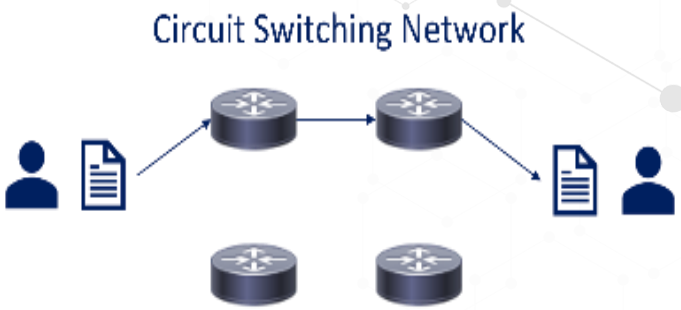
Welcome to the Fourth CBK Domain.

- **In this domain we cover:**
  - **Common network models**
  - **We cover how the internet/intranet works with:**
    - IP addresses: IPv4, IPv6, Private and Public Addresses.
    - Common well-known ports.
    - DNS, ARP, DHCP, NAT, PAT, and the other protocols we use to make our network function.
    - How we secure our communication on our local network and the internet.
    - Micro-segmentation, wireless, and cellular networks.
    - Common Attack types and how to mitigate them.
  - **Networking equipment and how we secure the different types.**
    - Routers, switches, firewalls, cables, …
  - **Network topologies and technologies.**
    - LAN, WAN, Ring, Star, Mesh.

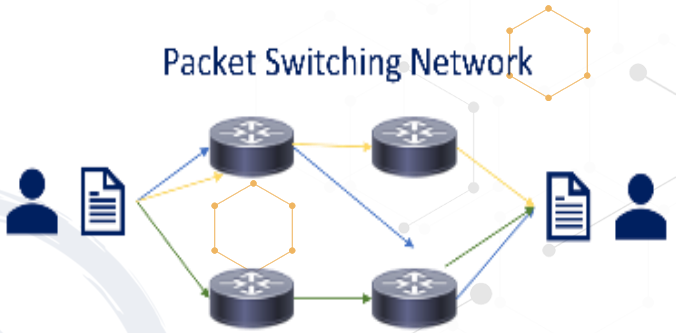
This chapter focuses on how our Network and Communications channels work and how to protect them. CBK 4 makes up 14% of the exam questions.

- **Network Basics and Definitions:**
  - **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.



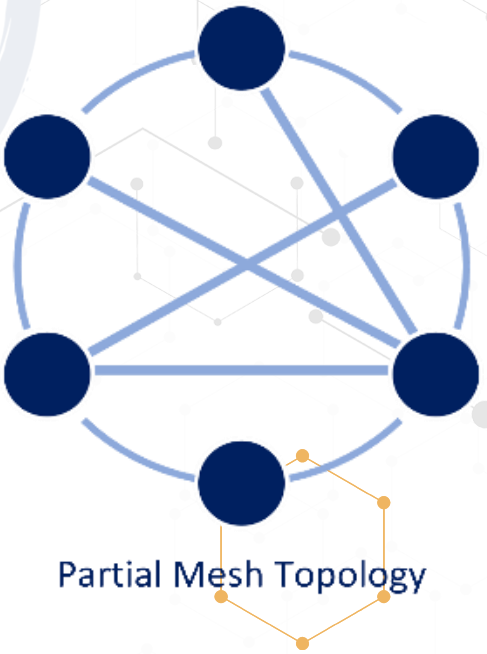
- **PAN (Personal Area Network)** - A personal area network is a computer network used for communication among computers and other information technological devices close to one person (PCs, printers, scanners, consoles …).
  - Can include wired (USB and FireWire) and wireless devices (Bluetooth and 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 airwaves.
- **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.

- **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.

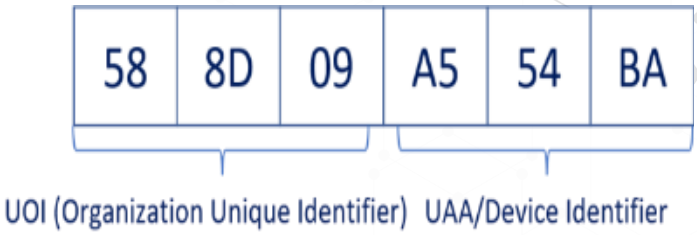
Definitions:

- **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).
  - The model is less used now and used as a reference point.
  - Know it for the exam, it is testable.

- **The OSI Model:**
  - **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.



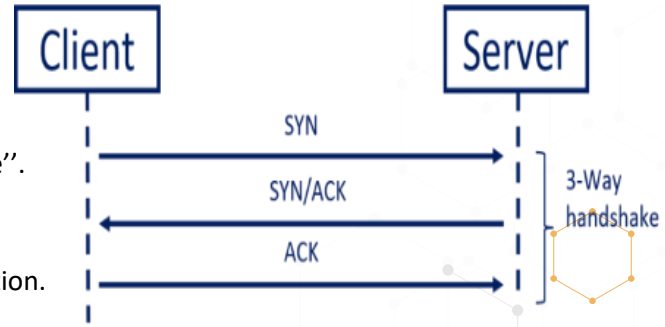
- **Layer 2 - Data Link Layer:**
  - Transports data between 2 nodes connected to same network.
  - LLC – Logical Link Control – error detection.
  - MAC address (BIA) – a unique identifier on the network card.



    - 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, …
  - If the exam asks which layer a protocol with "I" is and you do not remember answer layer 3.
    - IP, IGMP, IGRP, IPSEC, IKE, ISAKMP, … are all layer 3, all except IMAP which is layer 7.

- **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.



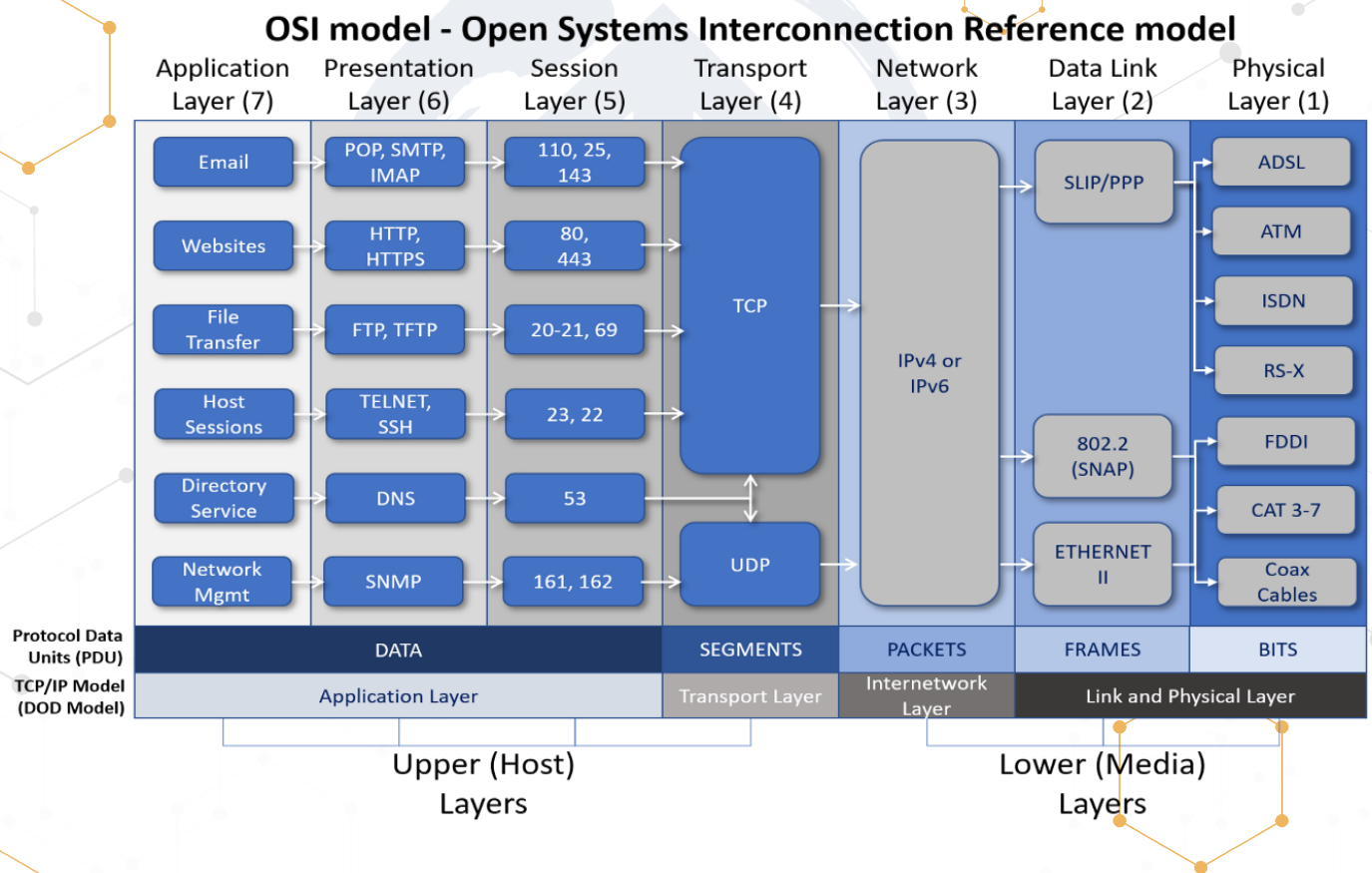
  - **TCP (Transmission Control Protocol):**
    - Reliable, Connection orientated, Guaranteed delivery, 3-way handshake, slower/more overhead, data reassembled.
    - **Attacks: SYN floods** – half open TCP sessions, client sends 1,000s of SYN requests, but never the ACK.
  - **TCP** Flags (9 bits 1-bit flags) (Control bits).
    - **NS**: ECN-nonce concealment protection.
    - **CWR (Congestion Window Reduced)** flag is set by the sending host to indicate that it received a TCP segment with the ECE flag set and had responded in congestion control mechanism.
    - **ECE**: ECN-Echo has a dual role, depending on the value of the SYN flag.
    - **URG** (1 bit): Indicates that the Urgent pointer field is significant.
    - **ACK** (1 bit): Indicates that the Acknowledgment field is significant.
    - **PSH** (1 bit): Push function. Asks to push the buffered data to the receiving application.
    - **RST** (1 bit): Resets the connection.
    - **SYN** (1 bit): Synchronize sequence numbers. Only the first packet sent from each end have this flag set.
    - **FIN** (1 bit): Last package from sender.

- **Layer 5 – Session Layer:**
  - Establishes connection between 2 applications: Setup > Maintenance > Tear Down.

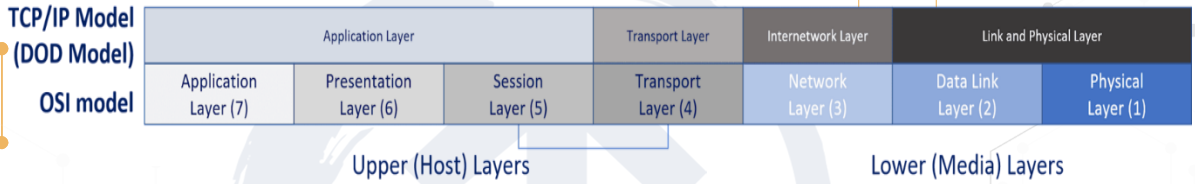
- **Layer 6 - Presentation Layer:**
  - Only layer with no protocols.
  - Formatting, compressing, encryption (file level).

- **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** (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** has 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).
    - The Internet Protocol performs two basic functions:
      - **Host addressing and identification:** This is done with a hierarchical IP addresses.

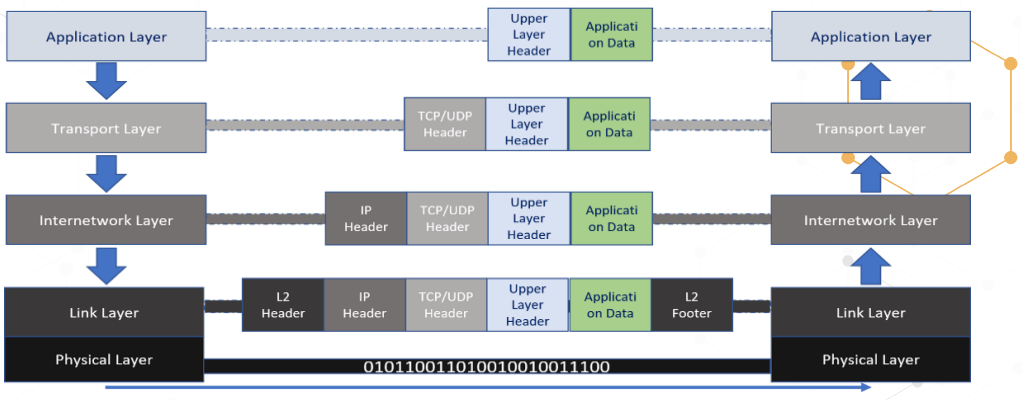
- **Packet routing:** Sending the packets of data (datagrams) from the source to the destination by forwarding them to the next network router closer to the final destination.

- Internet/Internetwork layer = OSI layer 3.

- **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.



- **MAC address (BIA):**
  - 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.

- **Protocols:**
  - **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).

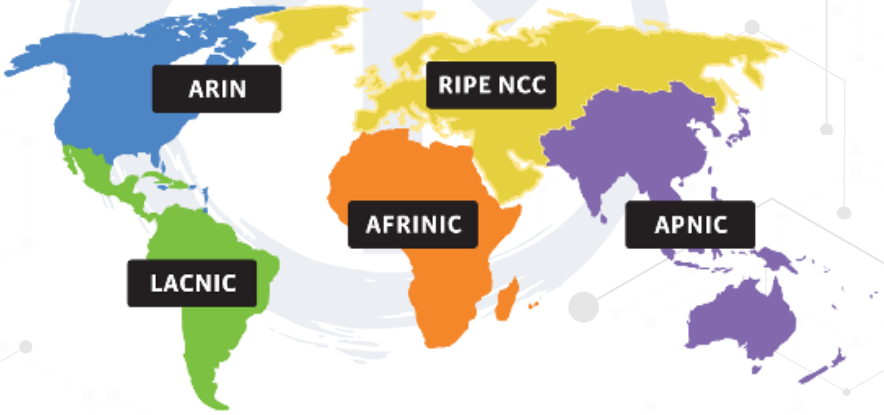
    - **Well-known Ports:**
      - 0-1023 - Mostly used for protocols.
    - **Registered Ports:**
      - 1024 to 49151 - Mostly used for vendor specific applications.
    - **Dynamic, Private or Ephemeral Ports:**
      - 49152–65535 - Can be used by anyone for anything.

- **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).
- **IP Addresses and Ports:**
  - **A Socket:**
    - 1 set of IP and Port.
    - UDP only uses 1 socket (connectionless), TCP uses 2 in a pair, 2 individual sockets making the pair.
  - **Socket Pairs (TCP):**
    - 2 sets of IP and Port (Source and Destination).
    - My Pair for the top one is:
      - Source pair:192.168.0.6:49691
      - Destination pair: 195.122.177.218:https
      - Well-known ports are often translated, port 443 is https.

Ports in use while browsing CISSP websites.

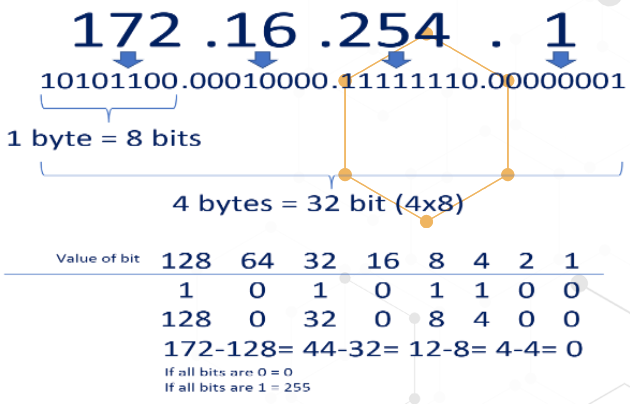
```
TCP    192.168.0.6:49691      195.122.177.218:https  ESTABLISHED
TCP    192.168.0.6:49814      157.55.56.154:40001    ESTABLISHED
TCP    192.168.0.6:49815      91.190.218.56:12350    ESTABLISHED
TCP    192.168.0.6:49995      195.122.177.218:https  ESTABLISHED
TCP    192.168.0.6:50490      vpn:https              ESTABLISHED
TCP    192.168.0.6:50674      ec2-52-4-144-94:https  ESTABLISHED
TCP    192.168.0.6:50678      ec2-54-242-92-62:5222  ESTABLISHED
TCP    192.168.0.6:50793      ec2-34-200-17-103:http  ESTABLISHED
TCP    192.168.0.6:51081      mail:https             ESTABLISHED
TCP    192.168.0.6:51082      mail:https             ESTABLISHED
TCP    192.168.0.6:51862      ec2-52-205-157-86:https  ESTABLISHED
TCP    192.168.0.6:52383      a2plcpnl0694:imaps     ESTABLISHED
TCP    192.168.0.6:52667      104.16.32.229:https    TIME_WAIT
TCP    192.168.0.6:52701      38.113.165.80:https    TIME_WAIT
TCP    192.168.0.6:52703      62.128.100.53:https    TIME_WAIT
TCP    192.168.0.6:52704      62.128.100.57:https    TIME_WAIT
```

- **IPv4/IPv6 Address Space Management:**
  - **IANA** (Internet Assigned Numbers Authority) governs the IP's address allocation.
  - **IANA** is a department of **ICANN** (Internet Corporation for Assigned Names and Numbers).
  - The world is divided into **RIR** (Regional Internet Registry) regions and organizations in those areas delegate the address space they have control over.
    - **AFRINIC** (African Network Information Center): Africa.
    - **ARIN** (American Registry for Internet Numbers): United States, Canada, several parts of the Caribbean region, and Antarctica.
    - **APNIC** (Asia-Pacific Network Information Centre): Asia, Australia, New Zealand, and neighboring countries.
    - **LACNIC** (Latin America and Caribbean Network Information Centre): Latin America and parts of the Caribbean region.
    - **RIPE NCC** (Réseaux IP Européens Network Coordination Centre) Europe, Russia, Middle East, and Central Asia.



- **IP Address and Traffic Types:**
  - **Unicast, Multicast, and Broadcast Traffic:**
    - **Unicast** - one-to-one traffic (Client to Server): The traffic is from a client to a host or reversed.
      - To capture all unicast traffic on a network, we use promiscuous mode on specific clients' network cards (Network IDSs/IPSs) and the switch port they are attached to has to be configured as a Span-port.
    - **Multicast** - one-to-many (predefined): The traffic is sent to everyone in a predefined list.
    - **Broadcast** - one-to-all (on a LAN network): The traffic is sent to everyone.
      - **Limited L3 Broadcast:** Uses the 255.255.255.255 broadcast IP address, routers do not pass (they drop it).
      - **Limited L2 broadcast:** Uses FF:FF:FF:FF:FF:FF broadcast MAC address, routers do not pass.
      - **Directed broadcast:** Sent to anyone logically connected to the same network.
        - A 192.168.19.12/24 will send to all hosts on that network, regardless if it is physically behind the same router or not. Accounting could have a VLAN spanning 3 separate remote buildings, the broadcast would be sent to them all.

- **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**.



- **IPv4:**
  - **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
  - As a band-aid solution to extend the depletion of IPv4 Addresses NAT and PAT were added:
  - **NAT (Network Address Translation):**
    - **Static NAT** Translates 1-1, we need 1 Public IP per Private IP we use, not practical and not sustainable.
    - **Pool NAT:** Also still 1-1, but a pool was available to all clients not assigned to specific clients.
  - **PAT (Port Address Translation):**
    - PAT was introduced to solve that issue, it uses IP AND Port number.
    - Also called One-to-Many or NAT Overload since it translates One public IP to Many private IPs.

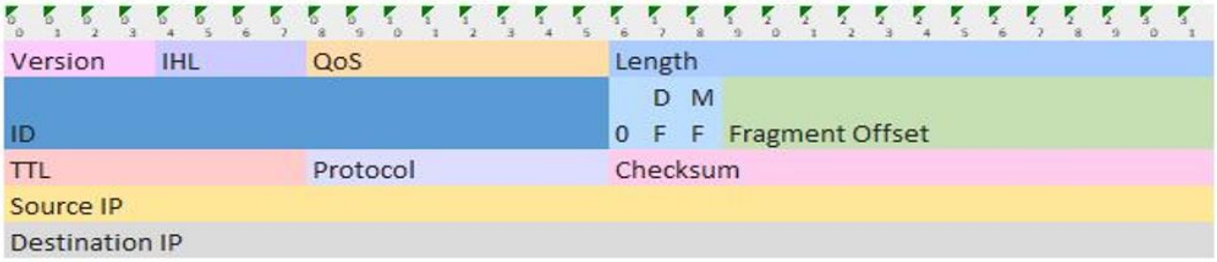
NAT TYPE	
Static	172.16.254.1 → 55.45.125.16
Pool	172.16.254.1 → 55.45.125.16 172.16.254.2 → 55.45.125.17 172.16.254.5 → 55.45.125.18 172.16.254.51 → 55.45.125.19
PAT	172.16.254.1 172.16.254.2 172.16.254.5 172.16.254.51 172.16.254.58 172.16.254.59 → 55.45.125.16

- **Classful IP Networks** were used early on the internet for public addresses. Networks were VERY large, some with 16 million+ IPs. Very inefficient use of IP addresses.
- **CIDR (Classless Inter-Domain Routing)** (also called slash notation):
  - We used CIDR to break our addresses into smaller logical segment, this saves addresses, we can make suitable sized IP ranges for our subnets and it is easier to add security to our subnets if they are logically segmented.
  - This would be the CIDR notation for our earlier IP address: 172.16.254.1/24.
  - This was done to the /24, indicates how many IPs are in that subnet, from that we know the broadcast and the range of host addresses.
  - Our /24 address would have 256 addresses, 255 are usable for hosts.
  - Earlier the first (0) and last (255) in a /24 could not be used, but now with newer technology and protocol use, only 255 is not usable since it is the broadcast address.

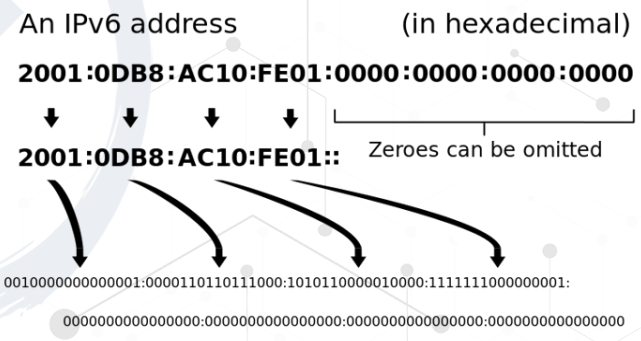
Address	Mask	How many
a.b.c.d / 32	255.255.255.255	1
a.b.c.d / 31	255.255.255.254	2
a.b.c.d / 30	255.255.255.252	4
a.b.c.d / 29	255.255.255.248	8
a.b.c.d / 28	255.255.255.240	16
a.b.c.d / 27	255.255.255.224	32
a.b.c.d / 26	255.255.255.192	64
a.b.c.d / 25	255.255.255.128	128
a.b.c.0 / 24	255.255.255.0	256
a.b.c.0 / 23	255.255.254.0	512
a.b.c.0 / 22	255.255.252.0	1,024
a.b.c.0 / 21	255.255.248.0	2,048
a.b.c.0 / 20	255.255.240.0	4,096
a.b.c.0 / 19	255.255.224.0	8,192
a.b.c.0 / 18	255.255.192.0	16,384
a.b.c.0 / 17	255.255.128.0	32,768
a.b.0.0 / 16	255.255.0.0	65,536
a.b.0.0 / 15	255.254.0.0	131,072
a.b.0.0 / 14	255.252.0.0	262,144
a.b.0.0 / 13	255.248.0.0	524,288
a.b.0.0 / 12	255.240.0.0	1,048,576
a.b.0.0 / 11	255.224.0.0	2,097,152
a.b.0.0 / 10	255.192.0.0	4,194,304
a.b.0.0 / 9	255.128.0.0	8,388,608
a.0.0.0 / 8	255.0.0.0	16,777,216
a.0.0.0 / 7	254.0.0.0	33,554,432
a.0.0.0 / 6	252.0.0.0	67,108,864
a.0.0.0 / 5	248.0.0.0	134,217,728
a.0.0.0 / 4	240.0.0.0	268,435,456
a.0.0.0 / 3	224.0.0.0	536,870,912
a.0.0.0 / 2	192.0.0.0	1,073,741,824
a.0.0.0 / 1	128.0.0.0	2,147,483,648
0.0.0.0 / 0	0.0.0.0	4,294,967,296

- **IP Headers contain:**
  - Version: IP version 4.
  - IHL: Length of the IP header.
  - QoS (Quality of Service).
  - Identification, Flags, Offset: used for IP fragmentation.
  - TTL (Time To Live): to prevent routing loops.
  - Protocol: Protocol number for TCP, UDP,...
  - Source and Destination IP addresses.
  - Optional: Options and padding.
  - MTU (Maximum Transmission Unit) - normally 1500 bytes in Ethernet usage.

- If a packet exceeds that size a router along the path may fragment into smaller packets.



- **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::
  - Our MAC address is **00:fa:22:52:88:8a**
  - It is a EUI-48 address we add "fffe" (for EUI-64) **00:fa:22:ff:fe:52:88:8a**
  - Set the U/L bit **20:fa:22:ff:fe:52:88:8a**
    - (The use of the universal/local bit in the Modified EUI-64 format identifier is to allow development of future

IPv6 address assigned on MAC Address

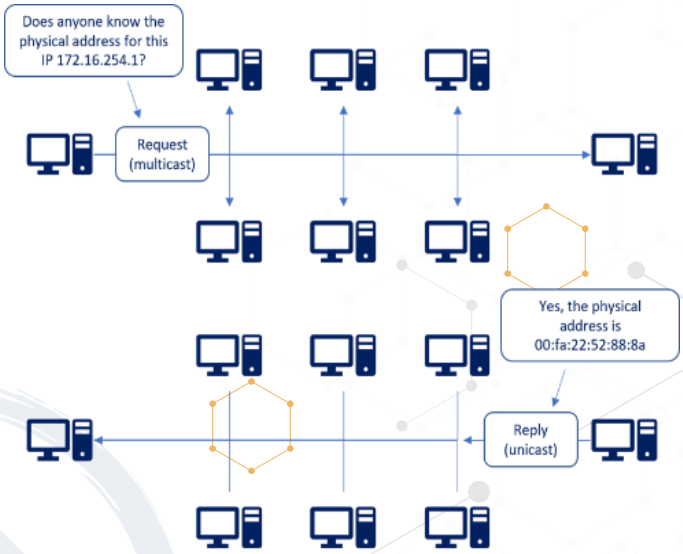
MAC Address		00	fa	22	52	88	8a	
Added "fffe" if 48bit	00	fa	22	ff	fe	52	88	8a
Set Universal/local bit	20	fa	22	ff	fe	52	88	8a
Add prefix and :	2001:0000:0000:00b8:20fa:22ff:fe52:888a							
Remove leading 0's	2001::b8:20fa:22ff:fe52:888a							
A link-local address is also assigned	fe80::b8:20fa:22ff:fe52:888a							

technology that can take advantage of interface identifiers with universal scope).

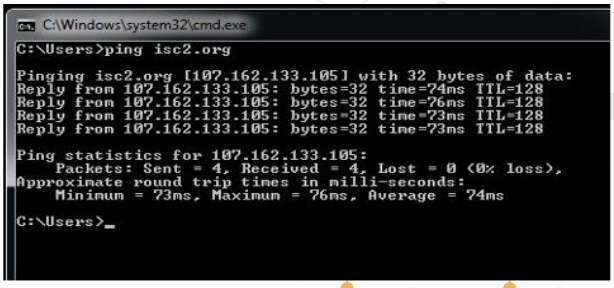
- Add our network prefix (2001:0000:0000:00b8) **2001:0000:0000:00b8:20fa:22ff:fe52:888a**
- Remove largest group of 0s **2001::b8:20fa:22ff:fe52:888a**
- Link Local address (only for local) **fe80::b8:20fa:22ff:fe52:888a**

- **IP Headers contain:**
  - Version: IP version 6 (4 bits)
  - Traffic Class/Priority (8bits).
  - Flow Label/QoS management (20 bits).
  - Payload length in bytes(16 bits).
  - Next Header (8 bits).
  - Time To Live (TTL)/Hop Limit (8 bits).
  - Source IP address (128 bits).
  - Destination IP address (128 bits).
  - MTU (Maximum Transmission Unit) - normally 1500 bytes in Ethernet usage.
    - If a packet exceeds that size a router along the path may fragment into smaller packets.

- **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.



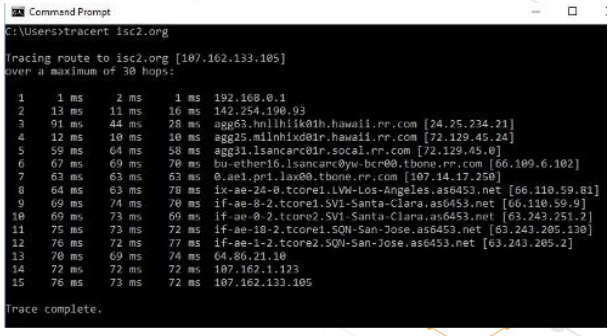
- **ICMP (Internet Control Message Protocol):**
  - Used to help IP, for Ping (Echo request/reply) and TTL Exceeds in Traceroute.
  - Often used for troubleshooting.
  - An ICMP Echo Request is sent to the IP, which then sends an ICMP reply back (or not).
  - Originally used (and still) to see if a host 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.
  - 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).

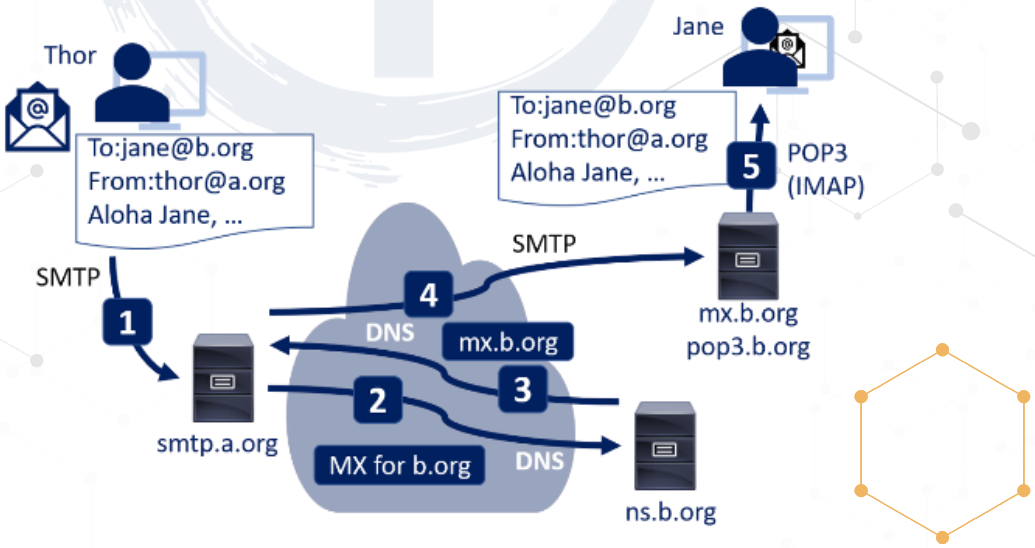


Traceroute to isc2.org (tracert on windows command line):
My local network > ISP > A few Hawaii hops > a few LA hops > 2x Santa Clara > 2x San Jose > Most likely ISC2 Firewall > and finally the actual webserver.

- **Telnet:**
  - Remote access over a network.
  - Uses TCP port 23, all data is plaintext including usernames and passwords, should not be used.
  - Attackers with network access can easily sniff credentials and alter data and take control of telnet sessions.
- **SSH (Secure Shell):**
  - Designed to replace or add security to unsecure protocols Telnet, FTP, HTTP,...
  - V1 had vulnerabilities long ago and v2 has as well recently.
  - Provides a 'secure' connection over an unsecured network (the internet).
  - The Snowden leak in 2013 showed the NSA can 'sometimes' decrypt SSL and get access to the data.
  - On July 6th 2017 WikiLeaks confirmed the CIA (ONLY this one time it is the Central Intelligence Agency) has developed a tool to crack the SSH protocol.
    - BothanSpy is an implant that targets the SSH client program Xshell on the Microsoft Windows platform.
    - Gyrfalcon is an implant that targets the OpenSSH client on Linux platforms centos, debian, rhel, suse, ubuntu.
- **FTP (File Transfer Protocol)** - Transfers files to and from servers:
  - No confidentiality or Integrity checks.
  - Should also not be used, since the vast majority of what we transport is over unsecure networks.
  - Uses TCP Port 21 for the control collection - commands are sent here.
  - Uses TCP Port 20 for the data collection - the actual data is sent here.
- **SFTP (SSH /Secure File Transfer Protocol)** - Uses SSH to add security to FTP.
- **FTPS (FTP Secure)** - Uses TLS and SSL to add security to FTP.

- **TFTP (Trivial FTP):**
  - Uses UDP Port 69.
  - No authentication or directory structure, files are written and read from one directory /tftpboot.
  - Used for "Bootstrapping" - Downloading an OS over the network for diskless workstations.
  - Used for saving router configuration.

- **Email Protocols:**
  1. The MUA (Mail User Agent) formats the message and using SMTP sends the message to the MSA (Mail Submission Agent).
  2. The MSA determines the destination address provided in the SMTP protocol, in this case jane@b.org. The MSA resolves the fully qualified domain name of the mail server in the DNS.
  3. The DNS server for the domain b.org (ns.b.org) responds with any MX (Mail eXchange) records listing for that domain, in this case mx.b.org, an MTA (Message Transfer Agent) server run by the recipient's ISP.
  4. smtp.a.org sends the message to mx.b.org using SMTP. This server may need to forward the message to other MTAs before the message reaches the final MDA.
  5. The MDA delivers it to the mailbox of user Jane.
  6. Jane's MUA picks up the message using either the Post Office Protocol (POP3) or the Internet Message Access Protocol (IMAP).



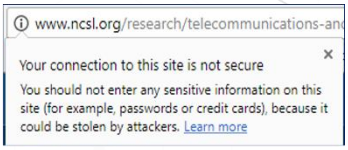
- **DNS (Domain Name System):**
  - Translates server names into IP Addresses, uses TCP and UDP Port 53
  - Google.com can get translated into 66.102.12.231 or 2607:f8b0:4007:80b::200e depending on requester's IP.
  - Uses gethostbyname() and gethostbyaddress()
  - **Authoritative name servers** - The authority for a given name space.
  - **Recursive name server** - Tries to resolve names it does not already know.
  - **Cache name server** - Keeps previously resolved names in a temporary cache.
  - DNS uses UDP for most requests and natively has no authentication. .
  - **DNS Poisoning** is similar to ARP poisoning, an attacker sends a fake address/name combo to another DNS server when asked and the server keeps it in its DNS records until it expires.

- **DNSSEC (DNS Security Extensions):**
  - Provides Authentication and Integrity using PKI Encryption.
  - Does **not** provide Confidentiality - Think of it a digital signature for DNS.

- **SNMP (Simple Network Management Protocol):**
  - Mostly used to monitor devices on our network (routers, switches, servers, HVAC, UPS ...).
  - An SNMP client agent is enabled or installed on the client.
  - The device can report port up/down, traffic utilization, temperature, memory use, HDD allocation,...
  - **SNMPv1** and SNMPv2 sends data in cleartext.
  - **SNMPv2** is still widely used, but should be avoided.
    - An attacker on the network can sniff the traffic, often the default community strings are used "public and "private".
    - If an attacker gains access to the private (write) string they can re-configure the device, shut it or interfaces down,...
  - **SNMPv3** uses encryption to provide CIA (Confidentiality, Integrity, and Availability).
    - This should be the standard across any organization.

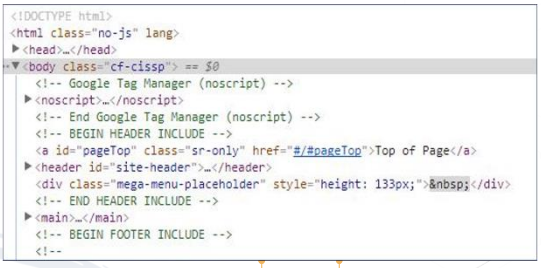
- **HTTP** and **HTTPS** - Transport HTML data.
  - **HTTP (Hypertext Transfer Protocol):**
    - Uses TCP port 80 (8008 and 8080), unencrypted website data sent across the internet.

HTTPS: Connection (notice the Secure)



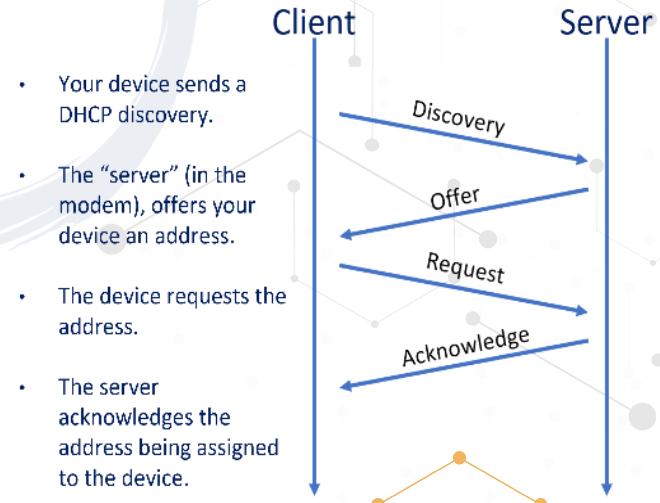
HTTP: Connection.

- **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.



HTML: The basic building block of webpages.

- **BOOTP (Bootstrap Protocol):**
  - Used for diskless workstations, used to determines OS (Downloaded with tftp) and IP Address.
  - Most system BIOSs support BOOTP, they can then load the OS without a disk.
- **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.



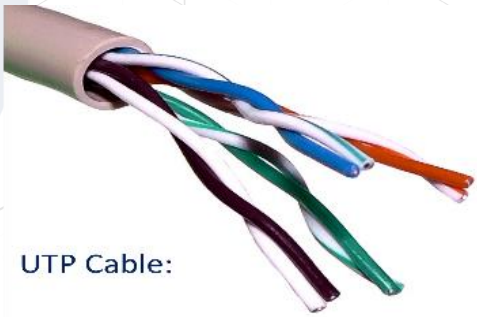
- Your device sends a DHCP discovery.
- The "server" (in the modem), offers your device an address.
- The device requests the address.
- The server acknowledges the address being assigned to the device.

- **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.

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

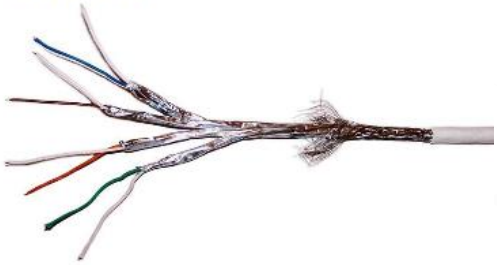
    - **Crosstalk** is the signal crossing from one cable to another, this can be a confidentiality issue.
    - **Attenuation** is the signal getting weaker the farther it travels.
      - Copper lines have attenuation, with DSL the farther you are from the DSLAM (Digital Subscriber Line Access Multiplexer) the lower speed you get.

  - **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.

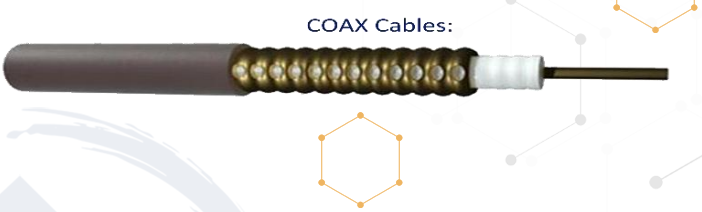


UTP Cable:

STP Cable:

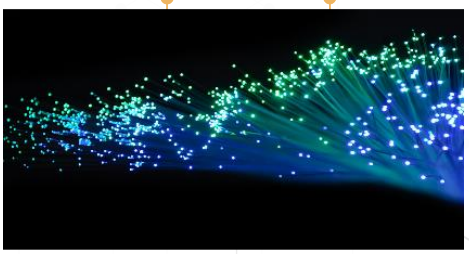


- **Coax (Coaxial) Cables:**
  - Most commonly used for cable TV and Internet services.
  - Coax Cables have built in layers:
    - **Copper core** in the middle.
    - A **plastic insulator** around the middle core.
    - A **copper braid/shield** around the insulator.
    - A **plastic outer layer**.
  - The braid/shield makes it less susceptible to EMI and the thicker core can provide higher speeds.



- **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 Technologies and Protocols:

- 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.
- **Fiber-optic** is commonly used between switches to servers and for backbone data transfers; rarely used for desktops.
- **Ethernet** is baseband and uses copper TP, coax, and fiber cables.
    - Ethernet was also not built for how we use networks today, so we bolt on functionality we want
- **Wireless** technologies are often built into Smartphones, tablets, and laptops.
    - In a wireless LAN, users can move unrestricted in the coverage area, the transfer from one wireless access point to another is often completely seamless.

- **CSMA (Carrier Sense Multiple Access):**
    - Clients on a network check to see if the shared line is in use, if not they will send their data.
    - Clients listen to see if the line is idle: If idle, they send; if in use, they wait a random amount of time (milliseconds).
- **CSMA/CD (CSMA/Collision Detection):**
    - Used for systems that can send and receive at the same time like Ethernet.
    - If 2 clients listen at the same time and see the line is clear they can both transmit at the same time causing collisions, CD is added to help with that scenario.
    - Clients listen to see if the line is idle: If idle, they send; if in use, they wait a random amount of time (milliseconds).
        - While transmitting, they monitor the network.
        - If more input is received than sent, another workstation is also transmitting.
            - They send a Jam signal to tell the other nodes to stop sending.
            - Wait for a random amount of time before starting to retransmit.
- **CSMA CA (CSMA/Collision Avoidance):**
    - Used for systems that can either send or receive like wireless.
    - They check if the line is idle: If idle, they send; if in use, they wait a random amount of time (milliseconds).
        - Slightly different than CD, on Ethernet networks clients are normally aware of other clients, on wireless that is not always the case.

- If a lot of congestion, the client can send a RTS (Request To Send), and if the host (the wireless access point) replies with a CTS (Clear To Send), similar to a token, the client will transmit.
- This goes some way to alleviating the problem of hidden nodes, in a wireless network, the Access Point only issues a Clear to Send to one node at a time.

Legacy Lan Systems:

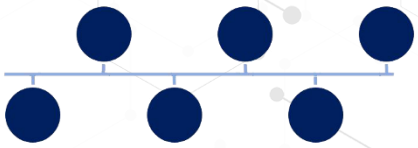
- **ARCNET (Attached Resource Computer Network):**
  - Used network tokens for traffic, no collisions.
  - Used a Star topology.
  - 2.5Mbps.

- **Token Ring:**
  - Used network tokens for traffic, no collisions.
  - Used a Ring topology.
  - 16Mbps.

- **FDDI (Fiber Distributed Data Interface):**
  - Used token-bus for traffic, no collisions.
  - Used a Ring topology.
  - Used fiber and not copper so not susceptible to EMI.
  - 100Mbps.

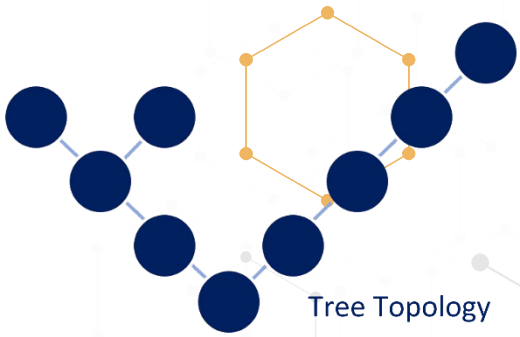
Physical LAN Topologies:

- **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.



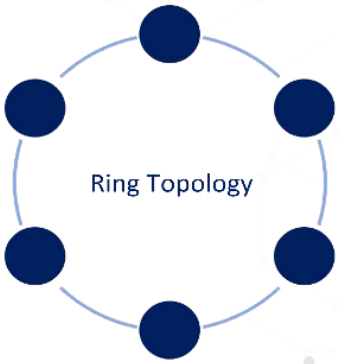
Bus Topology

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

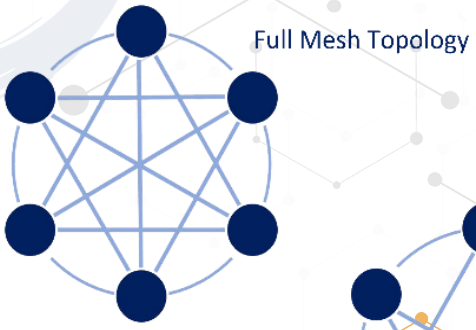


Tree Topology

- **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.

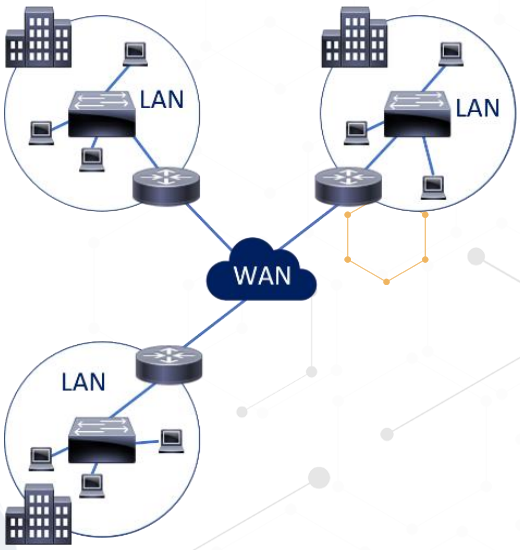


- **Mesh**:
  - Nodes are connected to each other in either a partial mesh or a full mesh.
  - **Partial Mesh**:
    - Nodes are directly connected to some other nodes.
  - **Full Mesh**:
    - All nodes are directly connected to all other nodes.
    - More redundant but requires a lot more cables and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

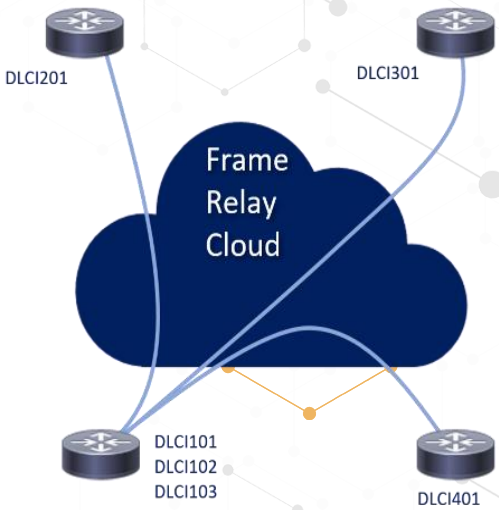


WAN (Wide Area Network) Technologies and Protocols:

- The internet is built of 1000s of WAN ISPs (Internet Service Providers) and Long-Haul providers.
- **Legacy Connections:**
  - Some are still in use today, but they are getting more rare, early on high-speed internet connections were mostly used by business.
  - For the exam, know the basics about them but no more.



- **T1** (US): Dedicated 1.544 Mbps circuit carrying 24 64-bit DS0 (Digital Circuit) Channels, this was done with 24 circuit-switched phone channels. Often also called DS1.
- **T3** (US): 28 bundled T1 lines, creating a dedicated 44.736 Mbps circuit.
- **E1** (Europe): Dedicated 2.048 circuit carrying 30 channels.
- **E3** (Europe): 16 bundled E1 lines, creating a dedicated 34.368 Mbps circuit.
  - **Frame Relay:**
    - Packet-Switching L2 protocol, it has no error recovery and only focuses on speed. Higher level protocols can provide that if needed.
    - **PVC (Permanent Virtual Circuit):**
      - Always up, ready to transmit data.
      - Form logical end-to-end links mapped over a physical network.
    - **SVC (Switched Virtual Circuit):**
      - Calls up when it needs to transmit data and closes the call when it is done.
    - Uses **DLCI** (Data Link Connection Identifiers) to identify the virtual connection, this way the receiving end knows which connection an information frame belongs to.

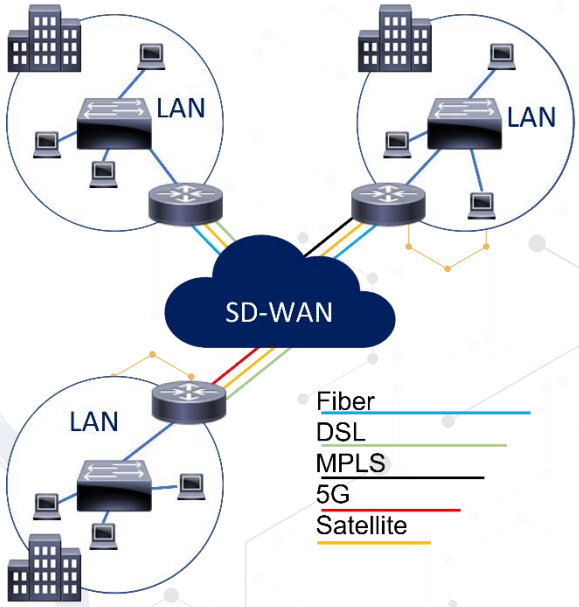


- **X.25:**
  - Used to be a standard protocol suite for packet switched WAN communication.
  - An X.25 WAN consists of Packet-Switching Exchange (PSE) nodes as the networking hardware and leased lines, plain old telephone service connections, or ISDN connections as physical links.
  - Uses error correction which can add latency.
- **SONET** (Synchronous Optical Networking):
  - Carries multiple T circuits over fiber optics.
  - Uses a physical ring topology.

- **MPLS (Multiprotocol Label Switching):**
  - Directs data from one node to the next based on short path labels and not IP addresses.
  - The labels identify virtual links/paths between distant nodes and not the endpoint.
  - Encapsulate packets for other protocols/technologies (T1/E1, ATM, Frame Relay, and DSL).
  - Packet-forwarding decisions are made only on the contents of this label and not by examining the packet.
  - With this, MPLS can create end-to-end circuits across any type of transport medium using any protocol.

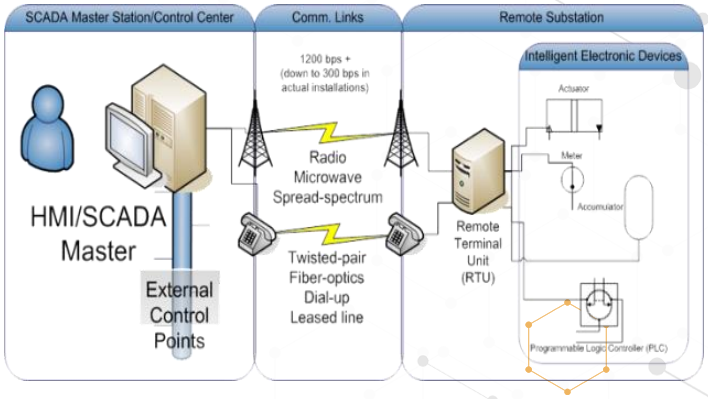
  - MPLS operates at a layer that is considered between the OSI models Data link layer (L2) and Network layer (L3), often referred to as a layer 2.5 protocol.
  - Often used to connect geographically distant locations of an organization with MPLS VPN connections.

- **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.



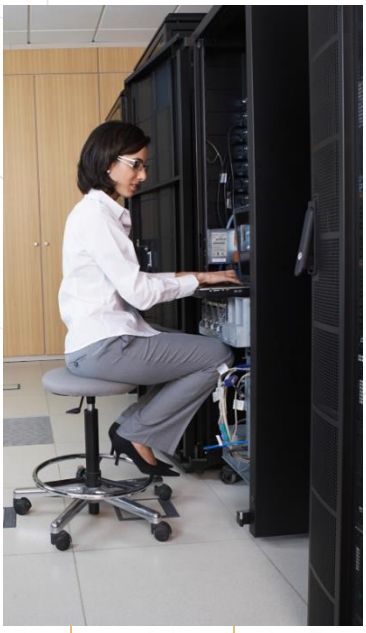
- **SDLC (Synchronous Data Link Control):**
  - A synchronous L2 WAN protocol that uses polling to transmit data.
  - Polling is similar to token passing but with the primary node polls and secondary nodes, allowing them to transmit data when polled.
  - Combined nodes can act as primary or secondary but using NRM transmission only.
- **HDLC (High-Level Data Link Control):**
  - The successor to SDLC.
  - Adds error correction and flow control and two additional modes (ARM/ABM).
- **The three modes of HDLC and the one of SDLC are:**
  - **NRM** (Normal Response Mode): Secondary nodes transmit when given permission by the primary only.
  - **ARM** (Asynchronous Response Mode): Secondary nodes may initiate communication with the primary node.
  - **ABM** (Asynchronous Balanced Mode): When nodes act as primary or secondary, initiating transmissions without receiving permission. This is most commonly used mode.

- **DNP3 (Distributed Network Protocol):**
  - We already covered this in the last domain, but it being a network protocol, here it is again.
  - A set of communications protocols used between components in process automation systems.
  - Mainly used in utilities such as electric and water companies.

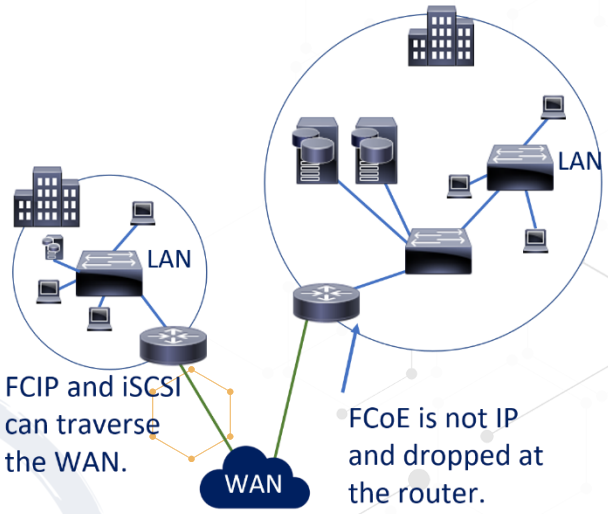


  - It plays a crucial role in SCADA systems.
  - Used by SCADA for communication between a Master Station (Control Centers) and Remote Terminal Units (RTUs), and/or Intelligent Electronic Devices (IEDs).

- **Storage Protocols:**
  - **SAN (Storage Area Network)** protocols provide a cost-effective way that uses existing network infrastructure technologies and protocols to connect servers to storage.
  - A SAN allows block-level file access across a network, it acts like an attached hard drive.
  - **FCoE (Fiber Channel over Ethernet):**
    - The fiber Channel's HBA (Host Bus Adapters) are unique cards to interface with storage; can be combined with the network interface (NIC) for economies of scale.
    - FCoE uses Ethernet, not TCP/IP, and because of that it is not routable.
  - **FCIP (Fiber Channel over IP):** Encapsulates fiber channel frames via TCP/IP.
  - **VSAN (Virtual Storage Area Network):**
    - A collection of ports from a set of connected fiber channel switches that form a virtual fabric.
    - Ports within a single switch can be partitioned into multiple VSANs; despite sharing hardware and multiple switches, can join a number of ports to form a single VSAN.

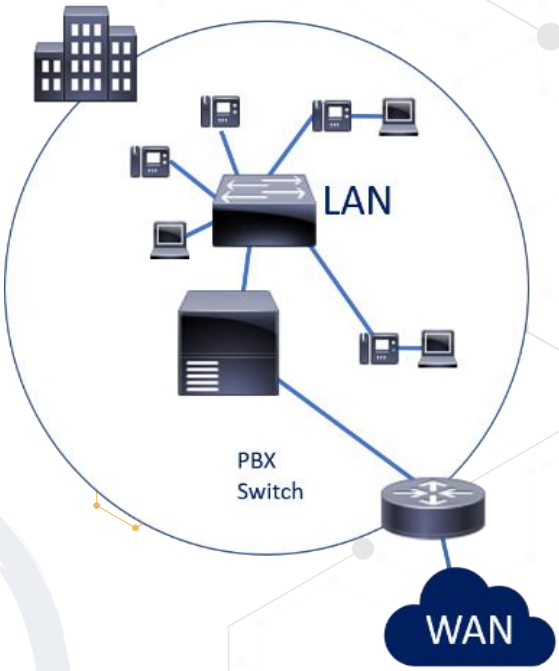


- **Storage Protocols**
  - **iSCSI (Internet Small Computer System Interface):**
    - Leverages existing networking infrastructure and protocols to interface with storage.
    - Uses the higher layers of the TCP/IP model for communication and can be routed like any IP protocol (so can FCIP).
    - Can be used for storage across a WAN.
    - Uses LUNs (Logical Unit Numbers) to provide for addressing storage across the network.
    - LUNs can also be used for basic access control for network accessible storage.



- **VoIP (Voice over Internet Protocol):**
  - A group of technologies for the delivery of voice communications and multimedia sessions over IP networks.
  - The digital information is packetized and transmitted using UDP IP packets over a packet-switched network.
  - They transport audio streams using special media delivery protocols that encode audio and video with audio codecs and video codecs.
  - VoIP is commonly used on VoIP phones, smartphones, PCs, and on Internet access devices; calls and text messages can be sent over 3G, 4G or Wi-Fi.
  - The security concerns of VoIP telephone systems are similar to those of any Internet-connected device.
  - Hackers who know about VoIP vulnerabilities can deploy denial-of-service attacks, harvest customer data, record conversations, and compromise voicemail messages.
  - The quality of internet connection determines the quality of the calls; where data traffic is more forgiving, VoIP is UDP and needs real time error free connections.

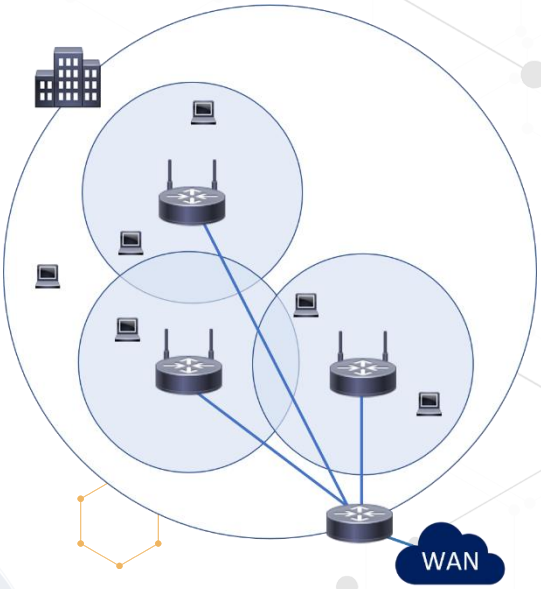
- Where regular phones may work, VoIP phone service will not work if there is a power outage or when the internet connection is down.
- We use many different VoIP protocols: SIP (Session Initiation Protocol), H.323, MGCP (Media Gateway Control Protocol), Gateway Control Protocol, RTP (Real-time Transport Protocol), RTCP (Real-time Transport Control Protocol),...



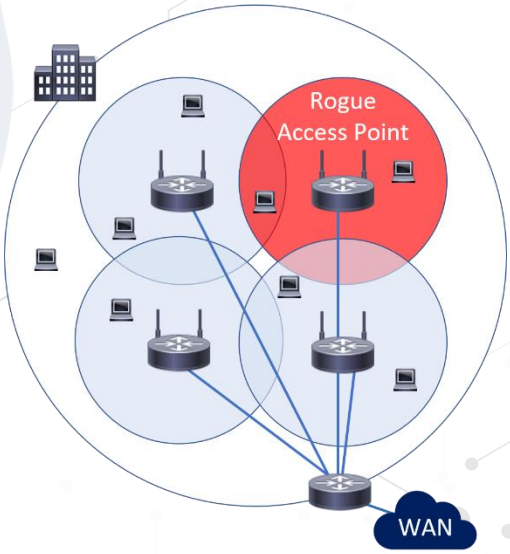
- **SDN (Software-Defined Networking):**
  - Allows network administrators via software to initialize, control, change, and manage network behavior dynamically.
  - Addresses the static architecture of traditional networks that doesn't support the dynamic, scalable computing and storage needs of more 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.

- **Virtual eXtensible LAN (VXLAN):**
  - It is an encapsulation protocol that allows VLANs to span subnets and physically distant locations.
  - VXLAN can support up to 16 million virtual networks, whereas VLAN is limited to 4,096.
  - To implement micro-segmentation without restricting segments to only local entities.
- **Software-defined Wide Area Network (SD-WAN):**
  - Derived from SDN, used to connect distant data centers, locations, and cloud services over WAN links.
- **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.

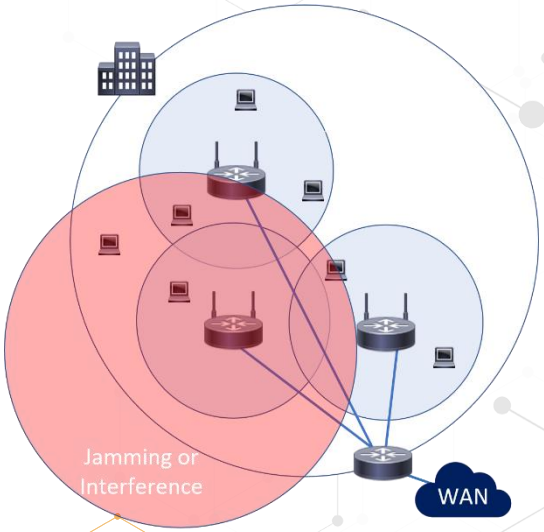
- A wireless computer network that links two or more devices using a wireless distribution method within a limited area (a home, a school, a coffee shop, or an office building).
- Gives users the ability to move around within a locally covered area and be connected to the network.
- Often multiple APs (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.



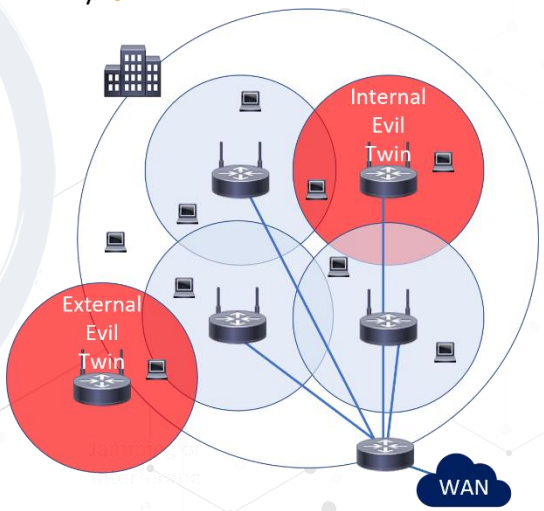
- **Wi-Fi Attacks:**
  - **Rogue Access Points:**
    - An unauthorized access point that has been added to our network without our knowledge.
    - This can be malicious by an attacker or just an employee wanting Wi-Fi somewhere with bad coverage.
    - Without our security posture, they are a very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



- **Wi-Fi Attacks:**
  - **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.



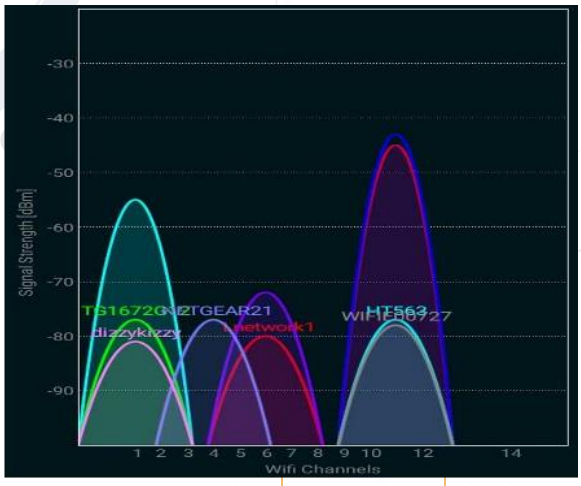
  - **Evil Twin:**
    - An evil twin is used when attackers are trying to create rogue access points so as to gain access to the network or access to information that is being put through a network.
    - Can be done on your network or not, the attacker simply names their access point the same as ours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



- **802.11 Standards:**
  - The 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing WLAN computer communication in the 2.4, 3.7, 5, and 6 GHz frequency bands.
  - There are more 802.11 protocols but for the exam know these.
  - The 2.4 GHz frequency can be very crowded; wireless, Bluetooth, microwaves, cordless phones, and baby monitors,... use that frequency.
  - The 5 GHz frequency is normally less crowded and has less interference than 2.4 GHz.
  - Now with the 6 GHz being available, one of it's largest selling points is a completely non-crowded frequency.
  - 5 and 6 GHz is a higher frequency with shorter waves, it does not penetrate walls, Floors, and other obstructions, as well as the longer 2.4 GHz waves.
  - It is easy to change the channel your Wi-Fi to a less crowded one.
  - Some access points management software can dynamically change the channels on individual access points to find better channels and provide less overlap.

802.11 network PHY standards

802.11 protocol	Release date:	Frequency (GHz)	Bandwidth (MHz)	Stream Data Rate (Mbit/s)	Approximate Range (Indoors):	Approximate Range (Outdoors):
802.11-1997	6/1/1997	2.4	22	1, 2	20 m (66 ft)	100 m (330 ft)
a	9/1/1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	35 m (115 ft)	120 m (390 ft)
		3.7				5,000 m (16,000 ft)
b	9/1/1999	2.4	22	1, 2, 5.5, 11	35 m (115 ft)	140 m (460 ft)
g	6/1/2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	38 m (125 ft)	140 m (460 ft)
n	10/1/2009	2.4 and 5	20	Up to 72.2	70 m (230 ft)	250 m (820 ft)
			40	Up to 150		
ac	12/1/2013	5	20	Up to 346.8	35 m (115 ft)	
			40	Up to 800		
			80	Up to 1733.2		
			160	Up to 3466.8		
ax	2/9/2021	2.4, 5, 6	80+80	Up to 9608	30 m (98 ft)	120 m (390 ft)



Wireless access points seen with a wireless sniffer, even if you hide the SSID they can easily be found.

- **802.11 Wireless NICs:**
  - **Operate in four different modes:**
    - **Managed/Client mode:**
      - A wireless access point is required.
      - Clients connect to an access point in managed mode; once connected, clients communicate with the access point only, they can't directly communicate with other clients.
    - **Infrastructure mode:**
      - A wireless access point is required.
      - Client must use the same SSID (service set identifier) as the access point and if encryption is enabled, they must share the same keys or other authentication parameters.
    - **Ad-hoc mode** network:
      - The WNIC does not require an access point but can interface with all other wireless nodes directly.
      - All the nodes in an ad hoc network must have the same channel and SSID.
      - A computer connected to the Internet via a wired NIC may advertise an ad-hoc WLAN to allow internet sharing.
    - **Monitor mode** or **RFMON (Radio Frequency Monitor) mode**:
      - Enables a computer with a WNIC to monitor all traffic received from the wireless network.
      - Unlike promiscuous mode, which is also used for packet sniffing, monitor mode allows packets to be captured without having to associate with an access point or ad hoc network first.

- **SS (Service Set)** is a set consisting of all the devices associated with an organization's WLAN (Wireless Local Area Network).
- **SSID (Service Set Identifier)** is the name of the wireless access point you see when you connect.
    - Clients must know the SSID before joining that WLAN.
    - The SSID is a configuration parameter.
    - SSIDs are normally broadcasted, but we can disable the broadcast in the access point configuration.
    - It is a security measure we want to use, but it is easy to bypass.
    - We can also use MAC address filtering on our wireless access points, this is another limited security feature.
    - MAC addresses are sent in plaintext on 802.11 WLANs, it is easy to sniff and spoof.

- **WEP (Wired Equivalent Privacy)** protocol, early 802.11 wireless security (1997).
    - No longer secure, should not be used.
    - Attackers can break any WEP key in a few minutes.
    - It was designed to not conflict with the Wassenaar Arrangement's 40bit limit on encryption and because of that, it was designed weaker than it should have been.
    - Many access points still have the WEP option today, but most are preconfigured with WPA2/PSK or WPA3/SAE3.
    - WEP uses 10 or 26 hexadecimal digits (40 or 104 bits).
    - It was used widely years back and was often the first security choice presented to users by router configuration tools.
    - WEP frames do not use timestamp and have no replay protection, attackers can inject traffic by replaying previously sniffed WEP frames.

- **WPA (Wi-Fi Protected Access)** (2003):
  - Interim standard to address WEP issues, should not be used.
  - Uses RC4 and TKIP (Temporal Key Integrity Protocol).
    - Neither are considered secure anymore.
    - TKIP uses a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and preventing the types of attacks that compromised WEP.
  - WPA has been designed specifically to work with wireless hardware produced prior to the introduction of the WPA protocol.

- **WPA2 (Wi-Fi Protected Access II)**, also called RSN (Robust Security Network) (2004):
  - Most commonly used but a slow move towards WPA3; the most secure form of WPA2 is WPA2-PSK (Pre-Shared Key) using AES.
  - AES provides confidentiality and CCMP (Counter Mode CBC MAC Protocol), a Message Integrity Check (MIC), which provides integrity. It can be configured to use older less secure protocols (TKIP).

- **WPA3 (Wi-Fi Protected Access III)** (2020)
  - Current standard but transition from WPA2 is slow.
  - 192-bit key strength and WPA3 replaces the pre-shared key (PSK) exchange with Simultaneous Authentication of Equals (SAE) exchange, uses AES-256 in GCM mode with SHA-384 as HMAC.

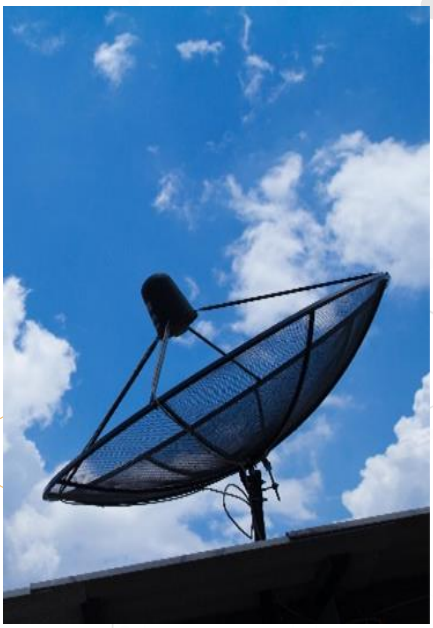
- **Bluetooth:**
  - A wireless technology standard for exchanging data over short distances using 2.4 GHz from fixed and mobile devices and building personal area networks (PANs).
  - Bluetooth has three classes of devices; while designed for short-distance networking, Class 1 can reach up to 100 meters.
  - 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.



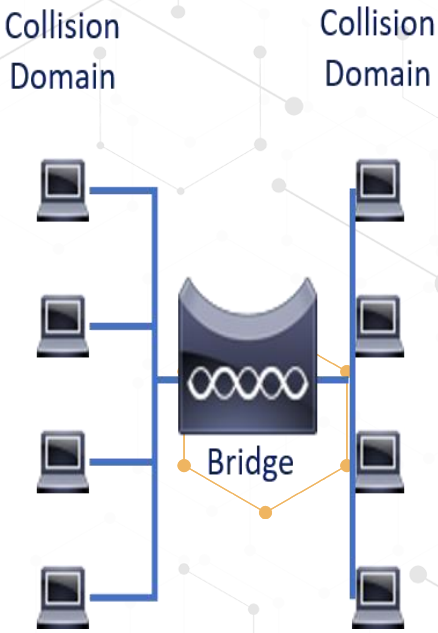
Cellular Networks:

- 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.

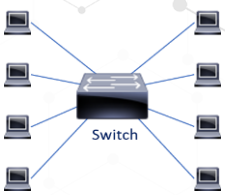
- **3G:**
  - Bandwidth: 2 Mbps, latency: 100-500 ms, average speed 144 kbps.
- **4G:**
  - Bandwidth: 200 Mbps, latency: 20-30 ms, average speed 25 Mbps, 16km (10 miles).
- **5G:**
  - Bandwidth: 5-20 Gbps, latency: <10 ms, average speed 200-400 Mbps, 500m (1500 ft).
  - High frequency, short-range,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

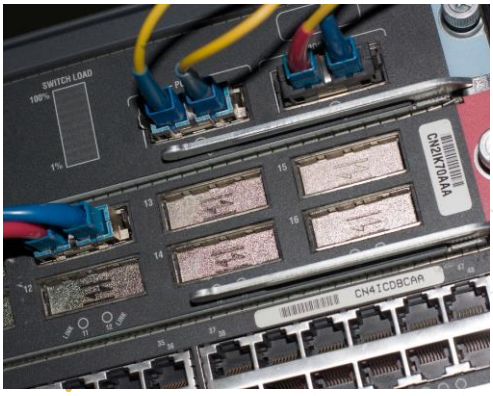
Secure Network Devices and Protocols:

- We have different network devices through the OSI and TCP/IP models and many have protocols specific to that device.
- **Layer 1 Devices:**
  - **Repeaters** receive a signal and retransmit it.
    - They are used to extend transmissions so that the signal can cover longer distances.
  - **Hubs** are repeaters with more than 2 ports.
    - All traffic is sent out all ports; no Confidentiality or Integrity, half-duplex, and not secure at all.
- **Layer 2 Devices:**
  - **Bridges** are 2 port switches used to separate collision domains, sends traffic across the 2 domains, but traffic from one domain is not seen on the other unless sent there.

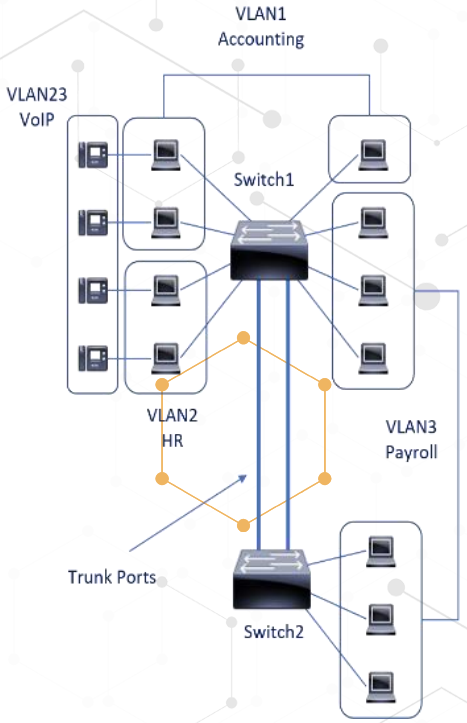


- **Switches** are bridges with more than 2 ports.
  - Each port is its own collision domain, fixing some of the issues with collisions.
  - Can range from 4 to 500+ ports.
  - Use MAC addresses to direct traffic.
  - Good switch security includes:
    - Shutting unused ports down.
    - Put ports in specific VLANs.
    - Using the MAC Sticky command to only allow that MAC to use the port, either with a warning or shut command if another MAC accesses the port.
    - Use VLAN pruning for Trunk ports.





- **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.

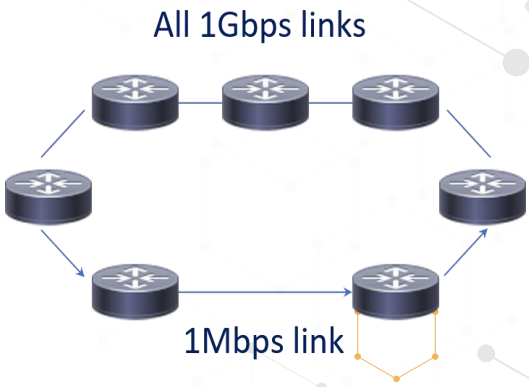
- **Layer 3 Devices:**
  - **Routers:**
    - Normally have a few ports vs. a lot on switches.
    - For our organizations, they are in the data centers.
    - In your home, they are often combined with a switch and wireless in one box.
    - Forward traffic based on source and destination IPs and ports.
    - 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.

- **Routers** have two operation planes:
  - **Control Plane:**
    - A router maintains a routing table that lists which route should be used to forward a data packet and through which physical interface connection.
    - It uses internal pre-configured static routes or by learning routes using a dynamic routing protocol.
    - Static and dynamic routes are stored in the **RIB** (Routing Information Base).
    - The control-plane logic then strips non-essential directives from the RIB and builds an **FIB** (Forwarding Information Base) to be used by the forwarding-plane.
  - **Forwarding Plane:**
    - The router forwards data packets between incoming and outgoing interface connections.
    - It routes them to the correct network type using information that the packet header contains.
    - It uses data recorded in the routing table control plane.

- **Layer 3 Protocols:**
  - We configure static routes for the certain paths, it is not scalable and would be impossible to maintain manually.
  - To help with that, we use dynamic routes learned through routing protocols.
    - **Convergence** is when a set of routers have the same routing information about the network they are in.
    - For routers to converge, they must have all available routes from each other via routing protocols, all routers agree on what the network topology looks like.
    - Any change in the network that affects routing tables will break the convergence temporarily until this change has been successfully communicated to all other routers.
    - All IGP (Interior Gateway Protocols) rely on convergence to function right.
    - When dynamic is enabled, every participating router will exchange what they know about the network.
    - How it is done and how much is shared depends on the routing protocol used.
    - The Exterior Gateway Routing Protocol BGP typically never converges because the Internet is too big for changes to be communicated fast enough.

- **Distance vector routing protocols:**
  - Only focus on how far the destination is in.

    Hops (how many routers in between here and there).
  - Do not care about bandwidth, they just use the shortest path.
  - In the example on the right the traffic will go over the 1Mbps link even with it being 1/1000th the speed of the 1Gbps links.
  - Not very used anymore, today we use Link-state routing protocols.

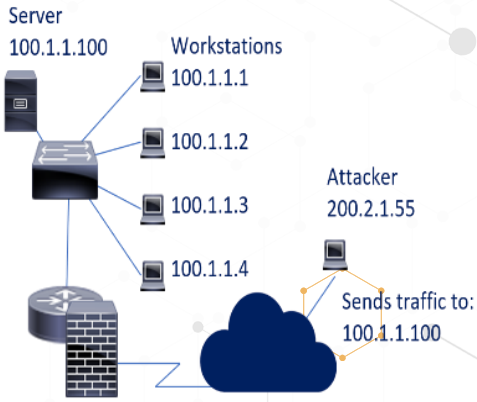


- **RIP (Routing Information Protocol):** Uses UDP port 520 for its transport protocol.
  - One of the oldest distance-vector routing protocols which uses the hop count as a routing metric.
  - Uses maximum hops to prevent routing loops, the maximum number of hops for RIP is 15, a hop count of 16 is considered an infinite distance and the route is considered unreachable, routes are updated every 30 seconds.
  - RIP uses split horizon, route poisoning, and hold-down to prevent incorrect information from propagating.
  - **Hold-down** timers are started per route entry when the hop count is changing from lower value to higher value.
    - This allows the route to get stabilized, during this time no update can be done to that routing entry.
  - **Route poisoning** is used to prevent a router from sending packets through a route that has become invalid.
    - Provides updates with unreachable hop counts immediately to all the nodes in the network.
  - **Split-horizon** route advertisement is used to prevent routing loops by stopping a router from advertising a route back onto the interface it learned the route from.
  - **Split-horizon** routing with **poison reverse** is a variant of split-horizon route advertising where a router actively advertises routes as unreachable over the interface over which they were learned by setting the route metric to infinite.
  - That immediately removes most looping routes before they can propagate through the network.

- **Link-state routing protocols:**
  - Each node independently runs an algorithm over the map to determine the shortest path from itself to every other node in the network.
  - The collection of best paths will then form the nodes routing table.
  - It is based on a link cost across each path which includes available bandwidth among other things.
  - Routing tables are synchronized at start up and updates are only when topology changes occur.
  - **OSPF (Open Shortest Path First):** Used within a single routing domain which is logically divided into areas.
    - Can be used on IPv4 (v2) and IPv6 (v3) networks and supports CIDR addressing model.
    - Detects changes in the topology, such as link failures, and converges on a new loop-free routing tables within seconds.
    - Does not use a transport protocol (UDP/TCP) but encapsulates the data directly in IP packets with protocol number 89.
- **Link-state routing protocols:**
  - **BGP (Border Gateway Protocol):**
    - The routing protocol used for the Internet.
    - BGP routes between AS (Autonomous Systems) which are networks with multiple Internet connections.
    - Has some distance vector properties but is considered a path vector routing protocol.
    - BGP makes routing decisions based on paths, network policies or rule-sets.
    - BGP routing tables are massive, some routers can have 100,000s of routes.
    - BGP currently has 860,000+ IPv4 and 100,000 IPv6 routes.
    - IPv4 BGP is predicted to grow by 50-60,000 per year and IPv6 by 30-40,000 per year.

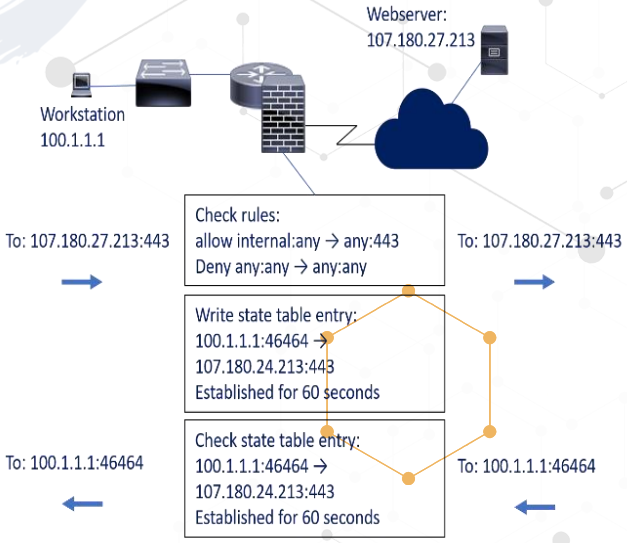
IPv4 Table	IPv4	Prediction
Jan 2016	586,879	
Jan 2017	645,974	
Jan 2018	699,000	
Jan 2019	760,000	
Jan 2020	814,000	
Jan 2021	866,000	
Jan 2022		915,000
Jan 2023		970,000
Jan 2024		1,024,000
Jan 2025		1,078,000

- **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.

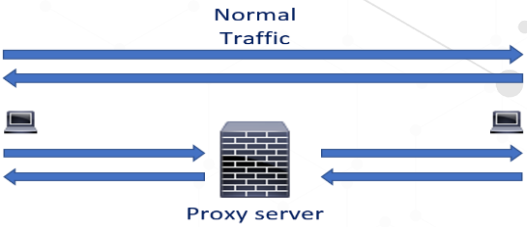


Source	Destination	Action
100.1.1.0/24	100.1.1.0/24	Permit
100.1.1.0/24	Any	Permit
Any	100.1.1.100	Deny
Any	Any	Deny

  - **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.

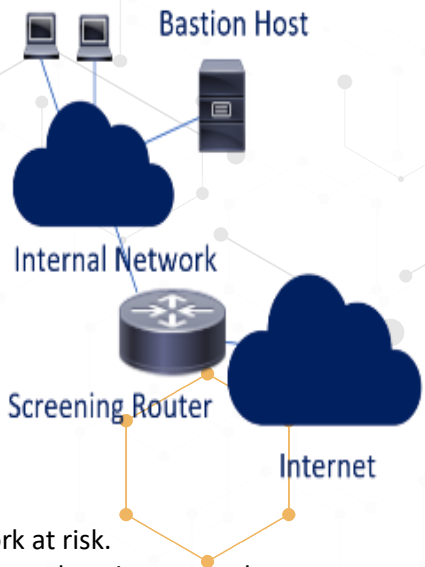


- **Application layer firewalls**, OSI Layer 7.
  - The key benefit of application layer firewalls is that they can understand certain applications and protocols.
  - They see the entire packet, the packet isn't decrypted until layer 6, any other firewall can only inspect the packet but not the payload.
  - 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.

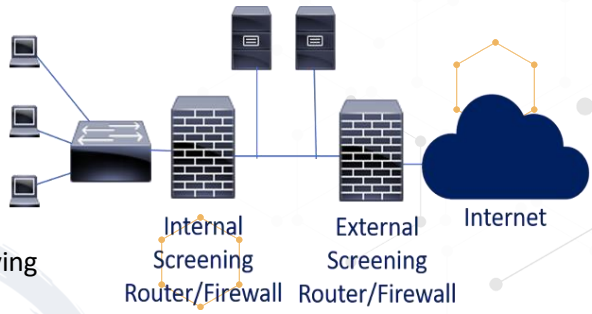
- **Firewalls Design:**
  - **A Bastion Host** is a special purpose host designed and configured to withstand attacks.
    - Normally hosts a single application, all other services are removed or limited to reduce the threat to the host.
    - It is hardened in this manner because of its location and purpose which is either on the outside of a firewall or in a DMZ (demilitarized zone) and usually involves access from untrusted networks or computers.

  - A **Dual-Homed Host** has two network interfaces, one connected to a trusted network and the other connected to an untrusted network (Internet).
    - The dual-homed host doesn't route.
    - Any user wanting to access the trusted network from the outside, needs to log into the dual-homed host and then access the trusted network from there.
    - No longer really used, mostly used premodern firewalls.

  - **Screened Host Architecture**:
    - An older flat network design using one router to filter external traffic to and from a bastion host via ACLs.
    - The bastion host can reach other internal resources, but the router's ACL denies direct internal/external connectivity.
    - The difference between dual-homed host and screened host design is screened host uses a screening router, which filters Internet traffic to other internal systems.
    - Screened host network design does not use defense-in-depth: a failure of the bastion host puts the entire trusted network at risk.
    - Screened subnet architecture evolved as a result, using network defense in depth by using DMZs.

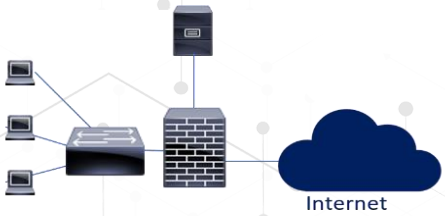


- **Screened Subnet Architecture:**
  - A screened subnet firewall is a variation of the dual-homed and screened host firewall.
  - It can be used to separate components of the firewall onto separate systems, achieving greater throughput and flexibility, although at some cost to simplicity.
  - As each component system of the screened subnet firewall needs to implement only a specific task, each system is less complex to configure.
  - A screened subnet firewall is often used to establish a **DMZ** (demilitarized zone).
  - Good design uses 2 different brands of firewalls to avoid both having the same vulnerabilities.

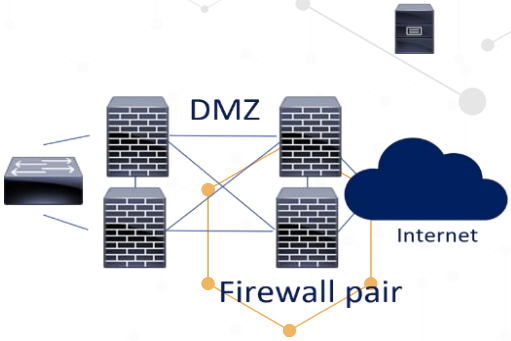


Screened Subnet using Dual Firewall DMZ

- **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



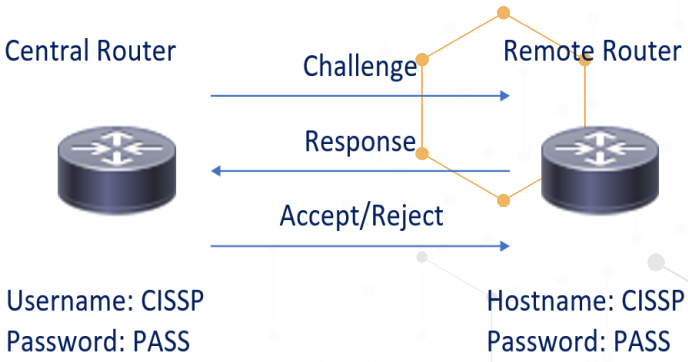
Firewall pair

- **Modem** (**Mo**dulator/**Dem**odulator):
  - **Dial-up modems:** Take binary data and modulate it into analog sound that can be sent over phone networks designed to carry the human voice.
  - The receiving modem then demodulate the analog sound back into binary data.
  - **ADSL modems** (asymmetric digital subscriber line): TP telephone cable can carry signals with higher frequencies than the cable's normal frequency rating.
  - The signal strength drops the longer the cable (Attenuation).
  - **Cable modems** use infrastructure originally intended to carry television signals and therefore designed from the outset to carry higher frequencies.
  - A single cable can carry radio, television, and broadband internet services without interference.
  - Newer types of broadband modems are also available, including satellite and power line modems.

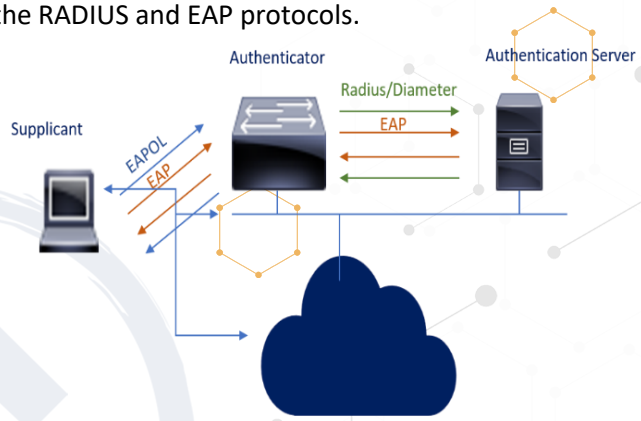
- **DTE (Data Terminal Equipment):**
  - An end device often a desktop or a server (called tail circuits) that converts user information into signals or reconverts received signals.
  - A DTE device communicates with the data DCE (Data Circuit-terminating Equipment).

- **DCE** is often a modem, it sits between the data terminal equipment (DTE) and a data transmission circuit.
  - The DCE does the signal conversion, coding, and line clocking and may be a part of the DTE or intermediate equipment.
  - Interfacing equipment may be required to couple the data terminal equipment (DTE) into a transmission circuit or channel and from a transmission circuit or channel into the DTE.
  - The DCE is at the end of an ISP's network, it connects to the customer DTE.
- The circuit is synchronous and both sides must synchronize to a clock signal provided by the DCE.
- The Demarc is the point where the DTE and DCE meet, where the network passes from ISP responsibility to customer.

- **Secure Communications:**
  - Securing our data-in-motion is one of the most difficult tasks we have.
  - The internet and IPv4 was never built to be secure and just like anywhere else we need to find the right balance of Confidentiality, Integrity, and Availability.
  - **Authentication Protocols:**
    - Communications or cryptographic protocols designed to transfer authentication data between two entities.
    - They authenticate to the connecting entity (often a server) as well as authenticate themselves(often a server or desktop) by declaring the type of information needed for authentication as well as syntax.
    - It is the most important layer of protection needed for secure communication between networks.
    - **PAP (Password Authentication Protocol):**
      - Authentication is initialized by client/user by sending packet with credentials (username and password) at the beginning of the connection.
      - One of the oldest authentication protocols, no longer secure. The credentials are being transmitted over the network in plain text making it vulnerable to simple attacks like Eavesdropping and man-in-the-middle attacks.
    - **CHAP** (Challenge-Handshake Authentication Protocol):
      - Provides protection against replay attacks by the peer through the use of an incrementally changing identifier and of a variable challenge-value.
      - Requires that both the client and server know the plaintext of a shared secret like a password, it is never sent over the network.
      - Providing better security compared to PAP which is vulnerable for both these reasons.
      - Used by PPP (Point to Point Protocol) servers to validate the remote clients.
      - CHAP periodically verifies the identity of the client by using a three-way handshake.
      - The CHAP server stores plaintext passwords of each client, an attacker gaining access to the server can steal all the client passwords stored on it.

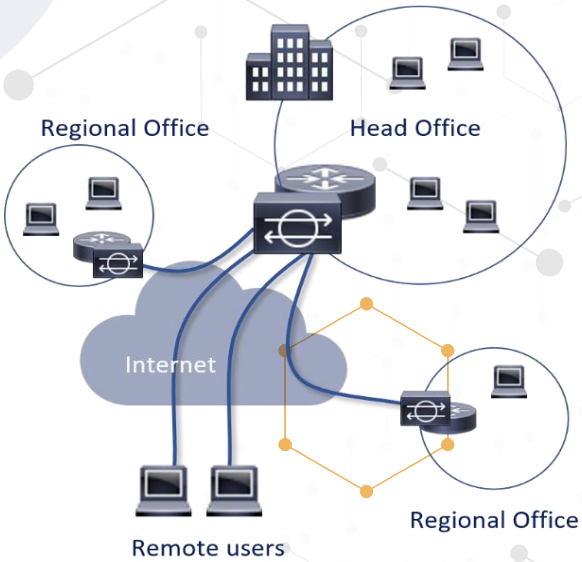


- **802.1X** defines the encapsulation of **the EAP (Extensible Authentication Protocol).**
  - 802.1X authentication involves three parties: a supplicant, an authenticator, and an AS (authentication server).
  - The **supplicant** is a client device (normally a workstation) that wants to attach to the LAN/WLAN, normally software running on the client that provides credentials to the authenticator.
  - The **authenticator** is a network device, a switch or wireless AP.
  - The **AS** (Authentication server) is typically a host running software supporting the RADIUS and EAP protocols.
  - In some cases, the authentication server software may be running on the authenticator hardware.
  - EAP is widely used in 802.11 (Wi-Fi), the WPA, and WPA2 standards; it was adopted with 100+ EAP Types as the official authentication mechanism.



- **PEAP (Protected EAP):**
  - A protocol that encapsulates EAP within a encrypted and authenticated TLS (Transport Layer Security) tunnel.
  - Developed by Cisco Systems, Microsoft, and RSA Security.
- **EAP-MD5:**
  - Very weak forms of EAP. It offers client to server authentication only, where most others provide mutual authentication.
  - Vulnerable to man in the middle attacks and password attacks.
- **LEAP (Lightweight Extensible Authentication Protocol):**
  - Cisco distributed the protocol through the CCX (Cisco Certified Extensions) as part of getting 802.1X and dynamic WEP adoption into the industry in the absence of a standard.
  - No native support of LEAP in the Windows OS.
- **EAP-TLS (EAP-Transport Layer Security):**
  - Uses PKI, requiring both server and client-side certificates.
  - Establishes a secure TLS tunnel used for authentication.
  - This makes it very secure but also complex and expensive.

- **EAP-TTLS (EAP Tunneled Transport Layer Security):**
  - Simpler than EAP-TLS by dropping the client-side certificate requirement, allowing other authentication methods for client-side authentication.
  - This makes it easier to deploy but also less secure.
- **PANA (Protocol for Carrying Authentication for Network Access):**
  - Allows a device to authenticate itself with a network to be granted access.
  - EAP will be used for authentication protocol, key distribution, key agreement, and key derivation protocols.
- **SLIP (Serial Line Internet Protocol):**
  - An encapsulation of IP designed to work over serial ports and modem connections.
  - On PCs it has been replaced by PPP, which is better engineered, has more features, and does not require its IP address configuration to be set before it is established.
  - On microcontrollers, SLIP is still the preferred way of encapsulating IP packets because of the very small overhead.
- **PPP (Point-to-Point Protocol):**
  - Used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, ...
  - PPP is also used over Internet access connections.
  - ISPs (Internet Service Providers) have used PPP for customer dial-up access to the Internet since IP packets cannot be transmitted over a modem line on their own without some data link protocol.
- **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.

- **PPTP (Point-to-Point Tunneling Protocol):**
  - Obsolete method for implementing virtual private networks because of many known security issues.
  - PPTP uses a TCP control channel and a GRE tunnel to encapsulate PPP packets.
  - No built-in encryption or authentication and PPP being tunneled to implement security.
- **L2TP (Layer 2 Tunneling Protocol):**
  - Tunneling protocol used to support VPNs or as part of the delivery of services by ISPs.
  - No built-in encryption or confidentiality, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

- **IPSEC (Internet Protocol Security):**
  - **SA (Security Association):** Simplex one-way communication, can be used to negotiate ESP (Encapsulation Security Payload) or AH (Authentication Header) parameters.
    - If 2 systems use ESP to communicate, they need 1 SA for each direction (2 total); if AH and ESP, 4 total.
    - A unique 32bit SPI (Security Parameter Index) is used to identify each SA connection.
  - **ISAKMP (Internet Security And Key Management Protocol):**
    - Manages the SA creation process.
  - **Tunnel mode** encrypts and authenticates the entire package (including headers).
  - **Transport mode** only encrypts and authenticates the payload, used for systems that speak IPSEC.
  - **IKE (Internet Key Exchange):**
    - IPsec can use different types of encryption (3DES or AES) and hashes (MD5, SHA1, SHA2, …).
    - IKE negotiates the algorithm selection process.
    - The 2 sides of an IPsec tunnel will normally use IKE to negotiate to the highest and fastest level of security, selecting AES over single DES for confidentiality if both sides support AES, for example.

- IPSec can protect data flows between a pair of hosts (host-to-host), a pair of security gateways (network-to-network), and a security gateway and a host (network-to-host).
- IPSec is an end-to-end security scheme operating in the Internet Layer of the TCP/IP model, only IPsec protects all application traffic over an IP network.
- IPsec can automatically secure applications at the IP layer.

- **SSL** and **TLS** – Confidentiality and Authentication for web traffic.
  - Cryptographic protocols for web browsing, email, Internet faxing, instant messaging, and VOIP.
  - You download the server's digital certificate which includes the sites public key.
  - **SSL (Secure Socket Layer)** Currently on v3.0.
    - Mostly used for web traffic.
  - **TLS (Transport Layer Security)** More secure than SSL v3.0.
    - Used for internet chat and email client access and used for securing web traffic.

- **ISDN (Integrated Services Digital Network)** - OSI layer 1-3.
  - Used for digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network.
  - A circuit-switched telephone network system which also provides access to packet switched networks.
  - It offers circuit-switched connections (for either voice or data) and packet-switched connections (for data) in increments of 64 kilobit/s but could be higher with channel bonding.

- **DSL (Digital Subscriber Line)** is a family of technologies that are used to transmit digital data over telephone line.
  - Often used to describe ADSL (Asymmetric DSL), the most common DSL technology.
  - DSL service can be delivered side by side with wired telephone service on the same line, this is possible because DSL uses higher frequency bands for data.
  - At the customer Demarc, a DSL filter on each non-DSL outlet blocks any high-frequency interference to enable simultaneous use of the voice and DSL services.

- **Callback** is a modem-based authentication system.
  - Was mostly used for securing dial-up connections.
  - The client computer calls the server computer.
  - After a greeting the client identifies itself, usually with a username.
  - The server disconnects the call.
  - Depending on the username and a list of users' phone numbers, the server will then establish a second call back to the client computer.
  - The client computer expecting this returned call will then answer and communications between the two computers will proceed normally.

- **Caller ID** does the same, but the user has to be calling from the right number.
  - It can easily be faked, many phones or phone companies allow the end user pick their caller ID.

- **Remote Administration** is controlling a computer from a remote location, we do this through software.
  - A remote location may refer to a computer in the next room or to one across the world.
  - Any computer with an Internet connection can be remotely administered.

- **RDP (Remote Desktop Protocol) -** A Microsoft proprietary protocol.
  - The user uses RDP client software for this, and the other computer must run RDP server software.
  - Providing a user with a GUI (Graphical User Interface) by default, the server listens on TCP and UDP 3389.
- **VNC (Virtual Network Computing) -** Non-MS proprietary and can run on most OSs (Using screen scraping).
  - It was at first used for remote administration of computers but is also being used more and more now for Remote Desktop Protocol for multi-user environments and helpdesk RDP access.

- Newer versions use HTTPS (TCP port 443) and has the GUI contained in a browser.
  - You install the software on the system you want to access and the one you want to access from, set up username/password and you can control that system from anywhere.
  - Commonly used include: Chrome Remote Desktop, LogMeIn, GoToMyPC, support.me,…

- **VDI (Virtualized Desktop Infrastructure/Interface):**
  - **Thin Clients:**
    - Diskless Workstation (Diskless node) has all the normal hardware/firmware except the disk, it has the lower-level OS (the BIOS) which performs the POST and it then downloads the kernel and OS.
    - Thin Client Applications - We use a Web Browser to connect to the application on a server on port 80 (HTTP) or port 443 (HTTPS), the full application is housed and executed on the server vs. on your PC.
    - Often stripped of non-essentials like CD drives, most ports,...

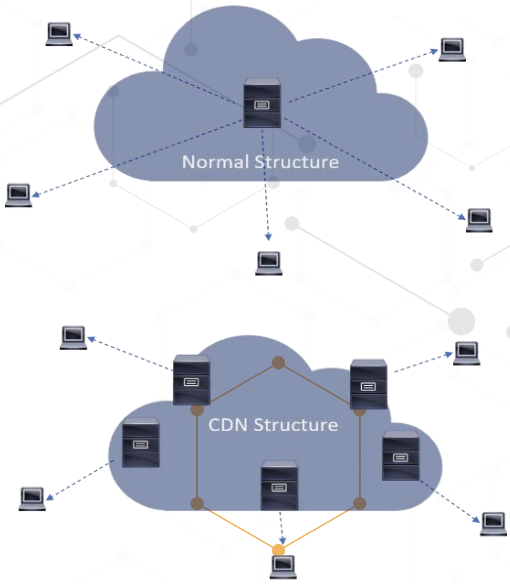
  - **Zero Clients:**
    - Getting more popular for VDI because they are even slimmer and more cost-effective than thin clients.
    - These are client devices that require no configuration and have nothing stored on them.
    - They are sold by Dell, Fujitsu, HP, Pano Logic,...

- **IM (Instant Messaging):**
  - Short messages are typically sent between two parties (one-to-one) or many to many (group IMs).
  - Some IM applications can use push technology to provide real-time text which transmits messages character by character as they are typed, others send when you hit enter.
  - More advanced instant messaging can add file transfer, clickable hyperlinks, Voice over IP, and video chat.
  - Commonly used chat protocols today include IRC, Jabber, Lync, and still used but very limited ICQ and AIM.
  - Today most IM'ing is done embedded in other applications like Facebook, LinkedIn, Twitter, or WhatsApp.
  - Many IM applications and protocols are not designed with security in mind, they are designed for usability.
    - A report on the level of safety offered by instant messengers, only 2 out of 18 instant IM apps they looked got "nothing of concern" on sending sensitive attachments and mining/selling customer data, the rest got "not recommended". The most popular messenger has 25 "not recommended" and only 6 "nothing of concern" when looking at privacy and security.

- IM connections are often sent in plain text, making them vulnerable to eavesdropping.
- Software often requires the user to open UDP ports, increasing the threat posed by potential security vulnerabilities.

- **Web Conferencing:**
  - An umbrella term for different types of online collaborative services including webinars, webcasts, and peer-level web meetings.
  - Commonly used ones are WebEx, Zoom, GoToMeeting, Google Meet, TeamViewer, ...
  - Done over TCP/IP connections, services often use real-time point-to-point communications as well as multicast communications from one sender to many receivers.
  - It offers data streams of text-based messages, voice, and video chat to be shared simultaneously across geographically dispersed locations.
  - Applications where web conferencing is used: Meetings, training events, lectures or presentations one-to-one or many-to-many like IMs.
  - The use of web conferencing should align with your organizations policies, some may, if not implemented right be a security vulnerability.
  - They can bypass some security by using SSL/TLS tunnels and acceptable products should be hardened.

- **CDN (Content Distribution Network):**
  - A geographically dispersed network of proxy servers and data centers.
  - The client is sent to the server node with the lowest latency in MS.
  - The client's webpages, software download, and video streaming are faster.
  - The provider saves on cost, sending traffic short distances vs. long distance and it provides redundancy and some DDOS protection.
  - The idea is to distribute service spatially relative to end-users to provide high availability and high performance.
  - Many different services can be provided over CDNs : video streaming, software downloads, web and mobile content acceleration, licensed/managed CDN, transparent caching, and services to measure CDN performance, load balancing, multi-CDN switching and analytics, and cloud intelligence.



- **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.

What we covered in the Fourth CBK Domain:

- In this domain we covered how our Network and Communications channels work and how to protect them.
- The OSI and TCP/IP logical models.
- How the internet/intranet works with:
  - IP addresses: IPv4, IPv6, Private, and Public Addresses.
  - Common ports.
  - DNS, ARP, DHCP, NAT, PAT, and the other protocols we use to make our network function.
  - The networking routing protocols.
  - How we secure our communication on our local network and the internet.
  - Micro-segmentation, wireless, and cellular networks.
  - Common Attack types and how to mitigate them.
- Networking equipment and how we secure the different types.
  - Repeaters, Hubs, Routers, Switches, Firewalls, cable types, ...
- Network topologies and technologies.
  - LAN, WAN, Ring, Star, Mesh,...

OSI model - Open Systems Interconnection Reference model