Computer Networking Course - Network Engineering (CompTIA Network+) Part 2

Network Topologies

What is a topology?

- a "map" that can describe how a network is laid out or how the nw functions
- can be described as either **logical or physical.**
    - logical: theoretical signal path
    - physical: physical layout of the nw

Peer-to-peer vs. client/server

- These are (not) topologies.
    - they don't describe signal path or the physical layout of the nw
    - they describe how the nw functions
- **peer-to-peer topo**
    - nodes control & grant access to resources on the nw
    - each node is responsible for the resources it is willing to share
- **client/server topo**
    - nw resources access is controlled by a central server(s)
    - a server determines what resources get shared, who is allowed to use the resources and even when the resources can be used
- **hybrid topo**
    - combination of two

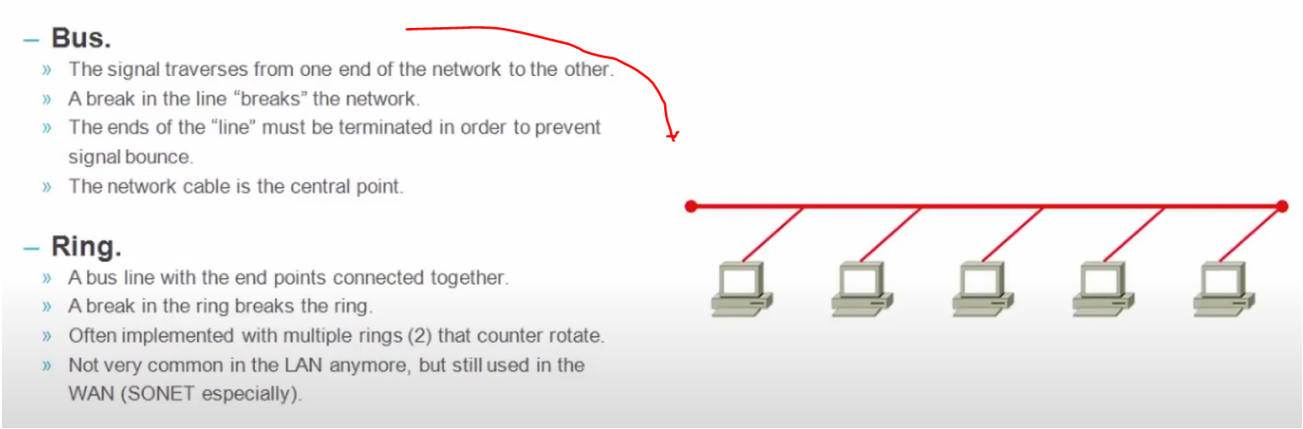
Network topology models

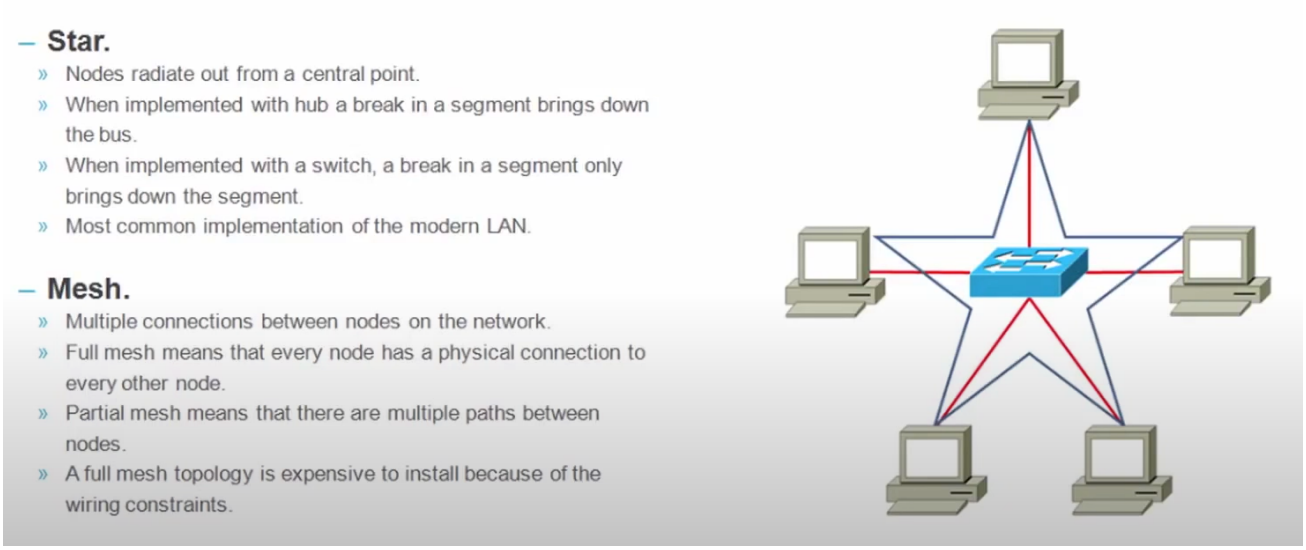
- the original ethernet standards established a "bus" topo for the nw, both logically & physically

  - "bus" topo: end2end, from one direction to the other direction and come back

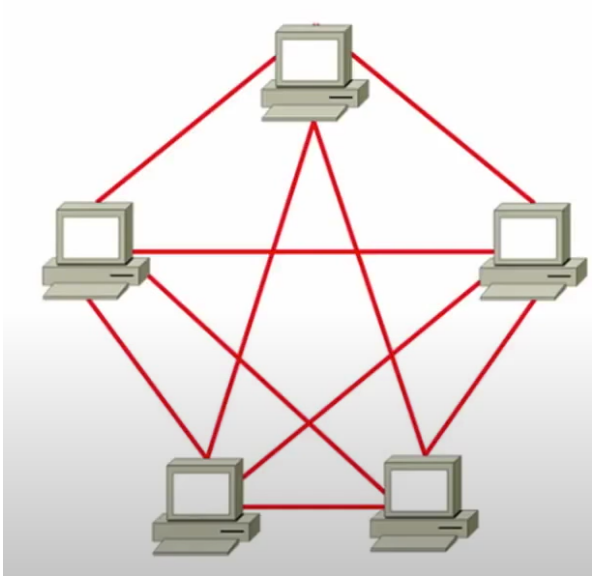
  - development of different physical topo, logical topo remained the same to maintain backward compatibility.

  - when discussing Ethernet nw: logical topo is always a "bus" topo while the physical topo can be different

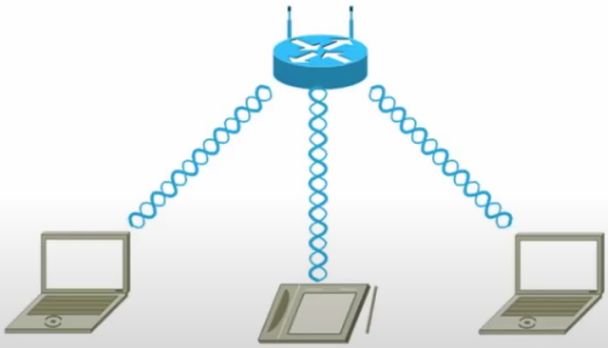
- 

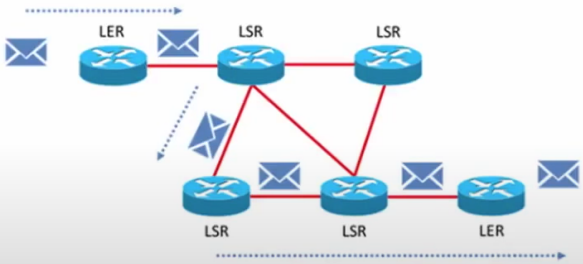
- 

  - Mesh:

- 
- – **Point-to-point.**
  - » Two nodes or systems connected directly together.
  - » Two PC connected with a crossover cable create a point-to-point topology.
  - » No central device is required to manage the connection.
  - » A common topology when implementing a WAN connection.

  – **Point-to-multipoint.**
  - » A central device that controls the paths to all other devices.
  - » Differs from a star in that the central device is intelligent.
  - » Wireless networks often implement point-to-multipoint topologies.
  - » When the WAP sends, all devices on the network receive the data, when a device sends it message is only passed along to the destination.
  - » Also a common topology when implementing a WAN connection.

  
- – **MPLS.**
  - » Multiprotocol Label Switching is a topology used to replace both Frame Relay switching and ATM switching.
  - » It's a topology because it specifies signal path and layout both.
  - » It is used to improve the QoS and flow of network traffic.
  - » Label edge router (LER): adds MPLS labels to incoming packets if they don't have them.
  - » Label switching router (LSR): forwards packets based on their MPLS labels.

- ring=bus with the ends connected
- star=nodes radiate out
- mesh=multipath
- p2p=direct connection

- p2multipoint=central control

Network infrastructure implementations

Design vs. function

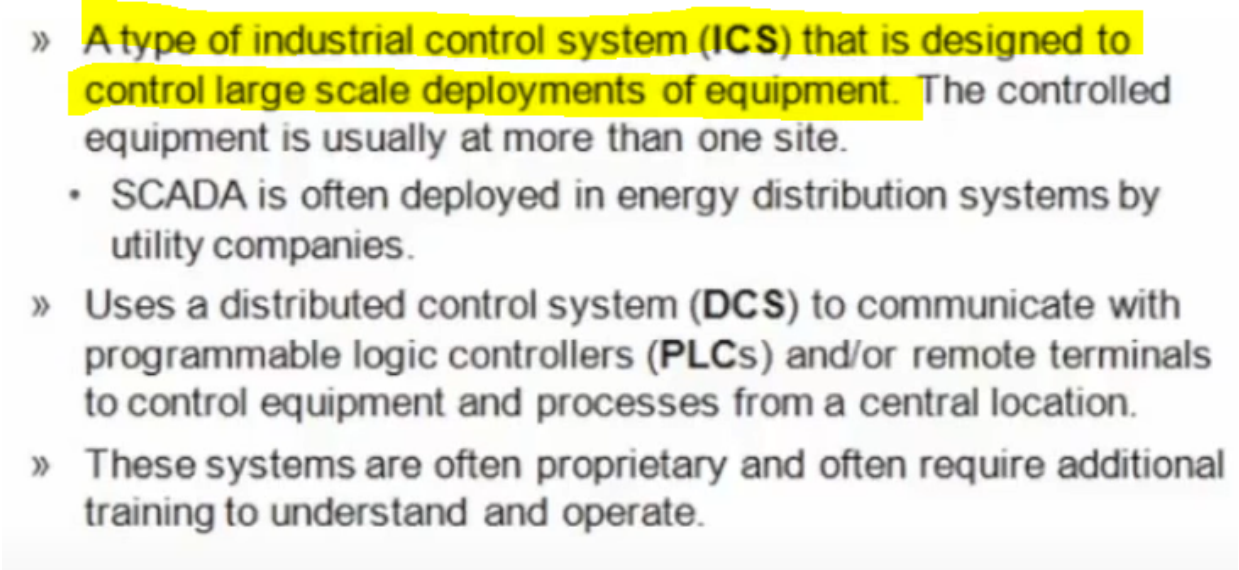
- if describe the nw's design, then the first place to start is to describe its topo
- if describe the nw's function, then the first place to start is to describe its category or infrastructure implementation

Categories of networks

- **Local Area Network (LAN)**
  - most LANs are encompassed by single nw addr range
    - the addr range may be broken into subgroups
    - each of these subgroups is called a **virtual LAN (VLAN)**
  - LANs can span from a small area to a builging or a small group of buildings
  - tend to be high speed
  - most common type of nw found in LAN: 802.3 (Ethernet) and 802.11 (wireless LAN) WLAN
- **Metropolitan area network (MAN)**
  - larger than a LAN
  - contain multiple LANs
  - often owned by municipalities
  - it sometimes called a **campus area nw (CAM)** when is owned by a private entity
- **Wide area network (WAN)**
  - spans significant geographic distances
  - a nw of nws
  - best example is the Internet

- if the all of the infrastructure implementation has a single owner, then it is not a WAN

- **Personal area network (PAN)**
  - extremely distance and size limited
    - often a connection between only 2 devices
  - common examples:
    - **Bluetooth**: ~ between a keyboard and computer
    - **IR (infrared)** connection between a smartphone and a printer
    - **NFC (near field comm)** between a smartphone and a payment terminal
  - tend to provide low throughput of data and have a low power output
    - throughput decreases when the distance between devices increases

- **Supervisory control and data acquisition (SCADA)**
  - 

- **Medianet**
  - nws designed and implemented specifically to handle voice and video
  - to remove QoS issues (e.g., latency and jitter) that can occur in other infrastructures
    - e.g., video teleconference (VTC) nw
  - may be implemented as its own infrastructure or as a sub-infrastructure

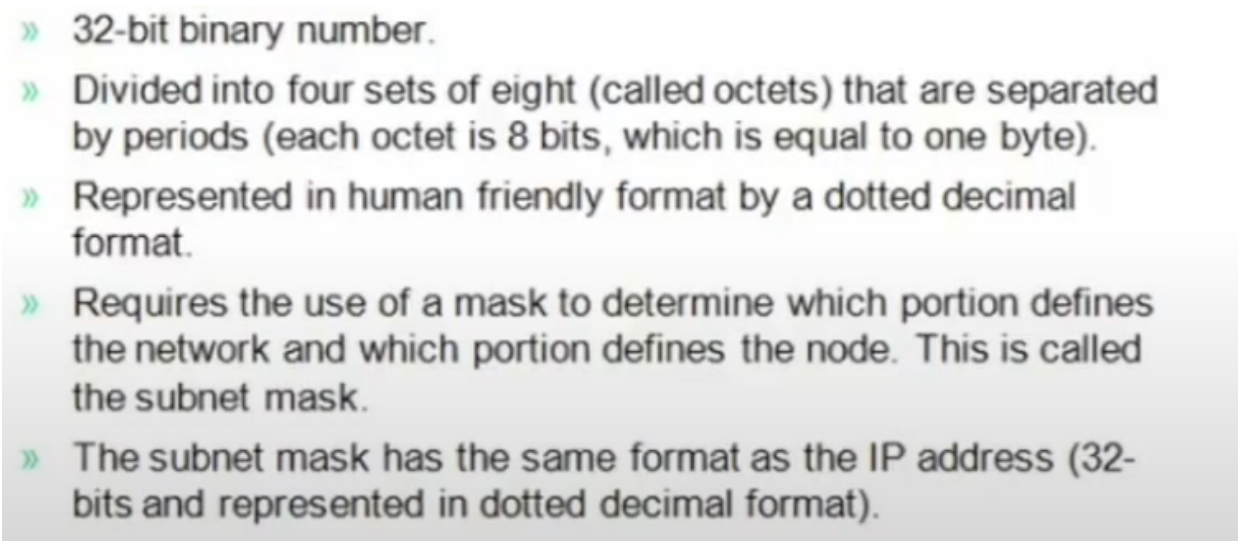
Introduction to IPv4

- IP addresses are the location of the PC or server, identified as both nw location and host location within that nw

Purpose of IP addressing

- provides a logical addressing scheme for our computers so that they can communicate on nws.
    - being logical means that an IP addr can be changed within minimal fuss at any time, unlike a MAC addr which is physically embedded into devices

IPv4 address properties

- 32-bit binary number, 2^32 possible addr combinations
- to keep everything neat and tidy and findable: implementation of subnet mask
    - used to determine nw and node/host portions of the IP addr.
- convert binary to decimal
- initial properties of IPv4
    - 

- **Interaction of IP address and subnet mask.**
  - 192.168.1.9 255.255.255.0
  - 192.168.1.9 = the IP address.
  - 255.255.255.0 = the subnet mask.
- **Deconstructing the IP address.**
  - First octet = 11000000 = 192
  - Second octet = 10101000 = 168
  - Third octet = 00000001 = 1
  - Fourth octet = 00001001 = 9
- **Subnet mask characteristics.**
  - Anything other than a 0 defines the network address.
- **Network address.**
  - The network address = 192.168.1
- **Node address.**
  - The node address = 9

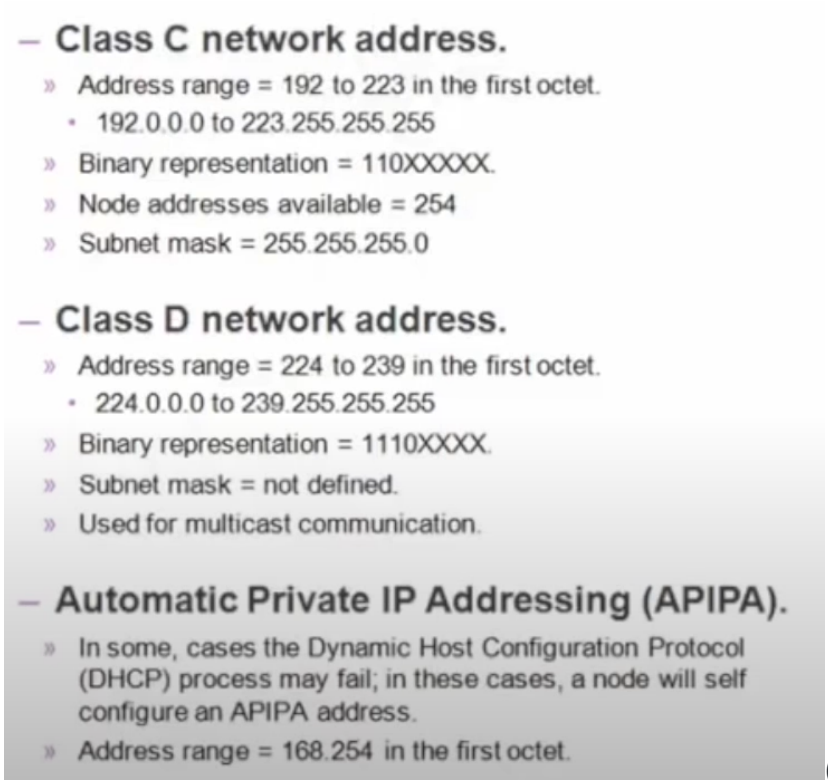
192.168.1.9
255.255.255.0

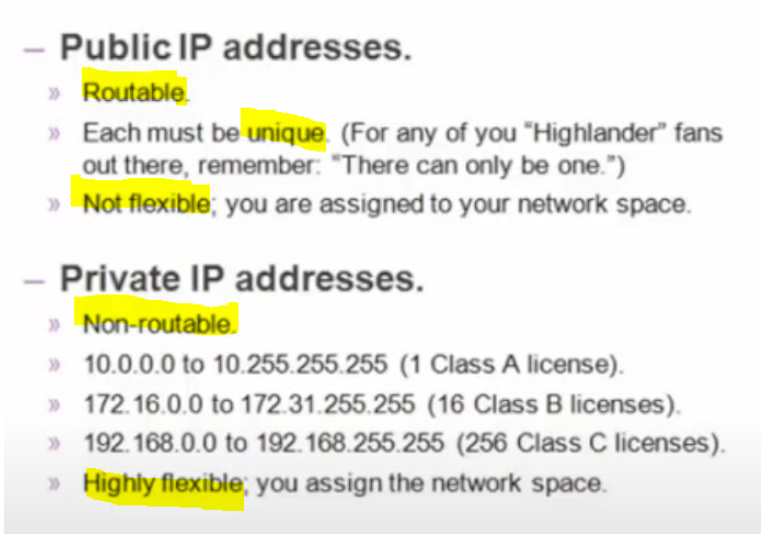
11000000.10101000.00000001.00001001
-
11111111.11111111.11111111.00000000
=
00001001

Classes of IPv4 addresses

- run out of assignable IPv4 addr

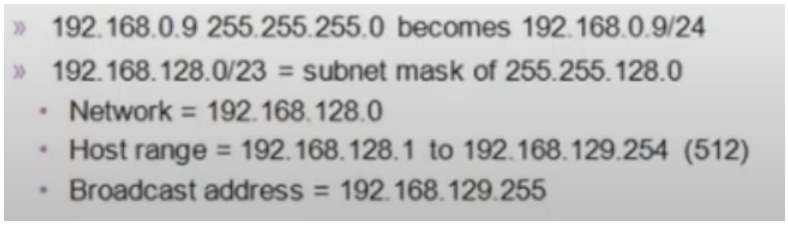
- **Class A network address.**
  - Address range = 0 to 127 in the first octet.
    - 0.0.0.0 to 127.255.255.255
  - Binary representation = 0XXXXXXX.
  - Node addresses available = 16,777,214
  - Subnet mask = 255.0.0.0
- **Class B network address.**
  - Address range = 128 to 191 in the first octet.
    - 128.0.0.0 to 191.255.255.255
  - Binary representation = 10XXXXXX.
  - Node addresses available = 65,534
  - Subnet mask = 255.255.0.0

- 

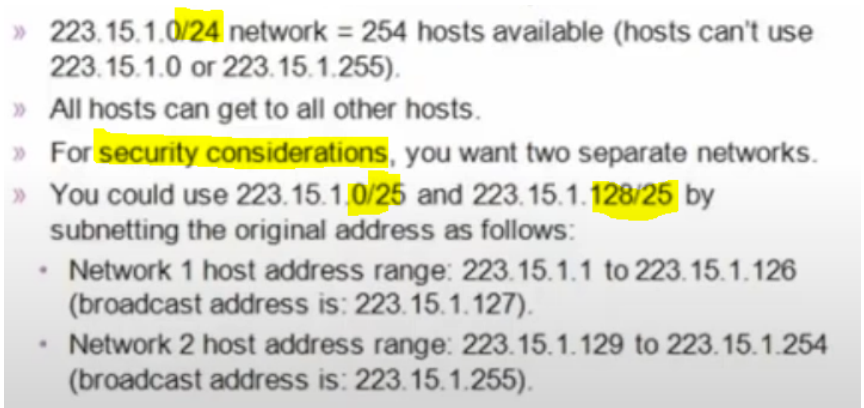
(APIPA)
- 

Classless of IPv4 addressing

- classes of addr limit flexibility
  - first routing protocols requires the class structure
- classless addressing
  - **classless inter-domain routing (CIDR)**
  - slow the growth of routing tables

    - slow the exhaustion of IPv4 addr
    - create more flexbility
        - fluid subnet mask
    - not affect the private addr space ranges
    - subnetting is possible and desirable
- CIDR notation
    - 

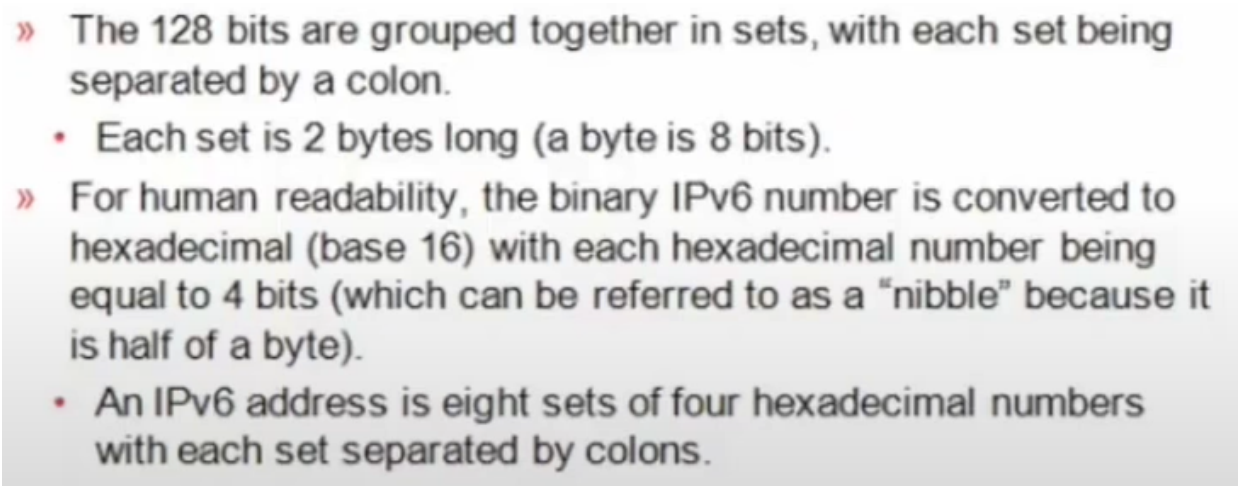
Subnetting IPv4 addresses

- subnetting cuts the addr space into smaller pieces
    - create flexibility in nw design
    - create efficiency in addr space utilization
- small office nw example
    - 

Introduction to IPv6

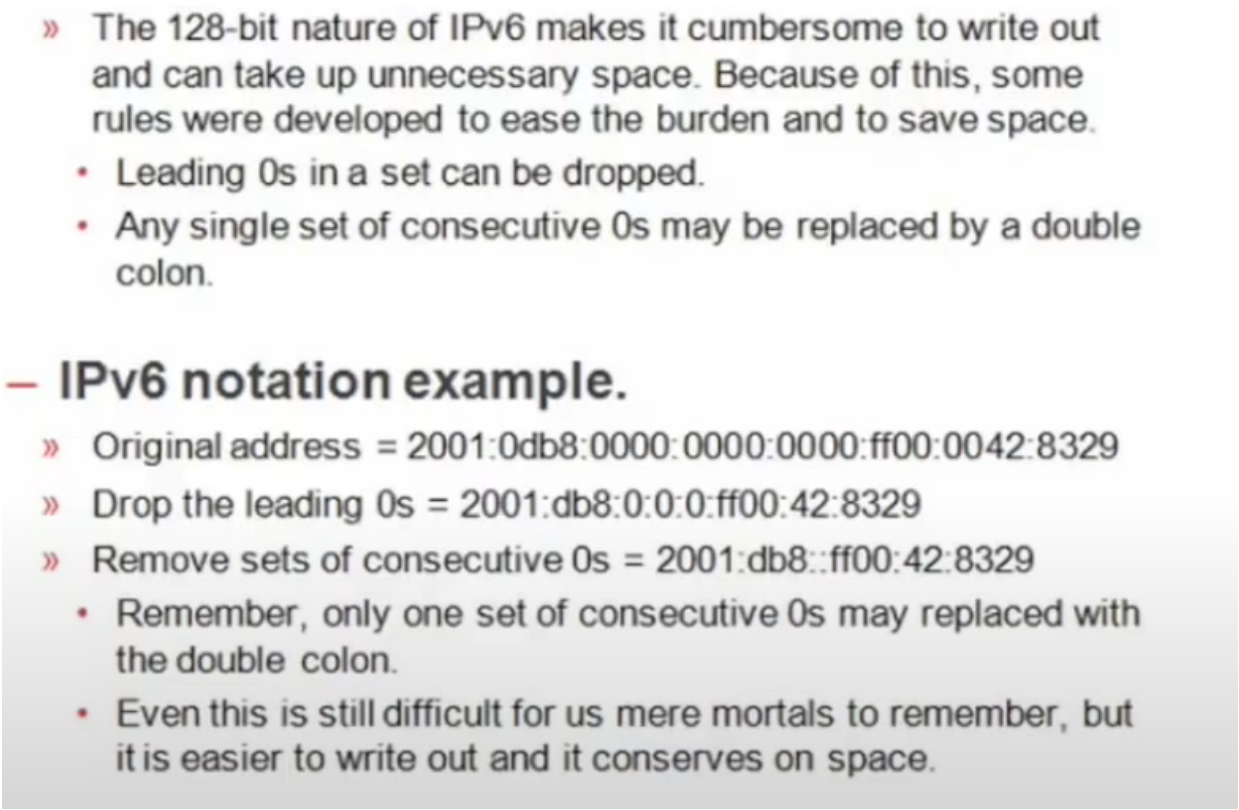
- Internet Assigned Numbers Authority (IANA)

IPv6 address structure

- works at L3 of the OSI model
    - L3: major focus is logical nw and host addressing
    - IPv6 provide logical nw and host addresses to devices
- 128-bit binary addressing scheme
    - 

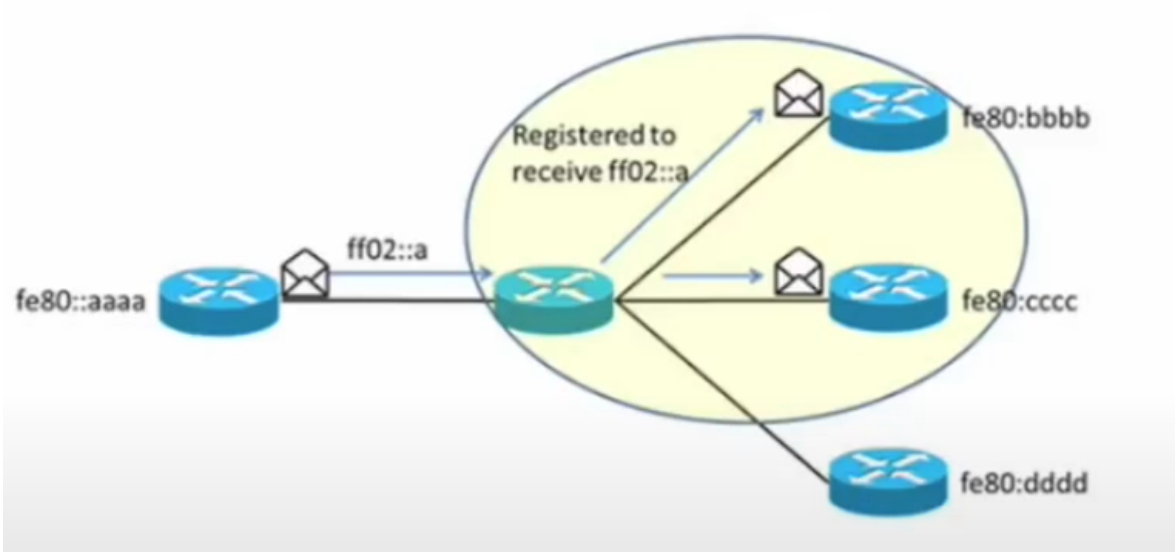
- **IPv6 local addr structure**
    - the first 64 bits represent the local nw, the last 64 bits represent the host
        - the local addr structure follows the Extended Unique Identifier (EUI) format EUI-64. The 48-bit MAC addr is padded with 16 bits to make it 64 bits in length
    - the local addr is called the ** **link local addr****, and always begins with **fe80**
- **IPv6 global addr structure**
    - last 64 bits is host addr
    - nw portion is composed of the routing prefix and subnet
        - follows CIDR convention
        - the subnet is composed of the bits between the prefix and the EUI-64 host addr
    - global IPv6 addr always begin in the range of 2000 to 3999.
- the need for DHCP has been eliminated in most cases
    - when implemented, IPv6 will auto-configure both the local and global addr. When a device first comes online, it will us **neighbor discover protocol (NDP)** to discover what

the required nw addr are, both local and global. This allows the device to configure its own IPv6 addr.

- IPv6 notation
  - 

IPv6 nw transmissions

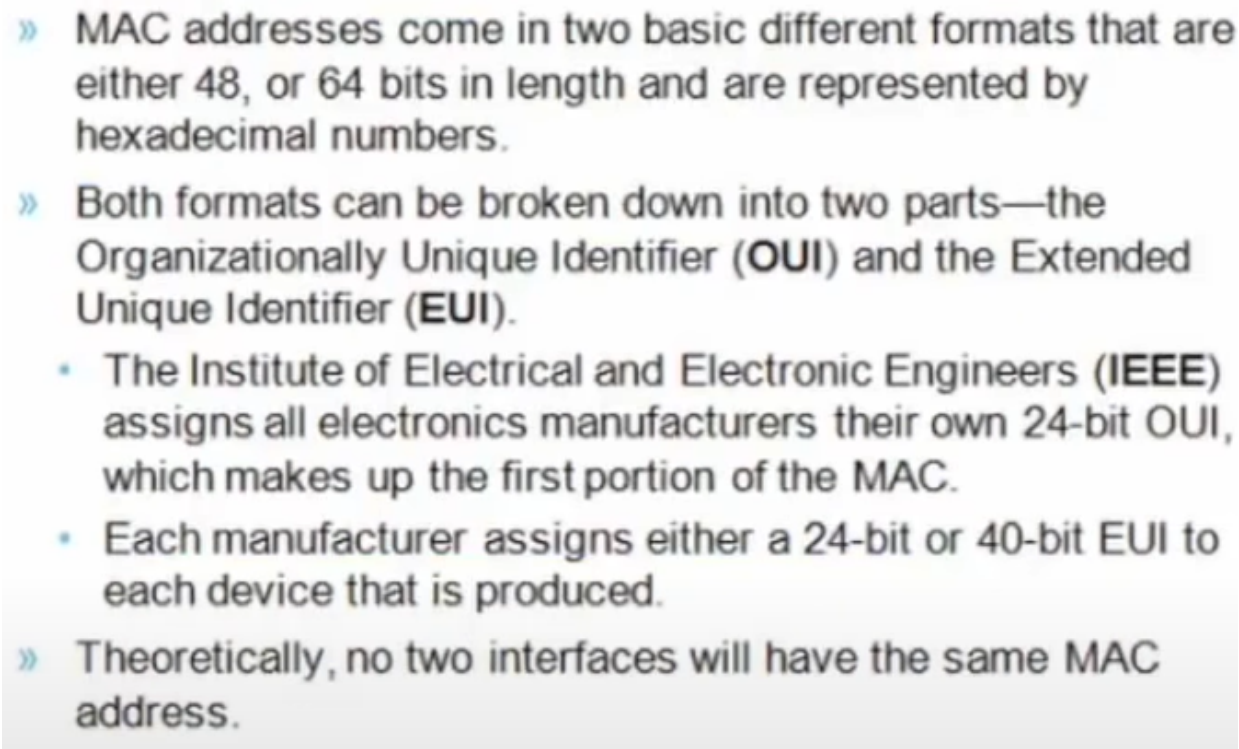
- **unicast**: 1-to-1 communication
  - can occur on the local nw (fe80) or the global nw (2000 to 3999)
- **multicast**: 1-to-few comm
  - routers register to receive multicast transimissions that involve the routing protocols they are programmed to use
    - multicast addr always begin with an **ff**

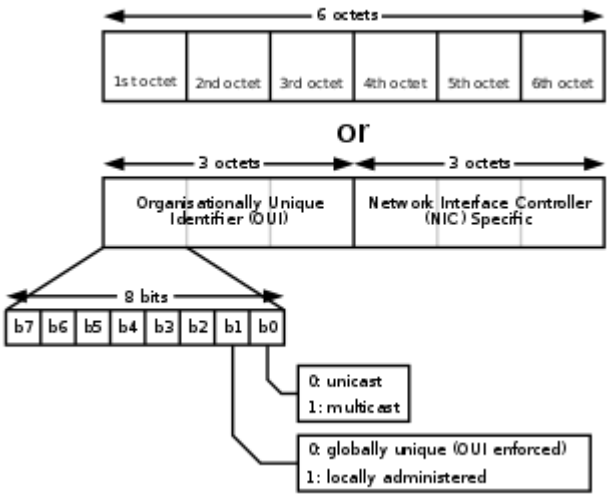
- 

- **anycast**: 1-to-the-closest
  - the router only sends the comm to the closest one
  - involves implementing DHCPv6
- **DHCPv6**
  - **IPv6 is capable of auto-configuring its own local and global addr**
    - in certain situations, that is not always desirable
  - DHCPv6 can be configured to hand out specific IPv6 addr when necessary
  - useful for when load balancing a nw, or for when nw redundancy has been created
- IPv6 and IPv4
  - **dual stack configuration**
    - the nw and devices on the nw receive both an IPv6 and IPv4 configuration
  - **tunneling**
    - **6-to-4**: used to encapsulate v6 data packets in and v4 datagram, allowing v6 packets to travel across or through all v4 nws
      - also called **Teredo tunneling**

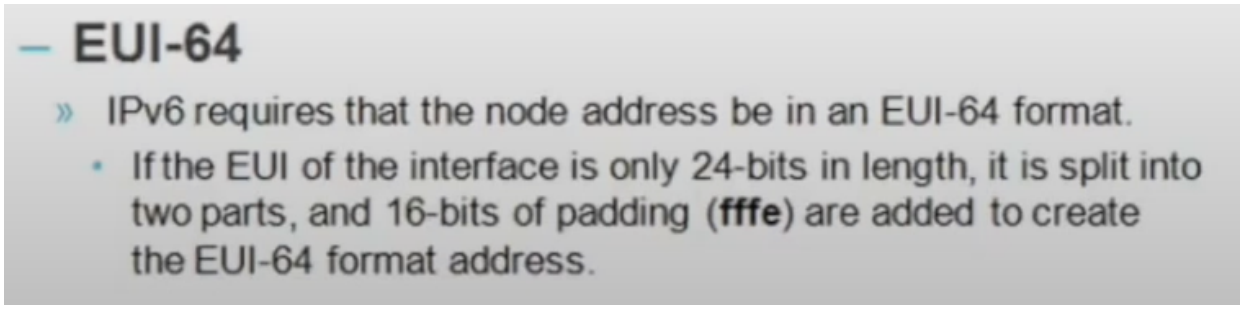
Special IP networking concepts

The media access control address (MAC)

- ***MAC addr: all nwing interfaces come with a special addr already configured ***
    - often referred to as the ** **physical addr**** or the burned in addr of the interface. It is set by the manufacturer and never changes.
    - switches and other open systems interconnection (OSI) **L2** devices rely upon the MAC addr in order to get nw packets to the correct destinations.
- MAC addr format
    - 

    - 

      (from wiki)

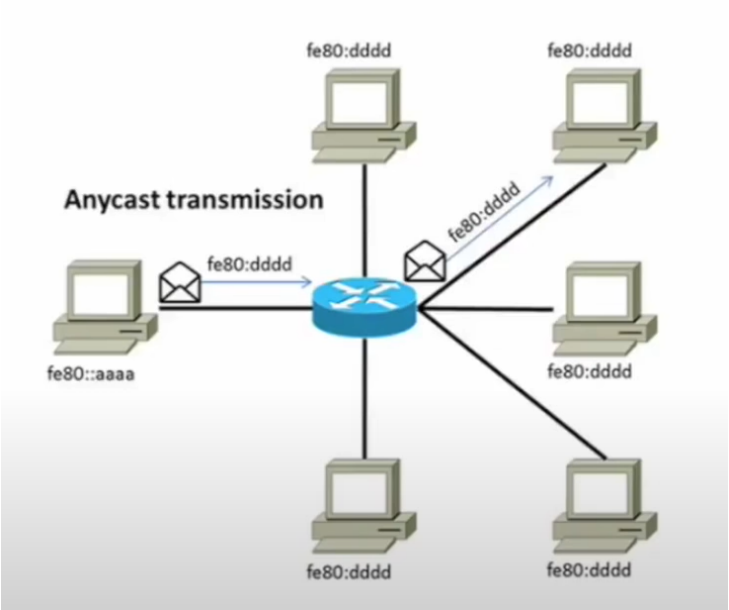
- 

Collision domains vs. broadcast doamins

- **Ethernet nws** use a tech called **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** when transmitting data.
  - with this, a device listens to the carrier signal on the nw media. If no other device is transmitting, the device is free to send data. If another device sends data, a collision is posiible. The devices listen for collisions, and will stop transmitting and wait a random period of time before attempting to transmit again.
- **Collision domains**
  - an area of the nw where nw packets can collide.
    - a collision can occur when 2 devices send packets at the same time
    - collision domains are broken up by switches, bridges, and routers
    - are not broken up by hubs
- **broadcast domains**
  - defined as all the nodes that can be reached by a broadcast transmission
    - all nodes that can be reached reside in the same nw
  - the domain cannot pass routers, so the domain is also defined by the subnet mask
- special notes
  - technically, v6 does not use broadcast transmissions
    - *v6 utilizeds multicast instead of broadcast transmissions *

Types of nw transmissions

- types of IPv4 nw transmissions

    - unicast: 1-to-1
    - muticast: 1-to-few (a specific src addr transmissions going to a set of registered dest addr)
    - **broadcast**: 1-to-all (to all addr on the local nws)
- types of IPv6 nw transmissions
    - unicast
    - multicast
    - **anycast**: 1-to-closest
        - going to a specific v6 addr that has been assigned to multiple devices. The router uses an algo to determine which MAC addr is the closest and only that device receives the anycast trans.
        - 

Introduction to routing concepts

Purpose of routing

- purpose: to connect different nws together to allow them to communicate and pass data traffic.
- routing protocols are how nws determine where to send nw traffic. They build routing tables to direct nw traffic.

Basic routing concepts

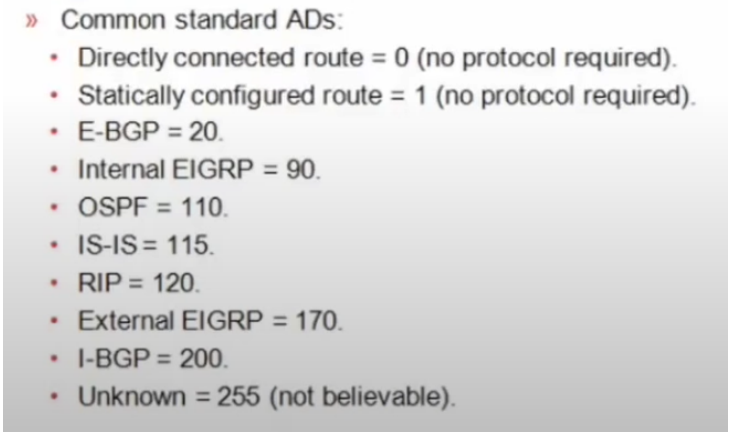
- **Static routing**
  - uses administrator defined routes
  - each router must contain the route
  - easy to set up (in a small nw)
    - not easy to maintain
- **Dynamic routing**
  - routers use protocols in order to determine the best route between 2 nws
  - admin determines which protocols will be in use
  - the routers must all use the same protocols
    - exception: route redistribution
  - routing protocols can be stacked within a router
- **the default route**
  - the direction that a router will send nw traffic when there is no known route in the routing table
    - assigned by an admin
    - usually a designated interface on the router or designated next hop interface
- **the routing table**
  - list of known routes to all known nw from the router's perspective
    - is established by an admin when static routing is used
    - dynamically built by routing protocols when dynamic routing is used
  - each routing protocol maintains a routing table
- **Loopback interface**
  - an administratively configured logical number assigned to a router to ease administrative functions or routing processes

        - often, the loopback interface is assigned in an IPv4 addr format
    - the interface may be completely logical, or a physical interface may be assigned to be the loopback interface.

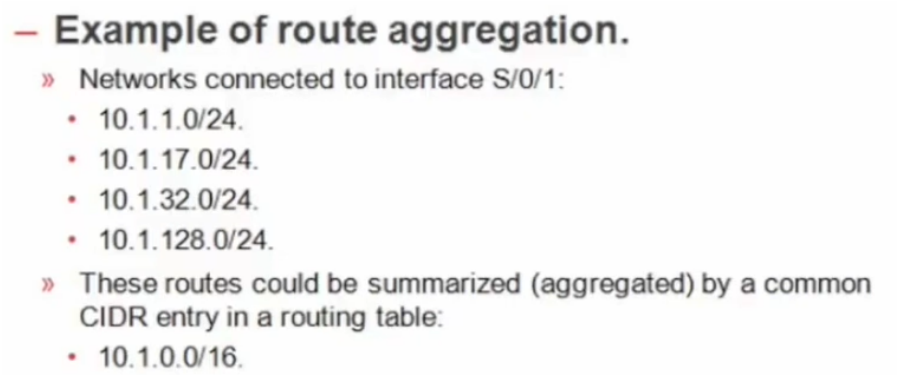
- **Routing loops**
    - a possible problem that can be created if interconnected routers have a breakdown in their routing algo
        - when a routing loop occurs, the nw keeps looping through the routers until some system or mechanism breaks the cycle.
        - they can create nw congestion or even bring down a nw
    - routing protocols use multiple methods to prevent loops from occuring
        - the time to live (**TTL**) field is also utilized to stop routing loops after they have occured.

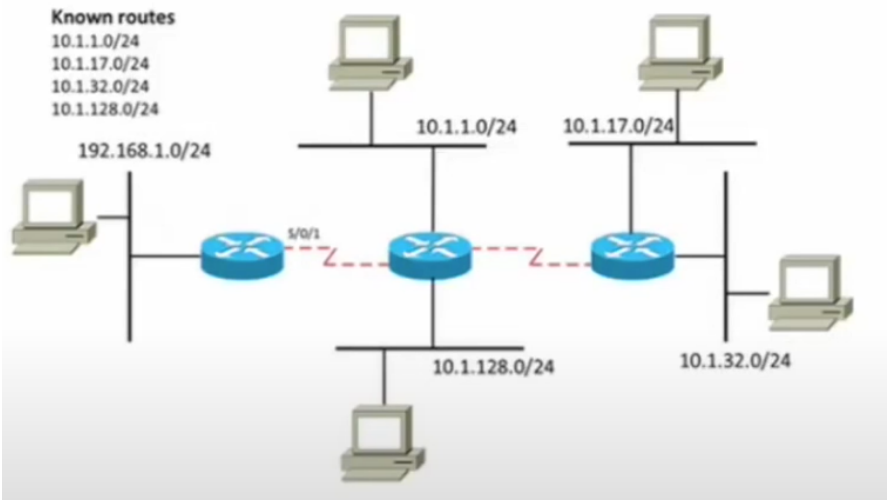
Routing metrics

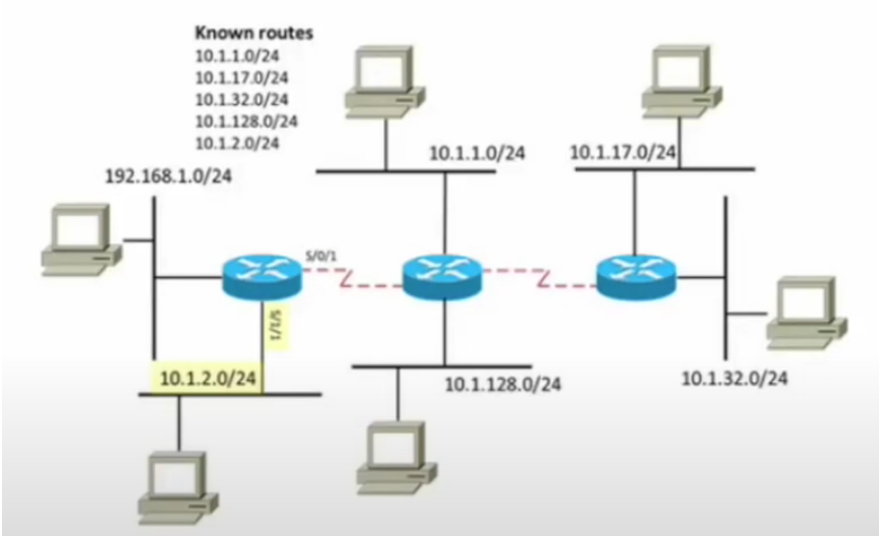
- There may be more than one route available to a remote nw. **Routing protocols use metrics to determine which route is the best to use**.
- the same basic metric may be used by different routing protocols. When this occurs, the metric is usually implemented in a different manner through the use of different algo.
- metrics
    - **Hop count**
        - the number of routers between two end points
    - **Maximum transmission unit (MTU)**
        - the max allowed size of a packet, measured in bytes
        - packets excced the MTU must be fragmented into small pieces, leading to more packets, and slower connection
    - **Bandwidth**
        - the speed of the nw connection (in Kbps, Mbps, or Gbps)
    - **Latency**

        - measure of time that a packet takes to traverse a link
    - **Administrative distance (AD)**
        - the believability of a routing protocol's advertised routes
            - different routing protocols are considered to be more trustworthy than others
        - routers use the AD to help determine which routing protocol to use when more than one protocol is installed on the router
        - the **lowest AD** of an advertised route will determine the protocol use
        - 

Route aggregation

- It is a process used by nw admin to **condense the size of routing tables**. They do so through the use of **CIDR** to summarize routes to different nws.
- 

- 

- route aggregation takes careful planning during the nw design phases
    - the above example would not work if interface S/1/1 on the same router was connected to nw 10.1.2.0 (non-contiguous nws)
    - 

High availability

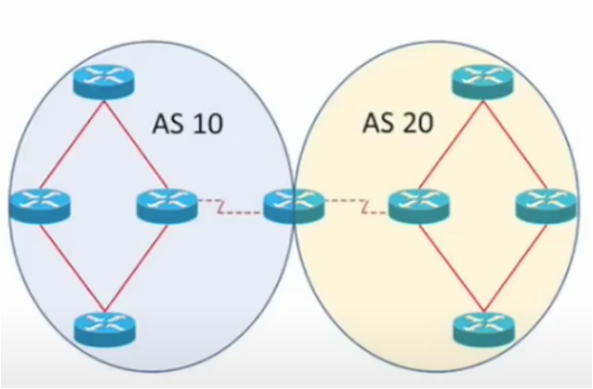
- Part of a nw admin's job is to ensure that nws reamin up and active for the max amount of time.
- to ensure nw don't go down, admins oftern **remove single points of failure**
- **single point of a failure** in a nw is the point where a single failure will casue the nw to cease functioning. nw admin oftern use high availability tench to remove them. An example of a high availability tech is the use of redundant links to outside nws.
- **Hot Standby Router Protocol (HSRP)**

    - a proprietary cisco method of creating a **fault tolerant link** using 2 or more routers with connections **outside of the local subnet**.
        - the 2 routers are connected together as well as having connections outside of the local nw
        - a **virtual IP addr** is created and shared between the routers
        - devices on the nw are configured to use the virtual IP addr as the default gateway for pakcets leaving the nw.
        - if a router goes down, the link outside the nw is still available
- **Virtual Router Redundancy Protocol (VRRP)**
    - is an **IETF (Internet Engineering Task Force) standard** that is similar in operation to HSRP.

Introduction to routing protocols

Interior vs. exterior gateway routing protocols

- **Interior gateway protocol (IGP)**
    - a category of protocols used within **autonomous nws**.
        - used between nws that you can control
    - the most popular IGP protocols are **OSPF** (Open Shortest Path First) and **RIPv2** (Routing Information Protocol version 2)
    - Note: **IS-IS** is popular with extrememly large autonomous nws like an **ISP**'s (internet service provider) nw.
- **Exterior gateway protocol (EGP)**
    - used between **non-autonomous nws**
        - used between nws under separate control
    - **BGP** (Border Gateway Protocol) is the most popular
- Autonomous nws: organizations have more than one nw that are routing traffic between

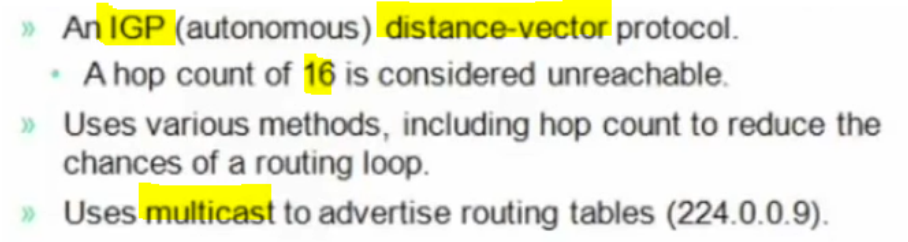
- some IGP routing protocols use an admin defined **autonomous system (AS) number** as one means of identifying which nws can directly communicate with each other.
- AS is not a metric, but a means of identifying a nw that might possible accept another nw's traffic.
- AS is only significant within autonomous nws and has no relevance outside of them.
- 

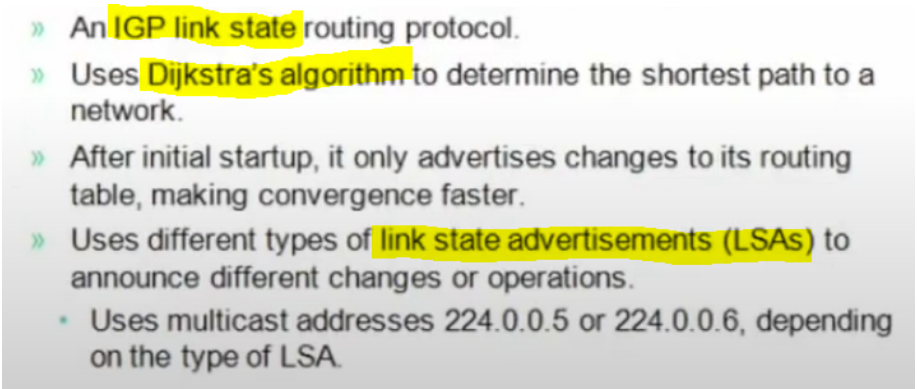
More routing concepts

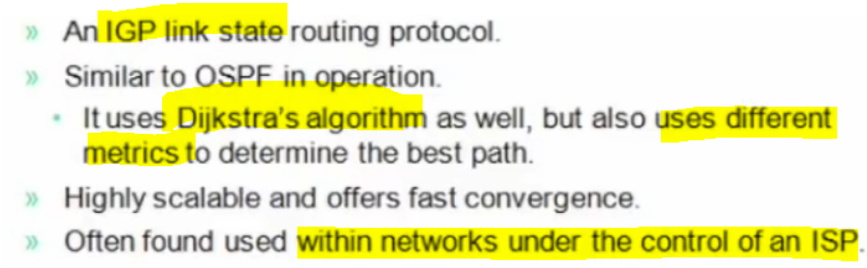
- Classification of routing protocols
  - IGP and EGP routing protocols can be broken out into 3 other catergories of protocols, which is designated by their main method of determing routes between nws.
  - **Distance-vector** routing protocols
    - routes are determined by how many routers exist between the src and dst.
    - Periodically, the whole routing table is broadcasted
  - **Link State** routing protocols
    - metrics are used to determine the best possible route between dsts. The protocol then only monitors the state of directly connected links and only makes changes when changes to links occurs.
    - only changes in link status are broadcasted.
  - **Hybrid** routing protocols
    - use aspects of both the distance vector and link state routing protocols.
- **Next hop**
  - next router in the path between 2 points

- **Routing table**
    - the database table that is used by a router to determine the best possible route between 2 points
- **Convergence (steady state)**
    - the amount of time that is takes all the routers in an AS to learn all the possible routes within that sys.
        - faster convergence times are desirable.

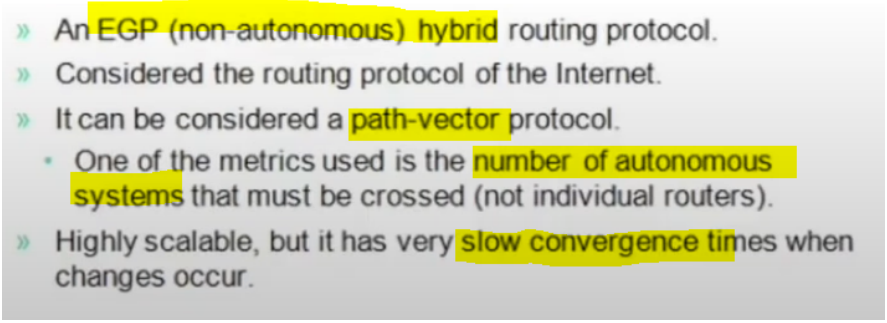
Routing protocols

- **Routing Information Protocol v2 (RIPv2)**
    - 

- **Open Shortest Path First (OSPF)**
    - 

- **Intermediate System-to-Intermediate System (IS-IS)**
    - 

- **Border Gateway Protocol (BGP)**



- **Enhanced Interior Gateway Routing Protocol (EIGRP)**
  - an advanced **distance-vector (hybrid) IGP** routing protocol developed by Cisco.
  - fast convergence time
  - uses a **Neighbor Table (directly connected routers)** and a **Topology Table** to build its routing table. The protocol only announced changes to the routing table (on multicast addr 224.0.0.10) in order to reduce bw consumption.

Basic elements of unified communications

Unified communications (UC)

- UC is not encompassed by a single product or device. It is a growing category in enterprise nws.
  - is the set of products and services that attempts to provide a consistent single user interface and experience across different media types and devices.
  - allows a user to send a msg from one type of media and have that media received as a different type of media.
- **Unified communications devices**
  - **UC server**
    - specialized servers that are designed to implement UC solns in the workplace
  - **UC gateways**
    - a nw device that is designed to translate between different signaling methods(e.g., **VoIP**). Gateway will translate an analog PSTN voice signal into a signal that can be understood on the VoIP nw.
  - **other UC devices**

        - any devices that can be used in the implementation of a UC soln, may include VoIP phones, email sys, video conferencing, and instant messaging nws.

Unified communications concepts

- **Presence**
    - an indicator used to communicate the willingness or ability of a user to accept communication
        - common presence statuses include available, online, offline, busy and do not disturb
    - presence services are important in UC solns, as they will track individual users across multiple devices and nws in real time through the use of multicast transmissions.
        - once a comm session has been established, unicast nw transmissions are used.
- **Quality of service (QoS)**
    - are implemented to improve the UC by managing nw traffic
    - **class of service (CoS)**: a QoS tech used to manage nw traffic by grouping similar types of traffic and assigning a nw priority to that traffic. A 6-bit **differentiated services code point (DSCP)** is used in the IP header to establish the CoS.

Voice over IP

- one of the most common implementations in a UC soln. Through the use of a presence service, calls can be routed to the correct location.
- 2 important protocols used in VoIP are **Session Initiation Protocol (SIP)** and **Real-time Transport Protocol (RTP)**
    - **SIP**: has 2 purposes
        - is used to established a communication session between two end points.
        - once session is completed, SIP tears down the connection.
    - **RTP**: is used during the communication session as the transport protocol, helping to provide QoS to the end points.

Virtualization technologies

Hypervisors and Virtual Machine Managers

- hypervisor can refer to any of the software that is used to manage virtual machines.
    - does not need a host OS
- **VM managers (VMM)** requires a host OS such as Windows or Linux

Components of virtualization

- **Virtual desktops**
    - a VM that functions as a desktop
        - any modern OS can be run inside of the VM desktop
        - multiple virtual desktops may be hosted on, or from, a single host systems
- **Virtual servers**
    - a VM that functions as a server
        - any modern server OS can be used
- **Virtual switches, firewalls, and routers**
    - a VM that fulfills the functions of a switch, firewall or router
    - VF and VR are particularly effective when combined with virtual nw interface controllers (**NICs**) and VS to create virtual nws.
- It is important to consider how the virtual nw is going to pass traffic to remote nws.
    - A connection must be created between the host sys's physical NIC and the virtual nwing equipment to allow nw traffic to pass through (if there is a desire for nw traffic to pass beyond the host sys)

Software defined networking (SDN)

- **SDN** is the process of allowing the administration and configuration of a nw to be done dynamically
    - the administrator can use a front end program to make adjustments to the nw with SDN.

- it allow nw administrators to dynamically adjust nw performance without the need to log into each individual device that needs to be adjusted to achieve the desired performance

Storage area networks

Justifications for storage area networks

- dramatic decrease in the actual cost of data storage is one of factors leading to icnreased demand for data storage
- another factor is: the demand for the data to be available from anywhere and accessible from any device increased
- A **storage area nw (SAN)** can be a soln to the need for both storage capacity and high availability.
    - advantages of SAN
        - **scalability**: the amount of data generated is huge and need to be stored.
            - as storage needs increase, the capa of the SAN can be easily increased to meet them.
        - **data availability**: demand increased for data to be available at anytime from anywhere.
            - SAN are deployed as part of a cloud computing soln, thus increasing availability
        - **optimization**: the serviers can be optimized to run applications more efficiently as the requirements to store data are removed from application servers.
            - data storage is also optimized

SAN technology

- **Storage area nw (SAN**): an **acutal nw of devices** that have the sole purpose of storing data efficiently.
    - a SAN may contain multiple NAS devices.
- **nw attached storage (NAS)**: is a specifically designed nw appliance that has been configured to store data more efficiently than standard storage methods.

    - is a **data storage appliance that is placed on a nw**.
- **Fibre channel (FC)**
    - a high speed nw tech originally developed to operate over fiber optic cables only.
        - now have been modified to allow the use of copper cabling in conjuction with the fiber
    - **commonly used to connect SANs**
        - use **fibre channel protocol (FCP)** as its transport protocol to transmit **SCSI (small computer sys interface**) commands to storage devices.
- **Internet SCSI (iSCSI)**
    - an IP based nwing standard used to connect data storage facilities and SANs.
        - allows SCSI commands and processes to take place over long distances.
- **Jumbo frames**
    - allows for greater throughput of data by allowing up to 9k bytes of data in a single frame
        - can increase the efficiency of the SAN

Basic cloud concepts

Cloud classifications

- cloud computing: virtual resources, provided by a service provider. It is highly configurable and changeable.
- classifications
    - **public cloud**
        - sys interace with services and devices within the publich cloud and on public nw (e.g., the Internet)
    - **private cloud**
        - sys only communicate with services and devices within the specified private cloud

    - **hybrid cloud**
        - public + private
    - **community cloud**
        - cloud services used by private individuals, organizations or groups that have a common interest

Types of cloud computing

- **Software as a service (SaaS)**
    - the end user purchases the rights to use an application without the need to configure the virtual servers that will deliver the application
        - usually delivered as a web application (within a web browser)
- **Platform as a service (PaaS)**
    - the user is provided with a development platform for the creation of software packages, without the need to configure the virtual servers and infrastructure that delivers it
- **Infrastructure as a service (IaaS)**
    - the end user is provided with access to virtual servers (**configurable** by the customer) and other virtual nw resources
        - highly configurable env
        - the end user supplies the software that is going to be used on the IaaS nw

Implementing a basic network

Plan the network

Configure the network