Computer Networking Course - Network Engineering (CompTIA Network+) Part 1

Devices

Layer 1 Devices

- OSI reference model
- **modem**: take a digital signal and convert to a analog signal and place it on wire. vice versa.
- Hub: not common any more. take the electrical signal arrived and replicate it out all of the other ports.

Layer 2 Devices

- **Switch**: utilize an ASIC chip to learn when a device is on the network and which ports it is connected to via the device's MAC address.
    - only communicate with the local network devices
- **WAP (wireless access point)**: a specific type of network bridge that connects/bridges wireless network segments with wired network segments.
    - most common type: bridge 802.11 wireless network segments with 802.3 ethernet network segments.
    - only local network devices

Layer 3 Devices

- **MLS (multilayer switch)**: provide L2 nw switching services, as well as L3 or higher OSI model services
    - most common is L3 switch: not only switching, but also programed to handle routing functions. (not limit to local network device)
    - expensive, not found in home and office, but interprise local area network
- **Router**: most common nw device for connecting different nw

    - use software programming for decision making, keep track of diiferent networks and find best route
    - can communicate with local and non-local nw devices

Security Devices

- **Firewall**: placed on routers or hosts (sw) or be its own device
    - functions at multilayers: L2,3,4,7
    - block packets from entering or leaving the nw
        - via stateless inspection: examine every packet against a set of rules
        - via stateful inspection: only examine the state of the connection between networks
    - first line of defense in protecting the internal nw from outside threats
- **IDS (Intrusion detection system)**: passive sys designed to identify when a nw breach or attack against the nw is occuring
    - *cannot* prevent or stop nw breach or attach on its own
    - receives a copy of all traffic and evaluates it against a set of standards
        - signature based: evaluate nw traffic for known malware or attack signature
        - anomaly based: suspicious changes
        - policy based: specific declared security policy
    - may deploy at host level (HIDS)
- **IPS (Intrusion prevention system)**: active sys designed to stop a breach or attack
    - designed to perform an action or set of actions to stop malicious activity
    - all traffic on the nw segment flows through the IPS to either enter or leave the segment
        - all traffic is evaluated against a set of standards (like IDS)
    - best to be placed between a router (with a firewall) and the destination nw segment
    - programmed to make active response to situations like:
        - block offending IP address

        - close down the vulnerable interface
        - terminate the nw session
        - redirect the attack
        - etc.
- **VPN (virtual private network) concentrator**: allow many more secure VPN connections to a network
    - provide proper tunneling and encryption
    - can function at multiple layers, but most func at L3, providing IPsec encryption through a secure tunnel
        - SSL VPN at L7

Optimization and Performance Devices

- **Load balancer**: content switch or content filter
    - used to load balance between multiple hosts that contain the same data to spread out the workload for greater efficiency
    - used to distribute the requests to a server farm among the various servers, to help not to overloaded
- **Proxy server**: requests resources on behalf of client machines
    - used to retrieve resources from outside untrusted nw
    - hide and protect the requesting client
    - can be utilized to filer allowed content
    - can increase nw performance by caching commonly requested web pages

Networking Services and Applications

The basics of the VPN

- VPN is used by remote hosts to access a private network through an encrypted tunnel through a public network.

- VPN types
    - the site-to-site
    - remote-access (host-to-site): allows select remote users to connect to the local nw; making connection uses VPN client software
    - host-to-host (SSL VPN): secure connection between 2 sys without VPN client software

Protocols used by the VPN

- **IPSec (Internet protocol security)**
    - L3
    - to secure a VPN connection
    - transmit unicast packets (1-to-1)
    - can be used with AH protocol
        - *AH*: only autentication, no encryption
    - can be used with ESP
        - **ESP**: both authenticate and encrypt packets
    - both AH and ESP operate in one of two modes:
        - transport mode: between 2 devices (host-to-host)
        - tunnel mode: between 2 endpoints (site-to-site)
    - IPSec implements internet security association and key management (ISAKMP) by default
- **GRE (Generic routing encapsulation)**
    - tunneling protocol that is able to encapsulate a wide variety of nw layer protocols
    - used to create a sub-tunnel with an IPSec connection
        - multicast or broadcast
- PPTP (point-to-point tunneling protocol)
    - older VPN tech that supports dial-up VPN

- **TLS (Transport layer security)**
    - cryptographic protocol used to create a secure encrypted connection between 2 end devices or application
    - largely replaced SSL
    - works at L5 and above
    - common use: create a secure encrypted internet session (SSL VPN)
- ***SSL (secure socket layer)***
    - older cryptographic protocol tha is similar to TLS
    - most common use: internet transactions

Network Access Services

- **NIC (Network interface controller)**
    - also called nw interface card
    - is how a device connects to a nw
    - works at:
        - L2: provide functional means of nw comm by determing which nw protocols will be used
            - provide local nw node address through its physical MAC addr
        - L1: determine how the nw data traffic will be converted into electrical signal
    - modern computers come with at least one built in ethernet NIC
- **RADIUS (Remote authentication dial in user service)**
    - remote access service that is used to authenticate remote users and grant them access to authorized nw resources.
    - it is a popular AAA (authentication, authorization, accounting) protocol
        - used to help ensure that only authenticated end users are using the nw resources they are authorized to use
    - only the end user's password is encrypted

- **TACACS+ (Terminal access controller access-control system plus)**
    - similar to RADIUS, but accounting features are not as robust as RADIUS, and all transmissions between devices are encrypted

Other Services and Applications

- **RAS (Remote access services)**
    - not a protocol, but a roadmap
    - description of the combination of software and hardware required for a remote access connection.
- Web services
    - creating a means of cross communication between sw packages or disparate platforms by translating communication into an XML format.
- Unified voice servie
    - create better voice communication systems

DHCP in the network

- **DHCP (Dynamic host configuration protocol)**: give the PC an IP address, tell the PC the default gateway and how to find a DNS server

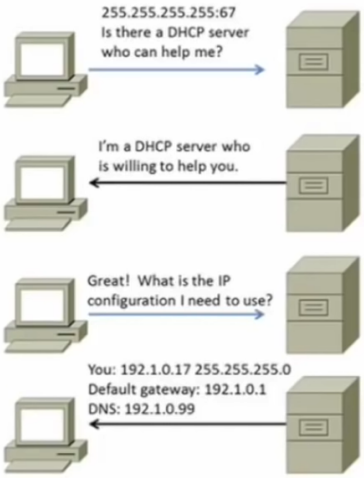
Static vs. dynamic IP addressing

- computer receive the IP configuration in one of 2 ways:
    - statically: assigned manually, work for small and stable nw but not when nw grows
    - dynamically (through service like DHCP)
        - administrator configure a DHCP server to handle the assigning process --- automate the process

How DHCP works

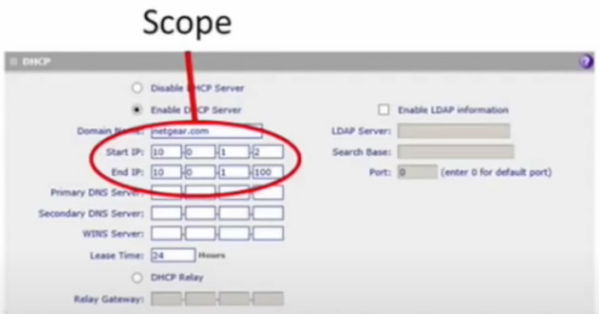
- typical DHCP process

- **Typical DHCP process.**
  - Upon boot up, a PC that is configured to request an IP configuration sends a DHCP **discovery packet**.
    - The discovery packet is sent to the broadcast address: 255.255.255.255:67 (UDP port 67).
  - The DHCP server receives the discovery packet and responds with an **offer packet**.
    - The offer packet is sent to the MAC address of the computer using UDP port 68.
  - The computer receives the offer packet from the DHCP server and returns a **request packet** (requesting the proper IP configuration) to the DHCP server.
  - Once the DHCP server receives the request packet, it sends back an **acknowledgement packet**, which contains the required IP configuration information.
  - Upon receipt of the acknowledgement packet, the PC changes its IP configuration to reflect the information received.



Components and processes of DHCP

- **Ports used.**
  - PC sends discovery packet to 255.255.255.255:67.
  - DHCP sends offer packet to the PC's MAC address on port 68.
- **Address scope.**
  - Administrator configures the IP address range with one that is available to be handed out.
- **Address reservations.**
  - Administrator reserves specific IP addresses to be handed out to specific MAC addresses. These are used for devices that should always have the same IP address (e.g., servers and routers).
  - Allows for these addresses to be changed from a central location instead of having to log in to each device separately.



- Processes:
  - **Leases.**
    - Configuration parameters are only good for a specified amount of time.
    - Leases are configured by the administrator.
  - **Options.**
    - Default gateway location.
    - DNS server addresses (there can be more than one).
    - Time server addresses.
    - Many additional options.
  - **Preferred IP configuration.**
    - A PC can have a preferred IP address.
    - The administrator can configure the DHCP server to either honor the preference or ignore it.

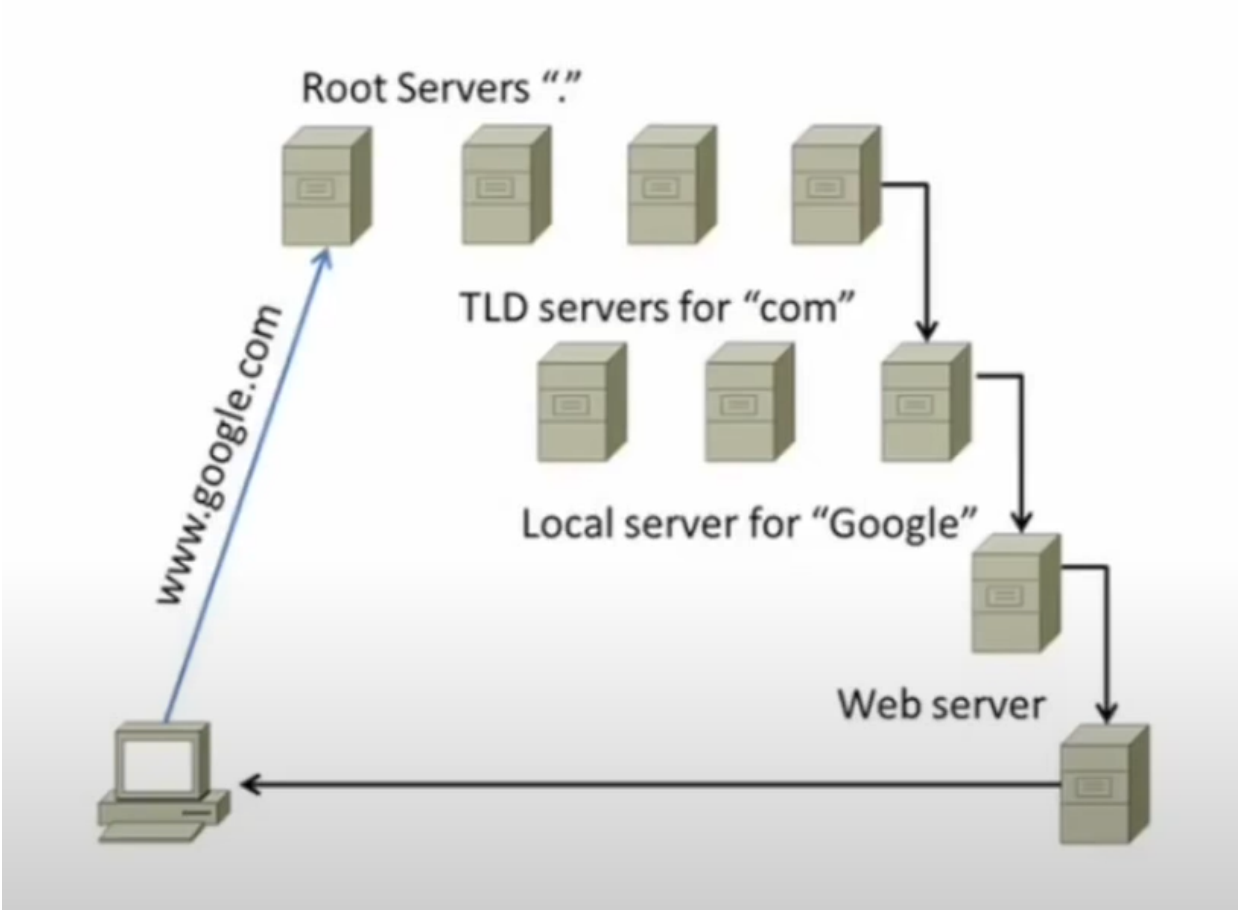
- **Broadcast transmissions cannot pass through a router**. The router can be configured to be a DHCP relay if no DHCP server on the local nw segment. When the DHCP realy receives a

discovery packet from a node, it will forward the packet to the nw segment on which the DHCP server resides. And so fewer configured DHCP servers are needed (reducing maintenance).

Introduction to the DNS service

DNS servers

- **DNS (Domain name system)**: map human friendly names to IP addresses.
    - hierarchical
    - from right to left (read back-forward)
- Different levels of DNS servers
    - **local DNS server**: the server on the local nw that contains the HOSTS file that maps the FQDN to IP addresses in the local subdomain
    - **top level domain (TLD) server**: the server contains the records for a top level domain (.com, .orgn, .net, .edu, etc)
    - **root server**: contains the records for the TLD servers

- 

    - **authoritative server**: responds to a request that has been specifically configured to contain the info. An authoritative response comes from the DNS server that actually holds the original record.
    - **non-authoritative**: responds to a request with DNS info that it received from another DNS server.

DNS records

- A record: maps hostnames to IPv4 addr.
- AAAA record: ~ to IPv6 addr.
- CNAME record: map canonical names to hostnames
- PTR record: pointer record that points to a canoncial name
- MX record: maps to the email server that is specified for a specific domain. It determines how email travels from sender to recipient.

Dynamic DNS (DDNS)

- permits lightweight and immediate updates to a local DNS databse. It is useful when the FQDN remains the same, but the IP addresses is able to change on a regular basis.
- DDNS updating
    - method of updating traditional name servers without the intervention of an administrator (no manual editing is required)

Introduce nw address translation (NAT)

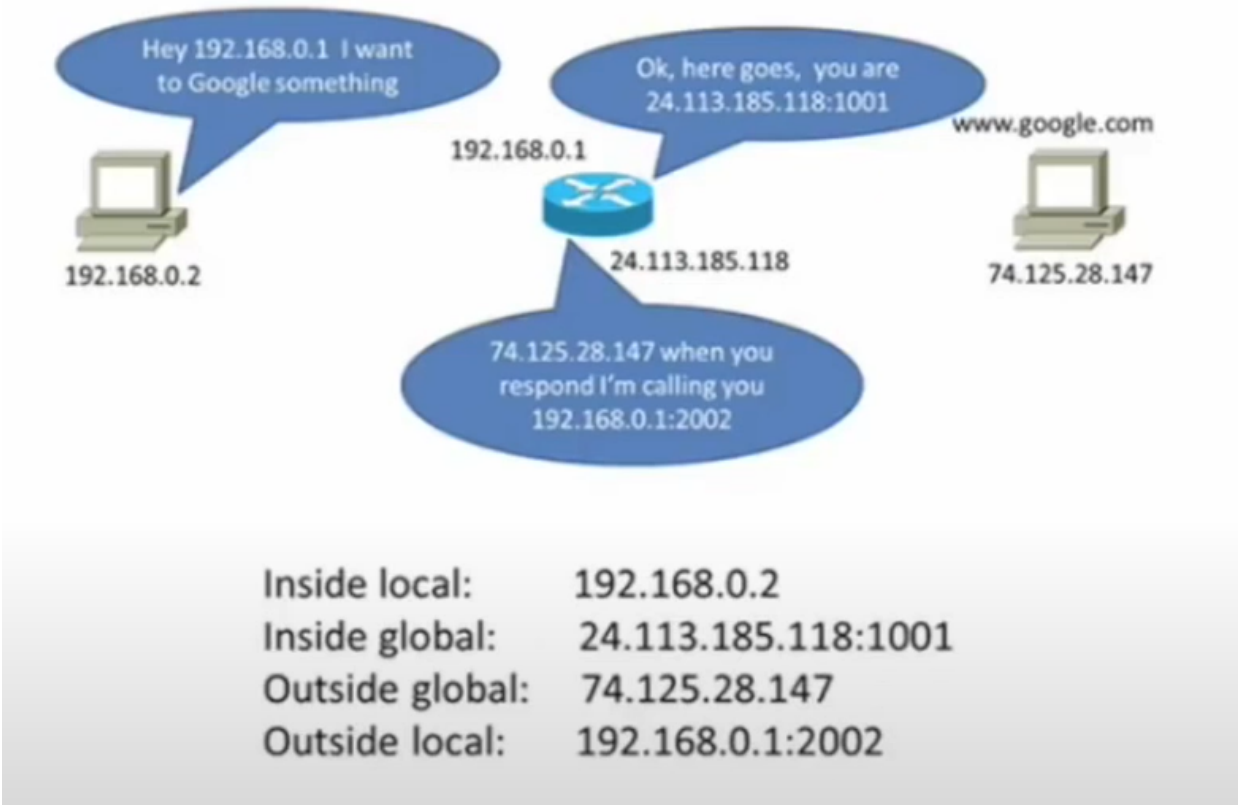
The purpose of nw addr. translation

- Solve the problem of how to route non-routable IP addresses.
    - private IPv4 address spaces are non-routable across public IPv4 nw, a router with NAT enabled will translate a private IP addr into a routable public IP addr.

How it works?

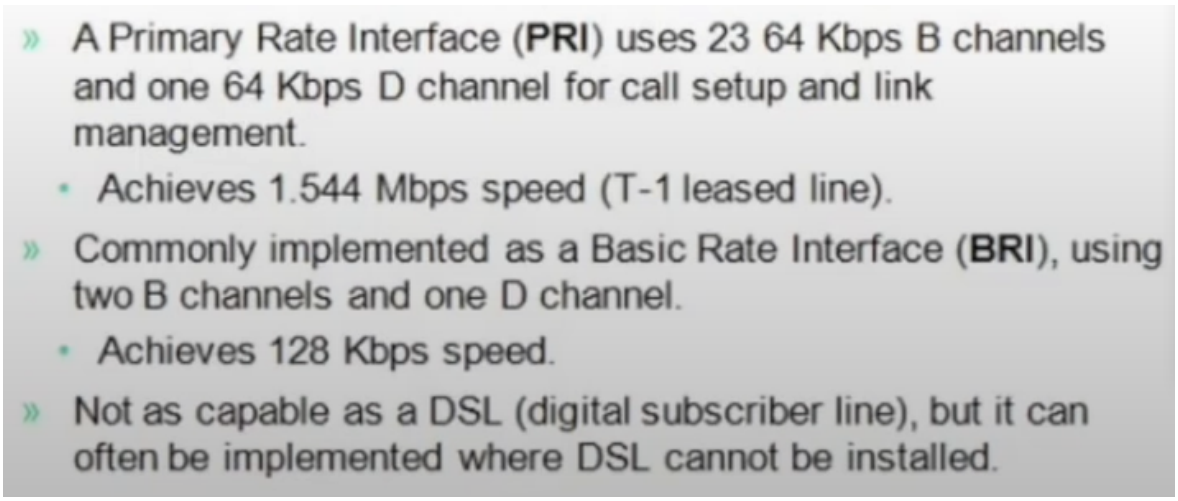
- 2 categories of NAT
    - **Static NAT (SNAT)**: each private IP addr is assigned to a specific routable public IP addr, and kept by the NAT enabled router.
        - when a device needs access outside of the local nw, the router translates the local IP addr to the assigned public IP addr.
        - not flexible and has scalability issues.
    - **Dynamic NAT (DNAT):** the router dynamically assign a routable IP addr to devices from a pool of available public IP addr.
        - more flexible than SNAT, but as more nw traffic, more access to remote nw required, the pool of available public IP addr needs to be increased.
    - **Port address translation (PAT)**: a type of DNAT that was developed to increase the scalability of NAT.
        - addition of dynamically assigning a port bumber to the end of the public IP addr.
        - still require a pool of public IP addr. but less public IP addr required and easier for administrator to maintain.
- The NAT terminology

- » **Inside local address:** a private IP address on the local network.
  - The private IP address assigned to a specific device.
- » **Inside global address:** a public IP address referencing an inside device.
  - The public IP address assigned to the inside device by the NAT enabled router to allow access outside of the network.
- » **Outside global address:** a public IP address referencing an outside device.
  - The public IP address assigned to a device outside of the local network.
- » **Outside local address:** a private IP address assigned to an outside device.
  - The private IP address assigned to an outside device on the interior of the local network.



WAN technologies (Wide Area NW)

Public switched telephone nw (PSTN)

- one of the most common physical infrastructures used in WAN tech due to its widespread availability.
- **Dial-up**
  - utilizes the PSTN to transmit nw traffic as an analog signal
    - require an analog modem to format the nw traffic
    - max theoretical speed: 56 Kbps
- **ISDN (Intergrated Services Digital NW)**
  - digital point-to-point WAN tech using the PSTN
  - completely digital service
    - require the use of a terminal adpater (TA) for the connection to the end node (digital modem)
    - 

- **xDSL**
  - A digital WAN tech using PSTN
  - require digital modem
  - dedicated digital line between the end point and a class-5 central office (CO) ---- withiin 18K feed of the CO
  - carries vocie and data
- **SDSL (Symmetric DSL)**

    - synchronous in nature (same upload and download speed)
    - not carry voice communication
- **ADSL (Asymmetric DSL)**
    - asynchronous
    - carry data and voice
    - most common implementation of DSL in the SOHO (small office and home office) env
- **VDSL (Very-high-bit-rate DSL)**
    - asynchronous
    - used when need high quality video and VoIP
    - only possible when located within 4K feed of a CO

Broadband cable

- coaxial cable networking
    - broadband connection to a location delivered by the cable company
        - can deliver voice, data and television --- all through the same connection
    - **headend**: all cable signals are received at this point; signals are processed and formatted than transmitted to the distribution nw
    - **distribution nw**: smaller service areas served by the cable company. can be composed of fiber optic cabling, coaxial cabling and/or hybrid fiber-coasxial cabling (HFC)
        - Unlike DSL, the bw is shared by the distribution nw --- increasing latency and congestion
    - DOCSIS (Data over cable service interface specification)

Fiber

- Fiber-optic networking
    - **use light to transmit data and voice**
        - allows for more bw over greater distances

- SONET (synchronous optical nw): fiber sun data transmission standard in US
- SDN (syn. digital hierarchy): international standard
- **OC (Optical carrier) levels**: base rates of transmission
- **DWDM (dense wavelength-division multiplexing)**: method of multiplexing serveral OC levels into a single optical fiber, increasing the bw of a single optical fiber
- **CWDM (coarse wavelength-division multiplexing)**: similar to DWDM, but only up to 8 channels on a single fiber
- **PON (passive optical nw)**: point-to-multipoint tech that uses a single optical fiber to connect multiple locations to the internet
  - use unpowered optical splitters

GSM/CDMA WAN connections

- Cellular carriers use one of two methods for connecting devices to their nw and they are not compatible.
- Currently, in US, AT&T and T-Mobile use **GSM (global system for mobile)**, Sprint and Verizon use **CDMA (code division multiple access)**.
- **Celluar networking**
  - involves using the cellular phone system for more than just phone calls.
  - **1G** cellular: voice transmissions
  - **2G**: add simple data transmission (text)
    - 2G EDGE: a stopgap between 2G and 3G
  - **3G**: beginning of cellular WAN networking
  - **4G**: an emerging tech, currently consists of LTE and WiMAX
  - **HSPA+ (Evolved high speed packet access)**: stopgap between 3G and 4G
  - **LTE (Long term evolution)**: use an all-IP based core with high data rates. compatible with 3G and WiMAX

WiMAX WAN connections

- **World Wide Interoperability for Microwave Access (WiMAX) networking**
    - was originally developed as a last mile alternative for use when DSL or cable was not available
        - provide an alternative broadband connection to a fixed location
    - uses microwave transmissions as an over-the-air method to transmit voice and data
        - requires a line of site between relay stations
    - can be used to cover significant geographic distances
    - often considered to be a type of 4G tech because of its compatibility with LTE nw
        - not compatible with 3G type nw

Satellite WAN connections

- **Microwave satellite networking**
    - uses microwave transmissions as an over-the-air method to transmit voice and data
    - can be used to extend nw into places that are hard to reach
    - **microwave radio relay**: method of transmitting through the atmosphere
        - require line-of-site relay stations, but can cover vast distances
        - may have latency problems
    - communication satellite (comsat) forms part of the microwave relay nw
        - may use a variety of orbits
            - molniya, geostationary, low-polar, or polar orbits
            - low-polar and polar orbits are used to boost the microwave signal before sending the signal back to Earth.

Metro Ethernet WAN connections

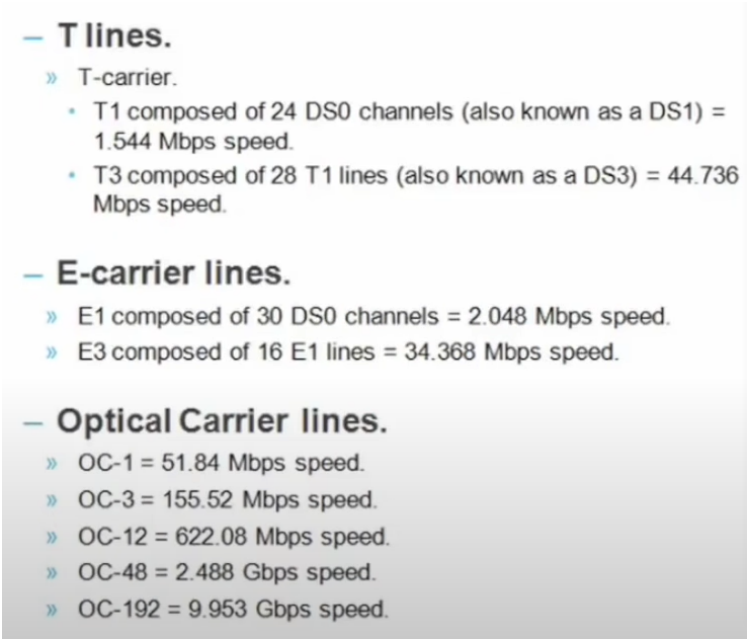
- it is when the service provider connects to the customer's site through an **RJ45 connector**

- the type of connection is actually dependent on the level of service that has been purchased by the customer, while customers view the WAN connection as an Ethernet connection.
- Metro ethernet is commonly deployed as a WAN tech by municipalities at the **metropolitan area nw (MAN)** level.

Leased line WAN connections

- **Leased line**
  - is a dedicated circuit (connection) between 2 end points used for communication. usually a digital point-to-point connection
  - can utilize either a plain old telephone service (POTS) line on the public switched telephone nw (PSTN), or can be a fiber optic cct provided by a telecomm company
  - tend to be more expensive for the customer, the speed is often limited by what customer willing to pay
  - multiplexing tech can be used to increase the amount of channels that are provided on the connection.
- **Point-to-point protocol (PPP)**: common data link layer protocol used with leased line nw.
  - simultaneously transmits multiple L3 protocols through the use of control protocols
  - include a feature called **multilink PPP**, allows for multiple physical interfaces to be bonded together and act as a single logical interface --- to **increase the available bw**.
- **types of leased line connections**
  - **T-carrier (US, Japan, South Korea)**
    - each T line cct level is composed of 24 digital dignal channels (called digital signal 0 DS0)
    - 24 DS0 make a DS1 channel
  - **E-carrier (Europe)**
    - composed of 30 DS0 channels
  - **Optical carrier (OC) lines**
    - OC data rates per channel

Common Standards

- Speed
  - 

Circuit switched vs. packet switched nws

- cct switched nw have a dedicated cct between 2 end points used for communication.
  - e.g., a phone call using a land line
  - most common in nws with leased line communication
  - only one path
- pkt switched nw: data is broken up into smaller chunks and moved through the nw, only to be reassembled at the other end.
  - data traffic is routed using the dest addr
  - data may take different paths through the nw
  - less expensive to maintain

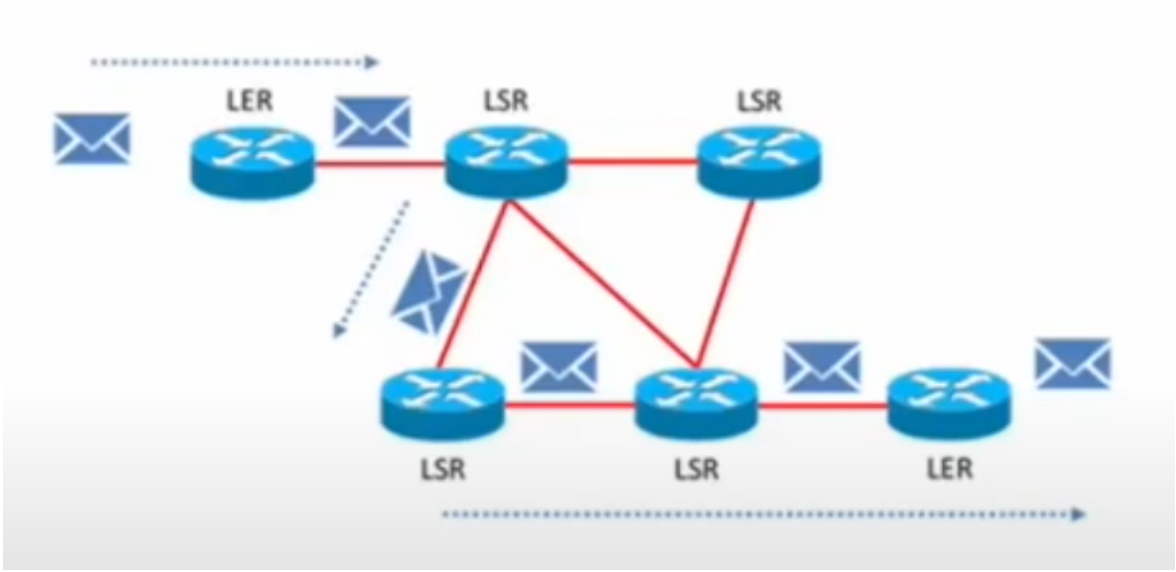
Frame relay vs. asynchronous transfer mode

- **frame relay**
  - a WAN tech in which **variable length** pkts are switched across a nw
  - less expensive than leased line

    - can be made to look like a leased line through the use of a **virtual cct (VC)**
    - tracks a VS using a **data link connection identifier (DLCI)**
    - **access rate**: the max speed of the frame relay interface
    - **committed information rate (CIR)**: guaranteed bw (min speed)
- **ATM**
    - a WAN tech in which **fixed length cells** (each cell is 53 bytes) are switched across a nw
    - can handle real time voice and video
    - fast tech, poor bw utilization (the small cell size reduces the efficiency of the tech)

Multiprotocol label switching

- **MPLS**
    - A topology that is growing in popularity
        - scalable
        - protocol independent
    - can be used to replace both frame relay switching and ATM switching
        - can also be used to pckt switch both frame relay and ATM nw traffic.
    - used to improve the QoS and flow of nw traffic
    - **label edge router (LER)**: add MPLS labels to incoming pckts if they don't have them
    - **label switching router (LSR)**: forwards packets based on MPLS labels.

- 

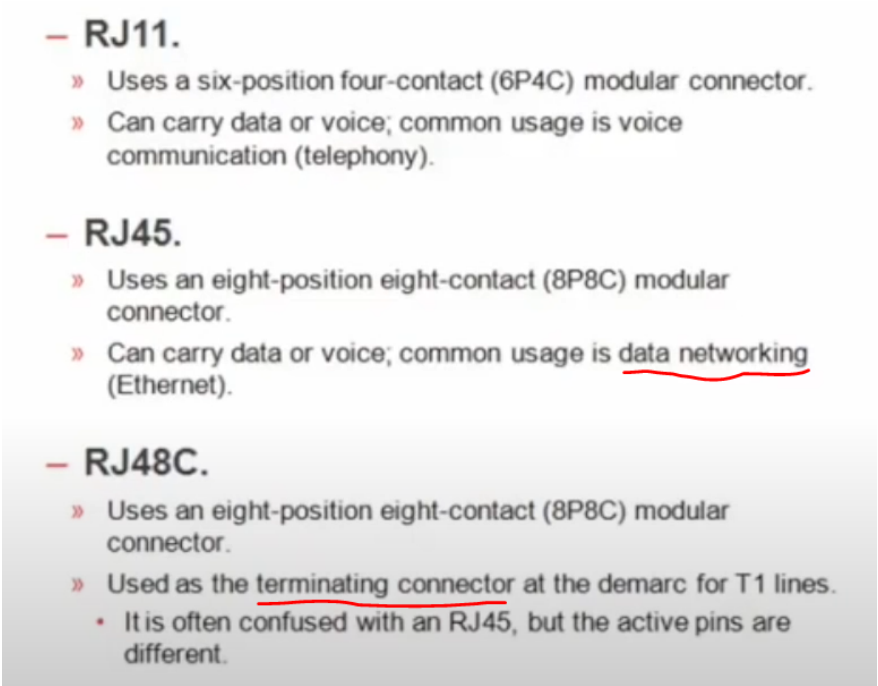
Network Cabling

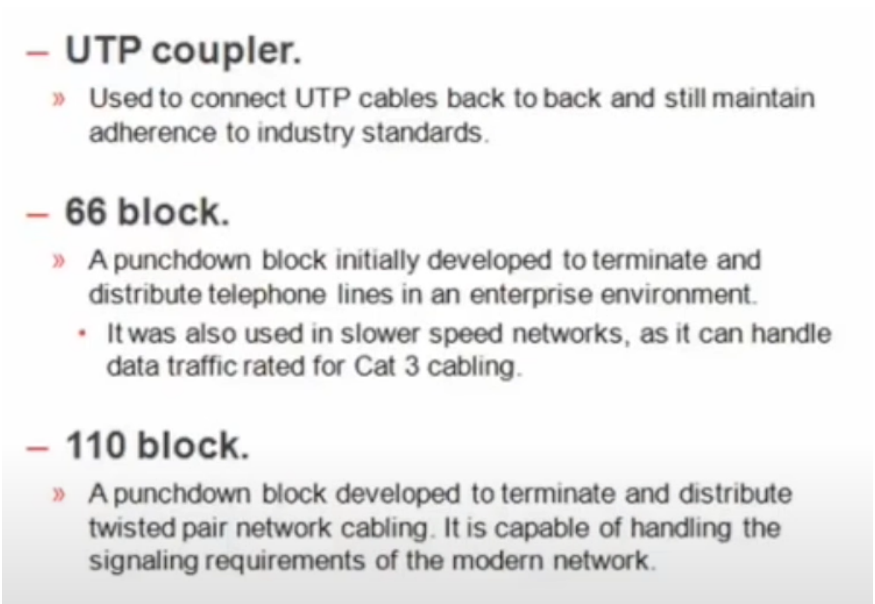
Twisted pair network cabling

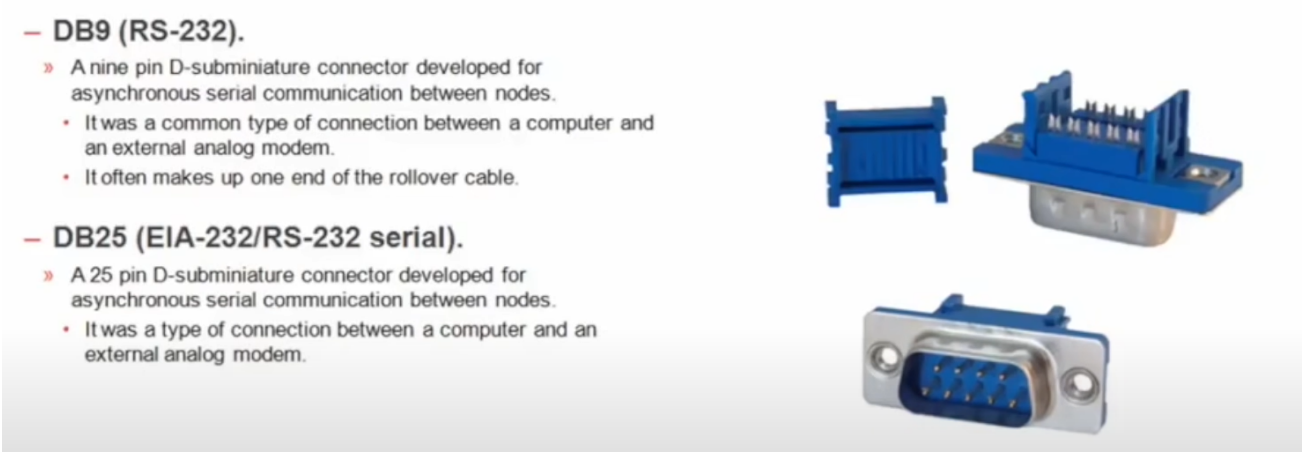
- twisted pair cables: standard in the modern LAN
    - composed of 4 pairs of wires contained within an insulating sheath. Each pair of wires is twisted together to reduce electromagnetic interference (EMI). The twist rates differ between the pairs of wires to reduce crosstalk between the pairs. The color are: w o/orange, w b/blue, w g/green, w b/brown.
- **unshielded vs. shielded twisted pair (UTP vs. STP)**
    - STP: has an additional shield that is either wrapped around each pair of wires or around all four pairs
        - reduce EMI and crosstalk, but more expensive
- **Plenum vs. non-plenum twisted pair**
    - most twisted pair is non-plenum grade
    - builing codes often call for plenum grade cable to be run in plenum spaces (areas designed to assist in the airflow of a building for HVAC purposes)
        - jacketed in either a fire-retardant cover or in a low-smoke PVC jacket
        - polymer or nylon strand woven into the cable to help take the weight of hanging cables and reduce the chance for cable to stretch --> cause the pair inside to break

- twisted pair is either a **straight-through cable **or a **crossover cable**, it can also be used to **create a rollover (console) cable**
    - **straight-through cable**: used to connect different types of devices together (cmp to sw, or sw to router)
    - **crossover cable**: connect similar devices together (PC to PC, or sw to sw)
    - rollover or console cable: required to connect to the console port on a sw or router. It is common for one end of the rollover cable to use an RJ45 connector, the other end use RS232 connector.

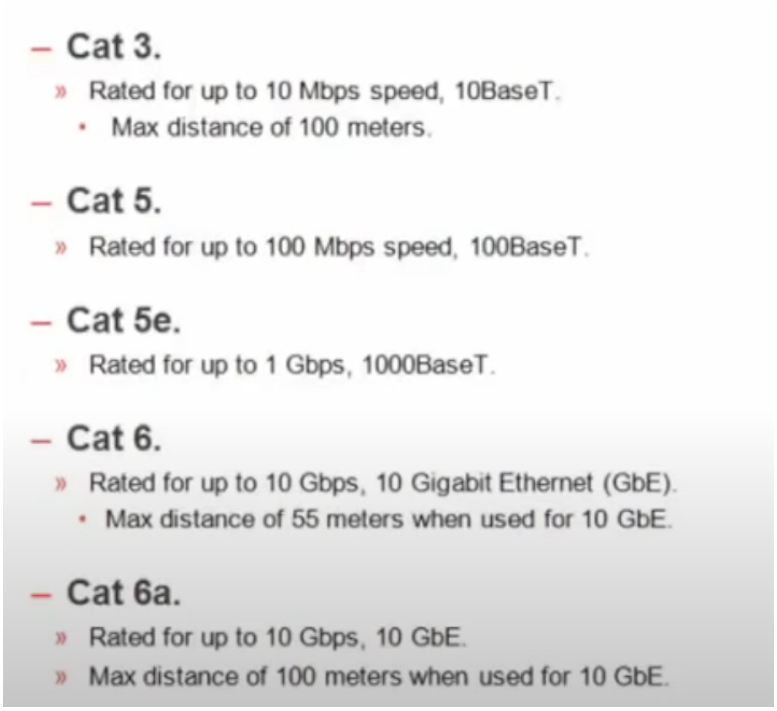
Twisted pair network connectors

- 

- 

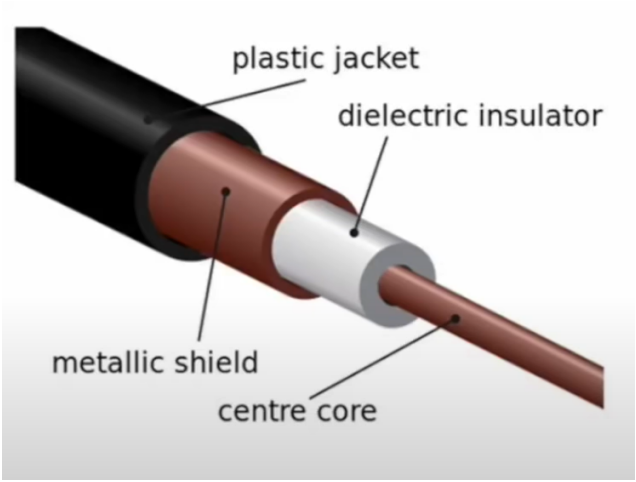
- 

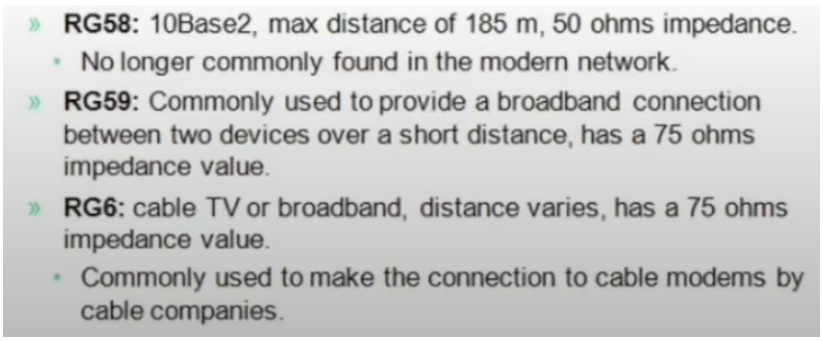
Categories of twisted pair

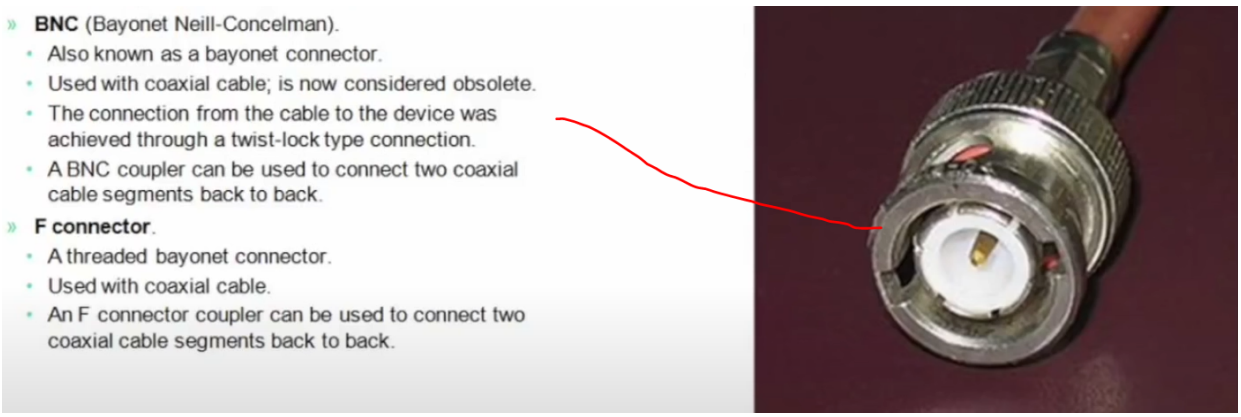
- 

Coaxial cabling

- one of the oldest ethernet cabling standards
- has been used for baseband (carries single digital signal)
- used for broadband (carries multiple digital signals)
- the inner metal mesh or foil layer helps to protect against EMI

- 

- coaxial cable types
  - 
    - **RG58:** 10Base2, max distance of 185 m, 50 ohms impedance.
      - No longer commonly found in the modern network.
    - **RG59:** Commonly used to provide a broadband connection between two devices over a short distance, has a 75 ohms impedance value.
    - **RG6:** cable TV or broadband, distance varies, has a 75 ohms impedance value.
      - Commonly used to make the connection to cable modems by cable companies.

- coaxial cable connectors
  - 
    - **BNC** (Bayonet Neill-Concelman).
      - Also known as a bayonet connector.
      - Used with coaxial cable; is now considered obsolete.
      - The connection from the cable to the device was achieved through a twist-lock type connection.
      - A BNC coupler can be used to connect two coaxial cable segments back to back.
    - **F connector**.
      - A threaded bayonet connector.
      - Used with coaxial cable.
      - An F connector coupler can be used to connect two coaxial cable segments back to back.

Fiber optic cabling

- relatively expensive and harder to work with
- not common in LAN env
- <u>resist all form of EMI and cannot be easily tapped</u>
  - harder to eavedrop

- can cover long distances at hight speed
- designated by fiber type, cladding size and jacket size
- the type of connector used on fiber optic cabling can impact the performance of the transmissions
    - UPC (Ultra physical contanct) connector
    - APC (Angled physical contanct) connector: better performing connector
- Fiber Types
    - **multimode fiber (MMF)**
        - use an infrared LED system to transmit the light
        - use multiple rays of light going down the cable
        - used for shorter fiber runs, under 2km
        - less expensive to implement than SMF
        - most common application in networking is MMF 62.5/125u
    - **single-mode fiber (SMF)**
        - use a laser-diode arrangement to transmit the light
        - use a single ray of light transmitted down the cable
        - used for longer runs that require high speed
            - traverse 40+ km
- Fiber optic cabling connectors

- **SC.**
  - Subscriber Connector, or Square Connector, or Standard Connector (Stick and Click).
  - A push-pull type of connector.
- **ST.**
  - Straight Tip (Stick and Twist).
  - A twist lock type of connector.
- **LC.**
  - Local Connector, or Lucent Connector, or Little Connector.
  - A type of connector that uses a locking tab to secure the connection.
- **MTRJ.**
  - Mechanical Transfer Registered Jack.
  - A small form factor connector that contains two fibers and that utilizes a locking tab to secure the connection.
- Fiber optic coupler.
  - Used to connect two fiber optic cables back to back.

Media converters

- common to see a nw contains more than one type of cabling
  - need to connect different types of media together
- media converter
  - common to connect: SMF to ethernet, MMF to ethernet, SMF to MMF, fiber to coaxial cabling

Cabling tools

- **Crimpers.**
  - Used to place cable ends on cables.
    - They can be designed to work with a single type of cable or with multiple types.
- **Wire strippers.**
  - Used to remove the insulating cover on wires and cables.
    - Many are designed to just cut through the insulation without damaging the cable contained in the insulation.
    - Some are also designed to cut all the way through the cable, so that excess cabling can be trimmed.
- **The punchdown tool.**
  - Used to secure cable wires into punchdown blocks. Good ones will trim the ends at the same time.
    - In many cases, punchdown blocks are used to terminate cable runs in a central location. Often, these blocks are on the backside of patch panels.

The cable tester.

- Used to test cables for common problems.
  - Misconfiguration of the pinouts.
  - The cable standard used (T568A or T568B).
  - Shorts or breaks in the cable.
  - Some types of testers can also test for cable length and quality (these are called **cable certifiers**).

TDR (time-domain reflectometer).

- A cable tester for copper cabling that can also determine the length of a segment and the electrical characteristics of the cable.
- They can also tell where a break is in a segment.
  - More expensive than a standard cable tester.

OTDR (optical time-domain reflectometer).

- Performs the same functions as a TDR, but used for fiber optic cabling.