block level striping with distributed parity, requires at least 3 disks.
  - Combined speed with redundancy.

RAID 5



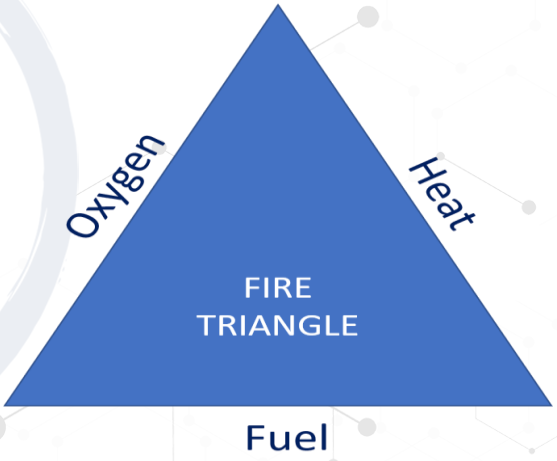
- RAID will help with data loss when we have a single disk failure if we use a fault tolerant RAID type, if more than one disk fails before the first is replaced and rebuilt, we will need to restore from our tapes.
- Most servers have the same disks with the same manufacturer date, they will hit their MTBF (Mean time between failures) around the same time.
- Larger data centers often have SLAs with the hard disk/server vendor, which also includes MTTR (Mean time to repair).
- This could be within 4 or 8 hours the vendor has to be onsite with a replacement disk.

- **System Redundancy:**
  - On top of the RAID and the backups we also try to provide system redundancy as well as redundant parts on the systems.
  - The most common system failures are from pieces with moving parts, this could be disks, fans, or PSU (power supplies).
  - Most servers have redundant power supplies, extra fans, redundant NIC's.
  - The NIC and PSU serve a dual purpose, both for internal redundancy and external. If a UPS fails, the server is still operational with just the 1 PSU getting power.
  - Redundant disk controllers are also reasonably common, we design and buy the system to match the redundancy we need for that application.
  - Often, we have spare hardware on hand in the event of a failure, this could include hard disks, PSU's, fans, memory, NICs.
  - Many systems are built for some hardware to be hot-swappable, most commonly HDD's, PSU's, and fans.

- If the application or system is important, we often also have multiple systems in a cluster.
- Multiple servers often with a virtual IP, seen as a single server to users.
- Clustering is designed for fault tolerance, often combined with load balancing, but not innately.
- Clustering can be active/active, this is load balancing, with 2 servers both servers would actively process traffic.
- In well-designed environments the servers are geographically dispersed.
- **Database Shadowing:**
  - Exact real time copy of the database or files to another location.
- **Electronic Vaulting (E-vaulting):**
  - Using a remote backup service, backups are sent off-site electronically at a certain interval or when files change.
- **Remote Journaling:**
  - Sends transaction log files to a remote location, not the files themselves.

Fire Suppression:

- **Fire Suppression** is done by removing one of the 3 requirements a fire has.
  - A fire needs Oxygen, Heat, and Fuel to burn.
  - Removing any of the 3 will put the fire out.
  - **Removing Oxygen** is done by replacing the oxygen in the room with something else or covering the fire, so the burning material doesn't have oxygen access (Halon, FM200, Argon).
  - **Removing Heat** is done by adding chemicals or water to the fire, cooling it down.
  - **Removing Fuel** is rarely done since the fuel is our equipment.



- **Fire Classes:**
  - Answer all questions from a **right point of view** and in a **top-down** security organization.

American	European	UK	Australian/Asian	Fuel/heat source
Class A	Class A	Class A	Class A	Ordinary combustibles
Class B	Class B	Class B	Class B	Flammable liquids
	Class C	Class C	Class C	Flammable gases
Class C	Unclassified	Unclassified	Class E	Electrical equipment
Class D	Class D	Class D	Class D	Combustible metals
Class K	Class F	Class F	Class F	Cooking oil or fat

- **Automatic Fire Suppression Systems:**
  - **Water:**
    - Removes the "heat" leg of the fire triangle by lowering the temperature.
    - Is the safest suppression agent, but for Data Centers:
    - Water + hardware = dead hardware.
    - Electricity could always be cut before water is used.
    - **Sprinkler Systems:**
      - Sprinklers have different types of bulbs for different temperatures.
      - Should be connected to alarm/warning sirens and lights.
      - Each sprinkler head is independent; it will trigger if the temperature for that bulb is met.

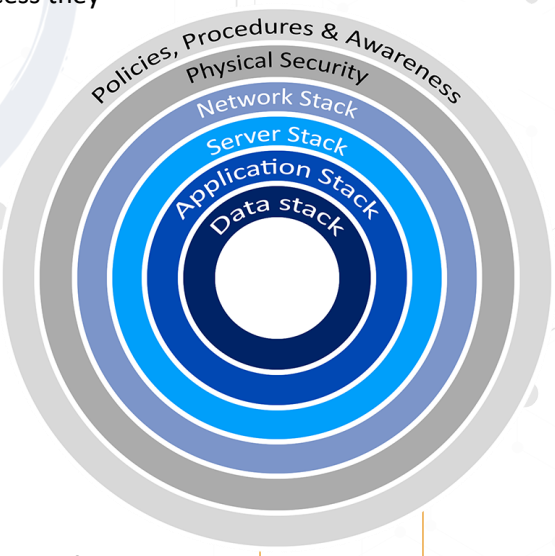
Temperature		Color of liquid alcohol inside bulb
°C	°F	
57	135	Orange
68	155	Red
79	174	Yellow
93	200	Green
141	286	Blue
182	360	Purple
227	440	Black
260	500	

- **Wet Pipe:** Sprinkler heads are closed. The pipes for the sprinkler system have water until the sprinkler.
- **Dry Pipe:** Sprinkler heads are closed.
- The pipe contains compressed air and a valve that stays shut as long as the air is present.

- **Fire Suppression:**
  - **Fire Extinguishers:**
    - A fire extinguisher is an active fire protection device used to extinguish or control small fires, often in emergency situations.
    - All portable fire extinguishers should be marked with the type of fire they are designed to extinguish.
    - Never use a fire extinguisher on a fire it was not intended for.
    - Use the **PASS** method to extinguish a fire with a portable fire extinguisher:
      - **P**ull the pin in the handle.
      - **A**im at the base of the fire.
      - **S**queeze the lever slowly.
      - **S**weep from side to side.

Secure Design Principles:

- **Least Privilege:**
  - We give employees the minimum necessary access they need, no more, no less.
- **Need to Know:**
  - Even if you have access, if you do not need to know, then you should not access the data (Kaiser employees).
- **Separation of Duties:**
  - More than one individual in one single task is an internal control intended to prevent fraud and error.
  - We do not allow the same person to enter the purchase order and issue the check.
  - For the exam assume the organization is large enough to use separation of duties, in smaller organizations where that is not practical, compensating controls should be in place.



- **Defense in Depth – Also called Layered Defense or Onion Defense:**
  - We implement multiple overlapping security controls to protect an asset.
  - This applies to physical, administrative, and logical controls.
- **Secure Defaults:**
  - A program or a system is as secure as possible when implemented.
  - We can then remove security for usability.
  - What is secure and usability is determined by risk analysis and usability tests.

- **Fail Securely:**
  - Systems are designed to prevents or mitigates unsafe consequences if the system fails.
  - If the system fails, it stays at least as secure as it was before the failure.
  - Open/safe vs. closed/secure.
- **Keep It Simple:**
  - Keeping our security simple, makes it better understood and accepted.
  - The more complex our security is the harder it is to control, troubleshoot, and manage.
- **Trust but Verify:**
  - Implicit trust but we verify you.
  - A majority of serious compromises are from privileged users (admins accounts).
- **Zero Trust (never trust, always verify) - NIST SP 800-207 - Zero Trust Architecture:**
  - We do by default not trust devices on our network, even if they have been verified.
  - We change our defenses from static, network-based perimeters to focus on users, assets, and resources.
  - With ZT there is no implicit trust given to assets or users based on their physical or logical location.
  - We use authentication and authorization of both subject and device that is done before a session to an enterprise resource can be established.
- **Privacy by Design:**
  - Proactive not reactive, Privacy as the default setting, Privacy embedded into design, Full functionality, End-to-end security, Visibility and transparency, Respect for user privacy
- **Shared Responsibility:**
  - With cloud computing the provider and customer share responsibility for the security.

➢ Domain 4: What we covered.

- **This is a GIANT domain.**

- Network Basics and Definitions.
- The OSI and TCP/IP model.
- IP Addresses, Port Numbers, and MAC Addresses.
- Wi-Fi and other wireless networks.
- Virtualization, Cloud, and Distributed Computing.
- Fault tolerance and resiliency.
- Data centers.
- Attacks and Attackers.

OSI model - Open Systems Interconnection Reference model