2024-11-26

Status: #incomplete

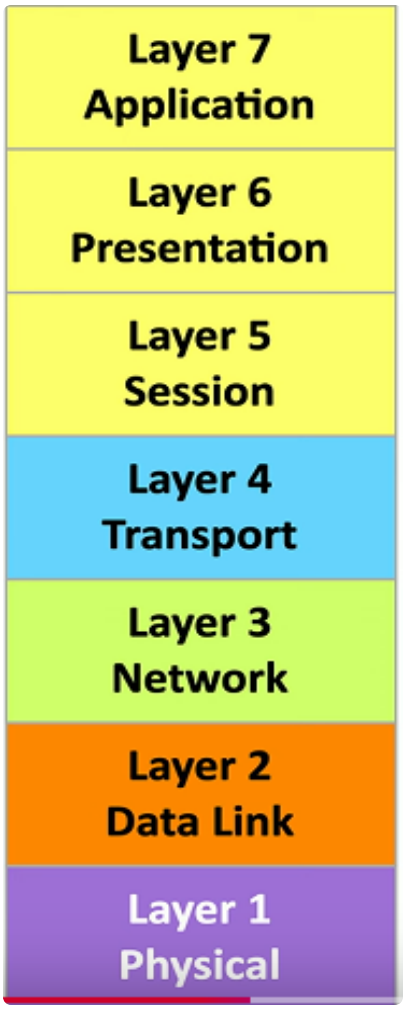
Tags: networking network+

Network+ N10-009

N10-009 Network+ Domain	% of Exam
1.0 - Networking Concepts	23%
2.0 - Network Implementation	20%
3.0 - Network Operations	19%
4.0 - Network Security	14%
5.0 - Network Troubleshooting	24%
Total	100%

1.1 The OSI Model

- Open Systems Interconnection Reference Model
- OSI Model = Guide -> Thus the term "model"
- This is not the OSI protocol suite, most of it's protocols did not catch on (suite as in entirety of models protocols)
- Unique Protocols at Every Layer
- Helpful Mnemonic to Remember Each Layer:
  - All (Application) People (Presentation) Seem (Session) To (Transport) Need (Network) Data (Data Link) Processing (Physical)
  - **All People Seem To Need Data Processing**

- 

Layer 1 - Physical Layer

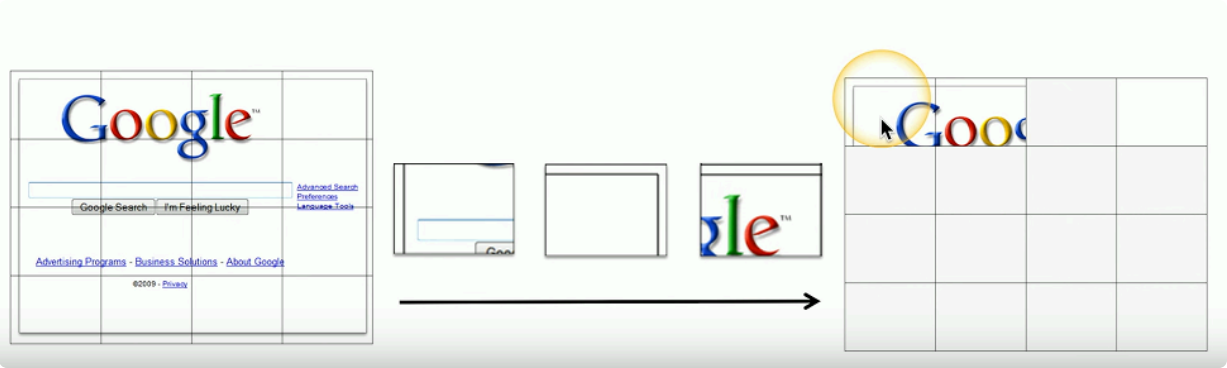
- The physics of the network
  - Signaling, cabling, connectors
  - This layer is not about protocols (Very Hardware Heavy)
- "You have a physical layer problem"
  - Fix your cabling, punch-downs etc
  - Run loopback tests, test/replace cables, swap adapter cards

  Layer 2 - Data Link Layer
- The basic network "language"
  - The foundation of communication at the data link layer
- Data Link Control (DLC) protocols
  - MAC (Media Access Control) address on Ethernet
- The "switching" layer

  Layer 3- Network Layer
- The "routing layer"
- Layer used by routers to determine how to forward traffic

- Internet Protocol (IP)
- Fragments frames to traverse different networks

  Layer 4 - Transport Layer
- The "post office" layer (Analogy : Parcels and letter)
- TCP (Transmission Control Protocol) and UDP (User Datagram Protocol)
- Often comes down to taking a large chunk on data , sending it in fragmented pieces then rebuilding it to its original form at its destination (See Figure Below)

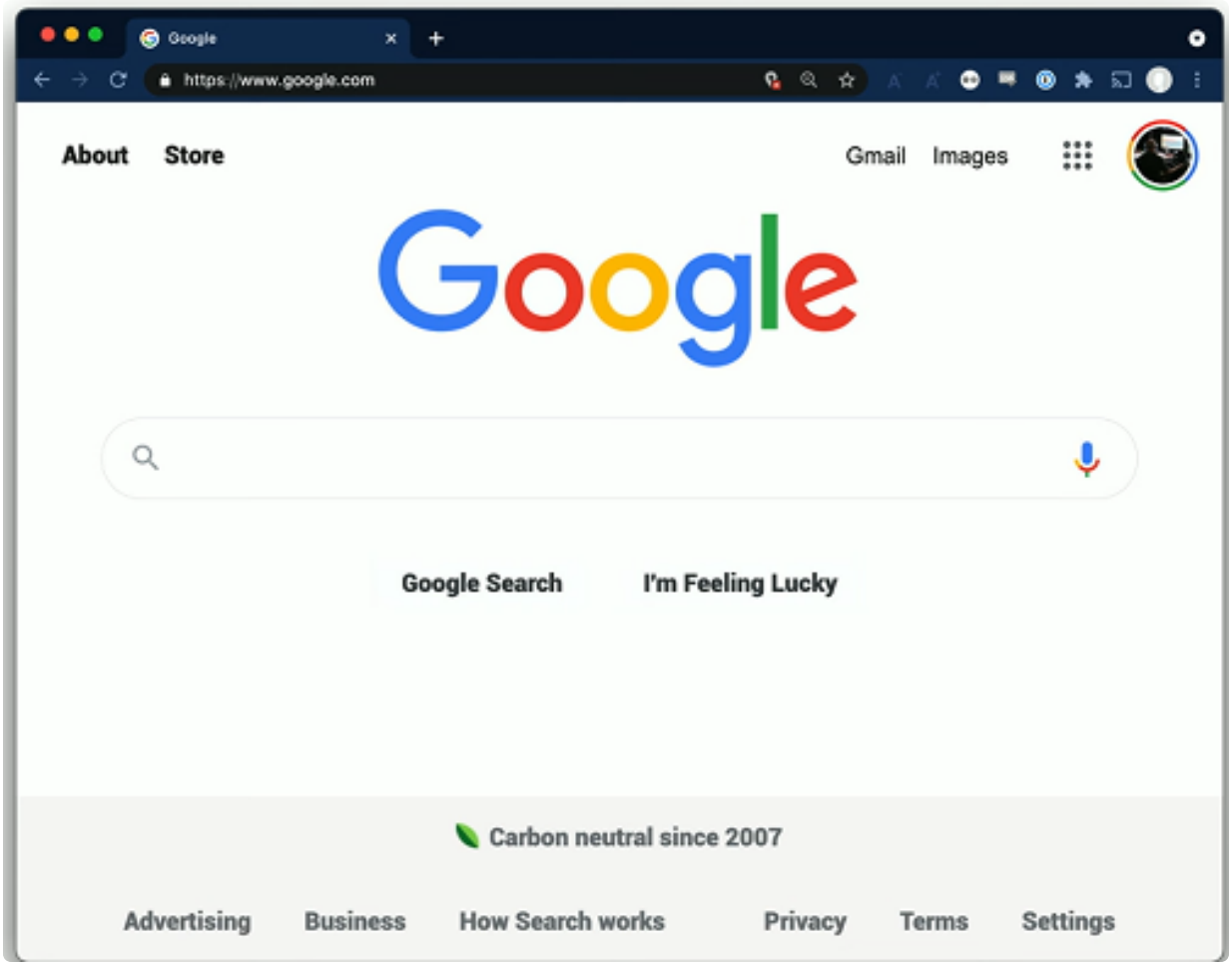


  Layer 5 - Session Layer
- Communication management between devises
  - Start, stop, restart
- Control protocols, tunneling protocols

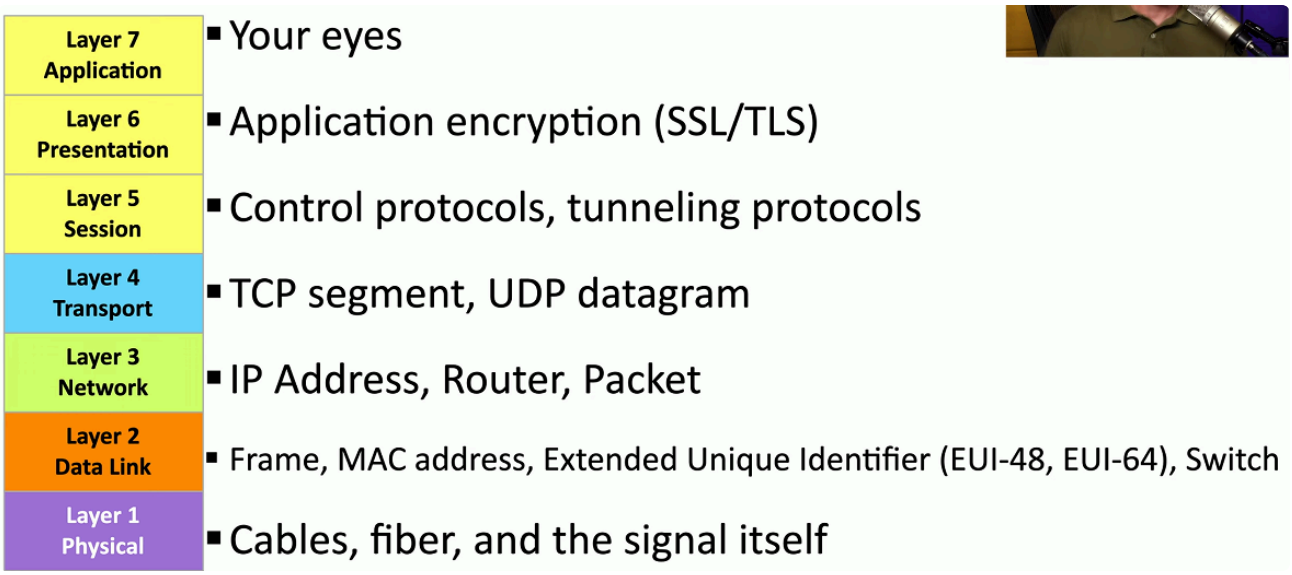
  Layer 6 - Presentation Layer
- Character encoding
- Application encryption
- Often combined with Application Layer

  Layer 7 - Application Layer

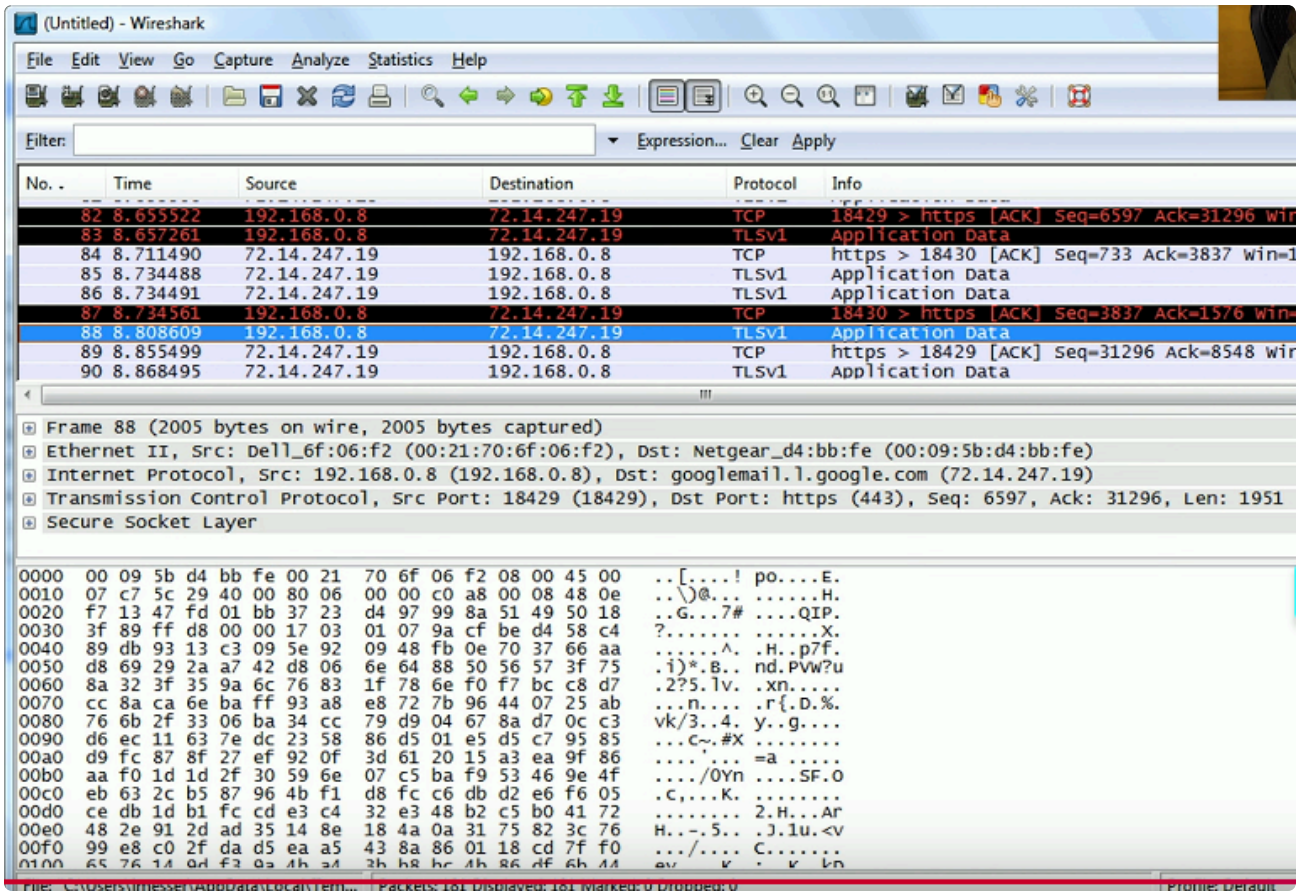
- The layer we see

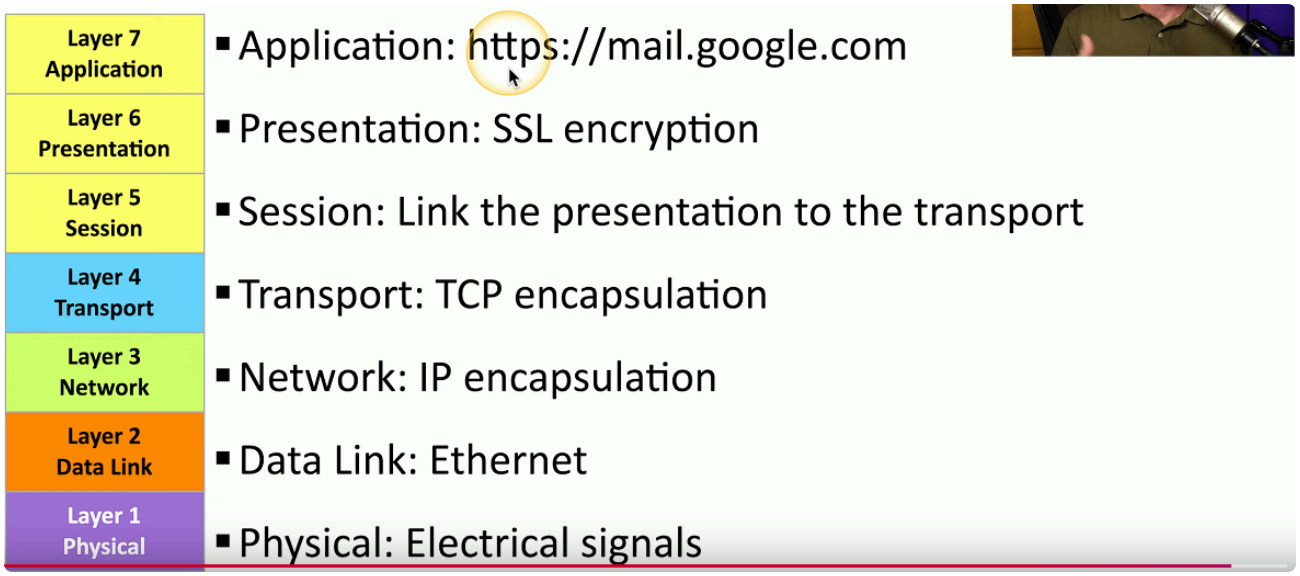


Real World To OSI Model Application:



Wireshark Captured Frame and How It Fits Into OSI Model





Breakdown:

Frame 88... : Refers to the physical electrical signals that were captured (Layer 1)

Ethernet II: Contains MAC Address and etc (Layer 2)

Internet Protocol: IP Mentioned must be network layer (Layer 3)

Transmission Control Protocol: TCP Mentioned (Layer 4)

Secure Socket Layer: This encapsulates all of Layer 5-7 in it

1.2 Networking Devices

Routers:

- Routes traffic between IP subnets
  - OSI Layer 3 Device (L3 = Network Layer)
  - Routers inside of switches sometimes called "layer 3 switches"
  - Layer 2 = Switch, Layer 3 = Router
- Often connects diverse network types
  - LAN (Local Area Network), WAN (Wide Area Network), copper, fiber

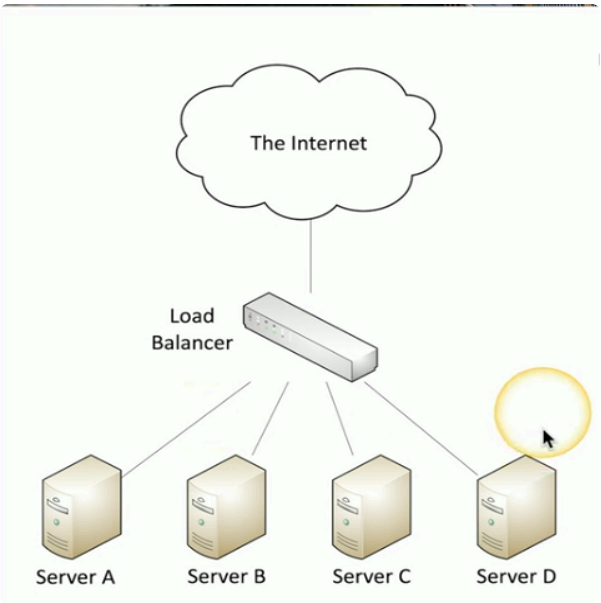
  Switch:
- Bridging done in hardware
  - Application-specific integrated circuit (ASIC)
- OSI layer 2 Device (L2 = Data Link Layer)
  - Forwards traffic based on data link address (MAC Address for example)
- Many ports and features
  - Core of enterprise network
  - May provide Power over Ethernet (PoE)
- Multi layer switch
  - Includes Layer 3 (routing) functionality

  Firewalls:
- Filter traffic by port number or application
  - Traditional vs. NGFW (New Generation Firewall)
- Encrypt traffic
  - VPN between sites
- Most firewalls can be layer 3 devices (routers)
  - They often sit in the ingress/egress of the network (Right at border of inflow and outflow of data)
  - Network Address Translation (NAT)
  - Dynamic Routing

  IDS and IPS:
- Monitor network traffic
- Intrusions
  - Exploits against OS, applications, etc
  - Buffer overflows, XXS (Cross site scripting), other vulnerabilities
- Detection vs. Prevention
  - Detection - Alarm or Alert
  - Prevention - Stop before getting into the network

  Load Balancer:
- Distribute the load
  - Multiple servers
  - Invisible to end user

- Large scale implementations
  - Web server farms, database farms
- Provides Fault Tolerenace
  - Minimal impact from server outages
  - Very fast convergence



- Configurable load
  - Manage across servers
- TCP offload
  - Protocol overhead
- SSL offload
  - Encryption/Decryption Capabilities provided by Load Balancer instead of by each individual server
- Caching on Load Balancer allows fast response
- Prioritization
- Content Switching -> Application centric blanacing

Proxies:

- Sits between users and external network
- Receives user requests and sends on users behalf
- Useful for caching info, access control, URL filtering, content scanning
  - URL = Uniform Resource Locator
- Applications may need to know how to use proxy in explicit cases
- Some proxies however are invisible (transparent) and do not affect OS or applications

NAS vs. SAN

- Network Attached Storage (NAS)
  - Connect to a shared storage device across the network
  - File-level access

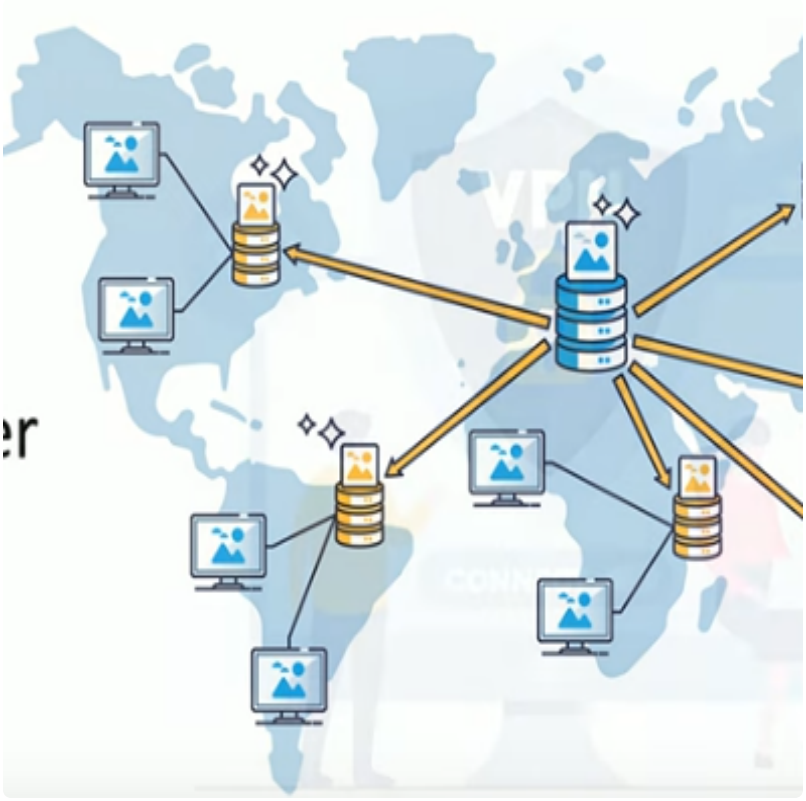
- Storage Area Network (SAN)
  - Looks and feels like a local storage device
  - Block level access (more efficient than file-level)
    - Only write and read changes of block rather than entire file
- Both require large bandwidth so they often use isolated network and high speed network technologies
  Access Point (AP)
- Not a wireless router
  - A wireless router is a router and an access point in a single device (Think home routers)
- Access point is a bridge
  - Extends the wired network on the wireless network
  - OSI layer 2 device (Data Link Layer)
  Wireless LAN Controllers
- Centralized management of all access points
  - Singular father device that controls all
- Can deploy new access points
- Conducts performance and security monitoring
- Configure and deploy changes to all access points
- Report on access point user
- These are often proprietary systems, the access points and wireless controller are paired from same provider

1.2 Networking Functions

Content Delivery Network (CDN)

- Speed up process of getting data
- Geographically distributed caching servers
  - Duplicate data
  - Users get data from local server rather than central server which may be in another continent for example

- Invisible to end user



Yellow areas show the regional CDN's people are accessing rather than the central server

Virtual Private Network (VPN)

- Secure private data traversing a public network
  - Encrypted communication on an insecure medium
- Often use Concentrator / head-end
  - Central connection point for all users connecting to VPN
  - Encryption/decryption access device
  - Often integrated into a firewall
- Many deployment options
  - Specialized cryptographic hardware
  - Software-based options (ProtonVPN, NordVPN etc)

Quality of Service (QoS)

- Control priorities of services
  - By bandwidth usage or data rates
- Traffic shaping, packet shaping

- Set important applications to have higher priorities
- Manage QoS through:
  - Routers, switches, firewalls, QoS devices

Time to live (TTL)

- How long should data be available?
  - Not all systems or protocols are self regulating, this allows us to tell a system to stop
- Creates a timer:
  - Wait until traversing a number of hops or wait until a certain amount of time elapses then stop (or drop) process
- Many differerent uses
  - Drop packet caught in loop, clear a cache...

Routing Loops

- Router A thinks next is to Router B, but router B thinks next hop is Router A
  - Loop created
  - Easy to have this happen with misconfiguration specially in static routing
  - TTL is used to stop this loop
    Ex Of Routing Loop Occuring:

```
C:\>tracert 10.4.10.1

Tracing route to 10.4.10.1 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      10.1.10.1
  2    0 ms      0 ms      0 ms      10.2.10.2
  3    0 ms      0 ms      0 ms      10.1.10.1
  4    0 ms      0 ms      0 ms      10.2.10.2
  5    0 ms      0 ms      0 ms      10.1.10.1
  6    0 ms     13 ms      0 ms      10.2.10.2
  7    0 ms      0 ms      0 ms      10.1.10.1
  8    0 ms      0 ms      0 ms      10.2.10.2
  9    0 ms     13 ms      0 ms      10.1.10.1
  10    0 ms      0 ms      0 ms      10.2.10.2
  11    0 ms      0 ms      0 ms      10.1.10.1
  12    0 ms      0 ms      0 ms      10.2.10.2
 . . .
```

IP (Internet Protocol)

- Loops could cause a packet to live forever
  - Drop the packet after x amount of hops
- Each pass through a router is a hop
  - Default TTL on macOS/Linux = 64 hops
  - Default TTL on Windows = 128 hops
  - Router decreases TTL by 1, once TTL 0 is reached the router drops the packet

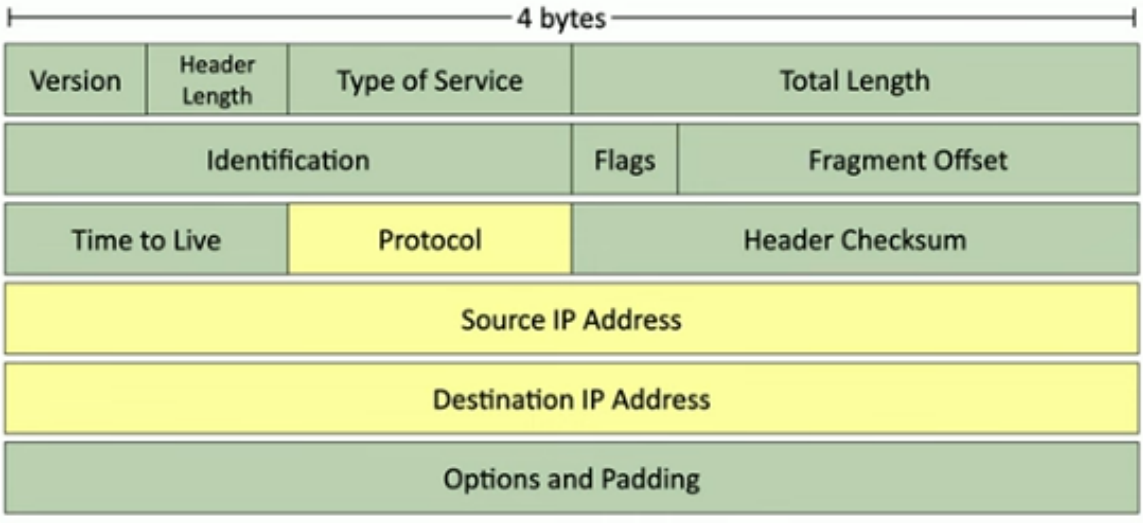
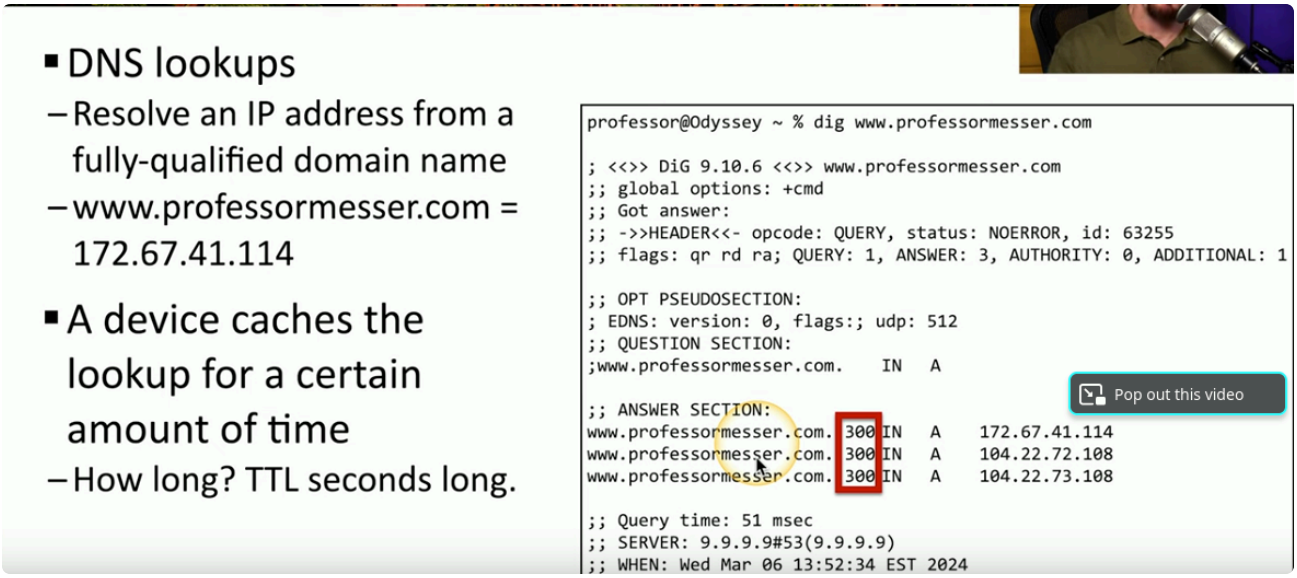


Image shows where TTL is stored

TTL In DNS (Domain Name System)



In this case the DNS TTL is 300 seconds, DNS uses seconds rather than hops. Meaning the IP is cached for 300 seconds until the DNS has to query it again

1.3 Designing the Cloud

- On-demand computing power
- Elasticity -> Scale up or down as needed
  - Applications also scale and have access from anywhere
- Multi-tenancy
  - Many different clients are using the same cloud infrastructure

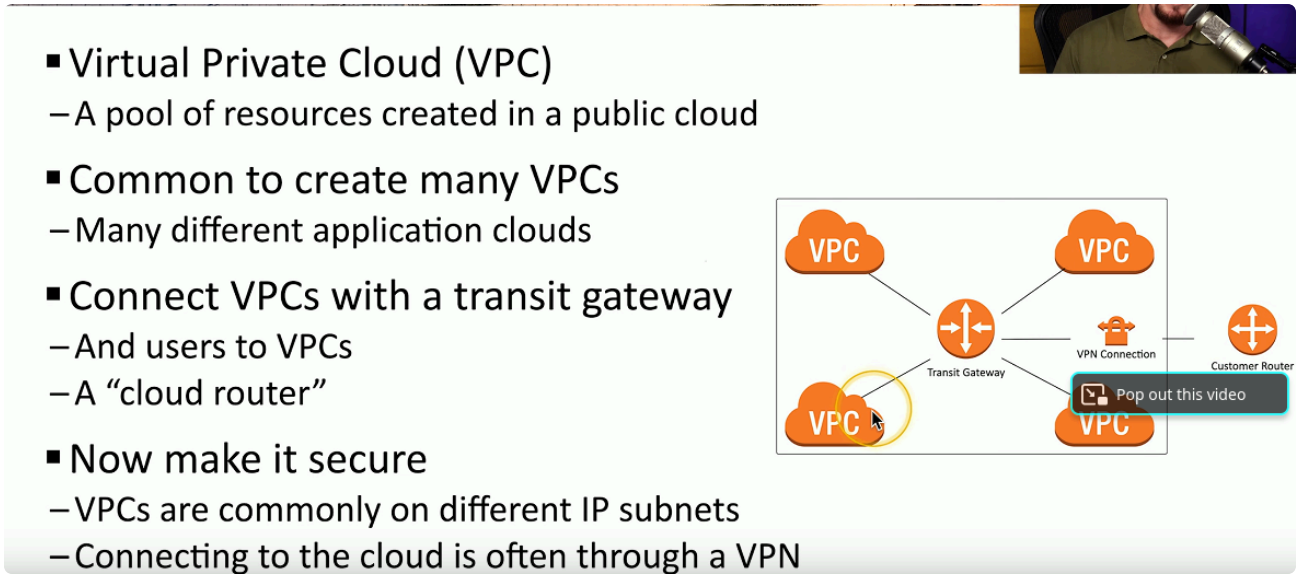
Virtual Network

- Server farm with 100 individual computers
- All servers are connected with enterprise switchers and routers with redundancy
- Migrate 100 physical servers to one physical server with 100 virtual servers inside (Through Cloud Infrastructure)
- What happens to our Network?

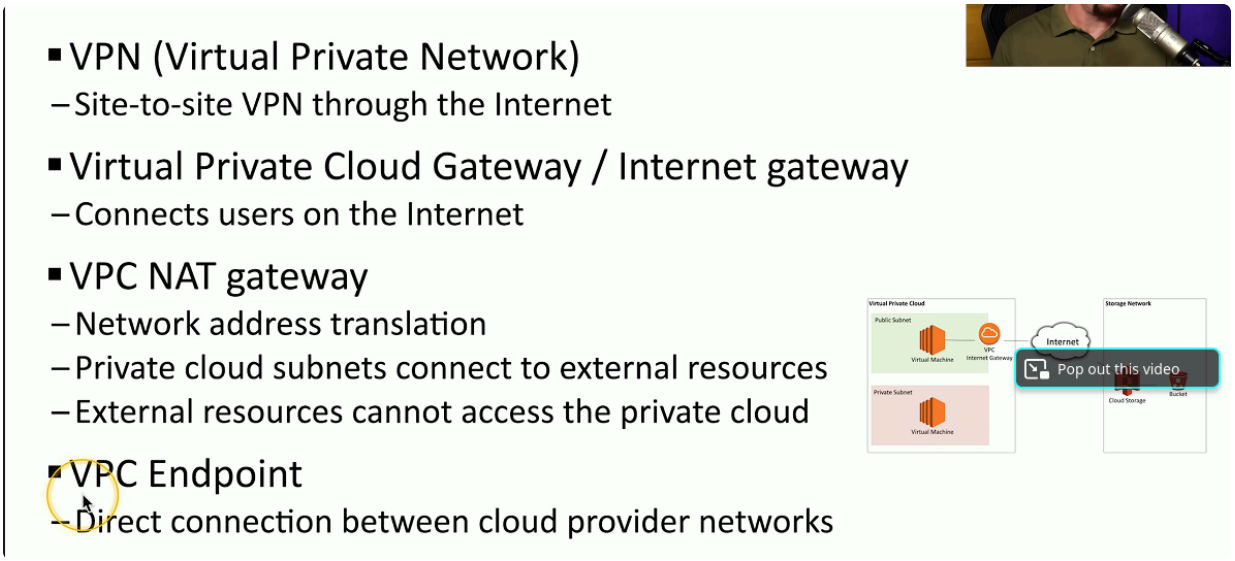
Network Function Virtualization (NFV)

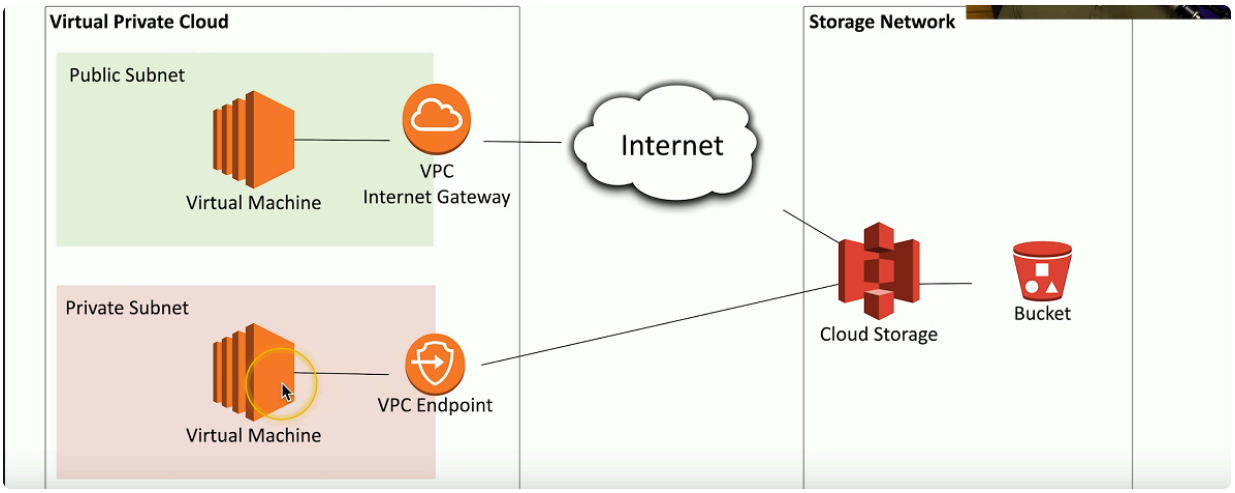
- Replace physical network devices with virtual version
  - Manged from the hypervisor
- Same functionality as previous physical device
  - Routing,switching, load balancing, firewalls etc...

Connecting to the Cloud:



- **Transit Gateway = "Cloud Router"**





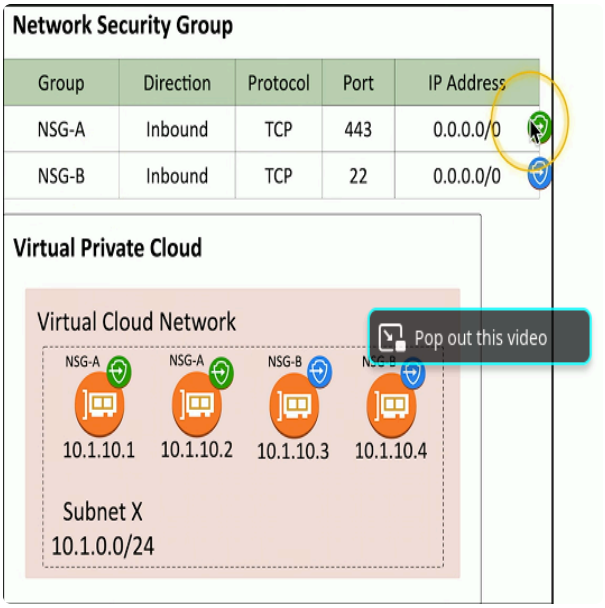
Security Groups and Lists (Like Firewall for the Cloud)

- Control inbound and outbound traffic flows
- Layer 4 Port Number (TCP or UDP port)
- Layer 3 Address
  - Individual addresses
  - CIDR Block notation
  - IPv4 or IPV6

Network Security List

- Assign a security rule to an entire IP subnet
  - Applies to all devices in the subnet
- Very broad
  - Can become difficult to manage as well as the fact that not all devices in a subnet necessarily have the same security posture
  - More granularity may be needed as broad rules may not provide right level of security

  Network Security Group
- Assign a security rule to a specific virtual nic (VNIC)
  - Applies to specific devices and network connections
- More granular than network security lists and more control
  - Different rules for devices in same IP subnet
  - Best practice for cloud security rules



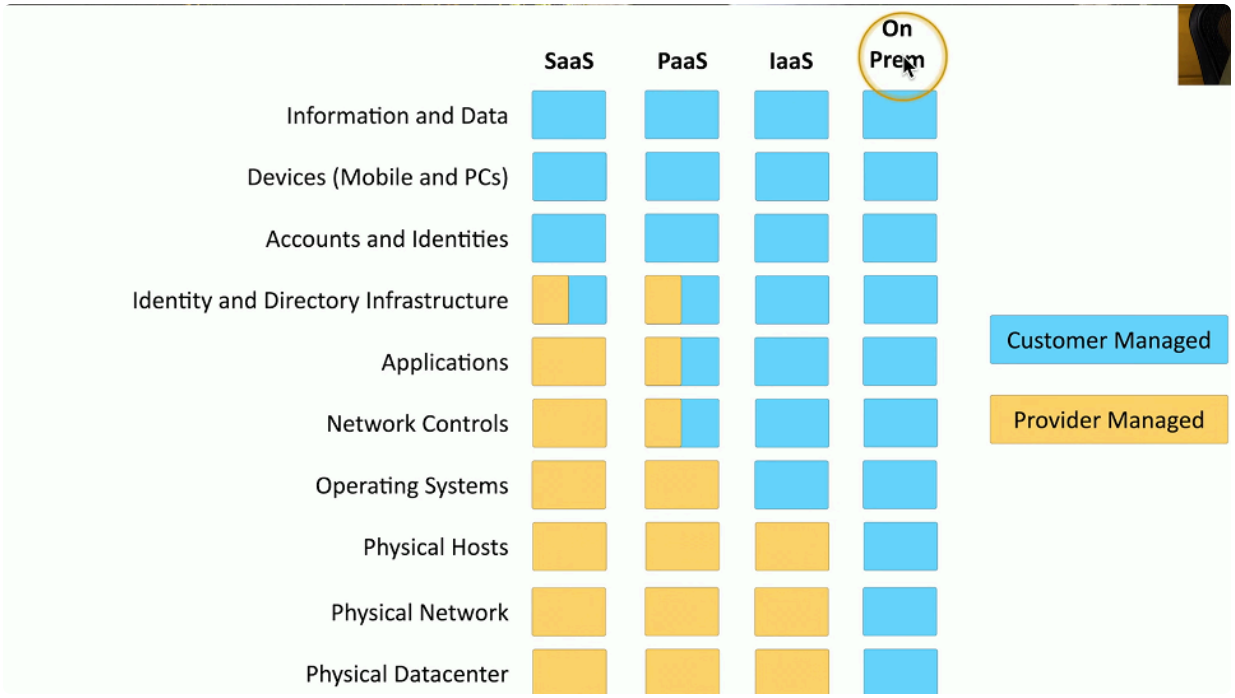
Note how although all devices are in the same Subnet X (10.1.0.0/24) they are separated by group NSG-A and NSG-B

1.3 Cloud Models

- Public : Available to everyone over the Internet
- Private : Your own virtualized local data center
- Hybrid : Mix of public and private

SaaS (Software as a Service)

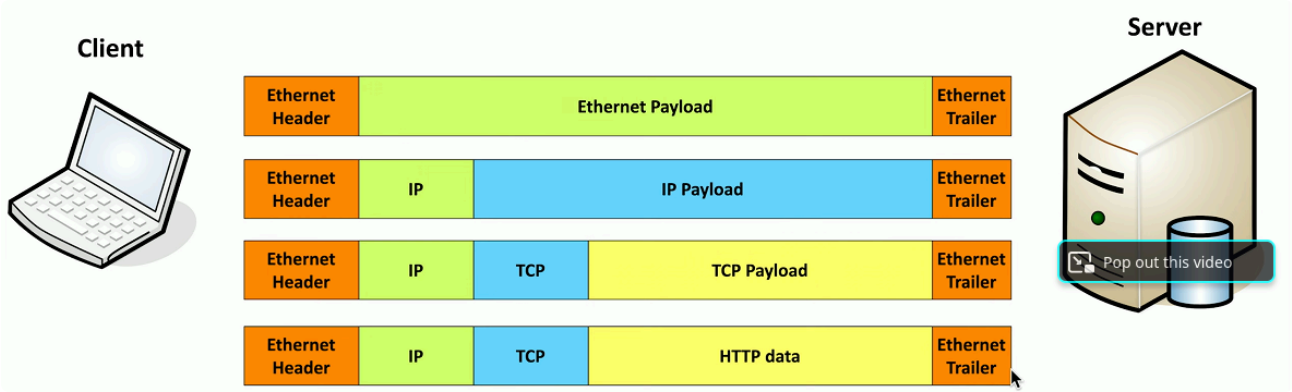
- On demand software
- No local installation
- Central management of data and applications
- No dev work required
  - Google Mail, Office 365
  IaaS (Infrastructure as a Service)
- Outsource your equipment
- Still responsible for management and security
- Data still out there but more control
- Web server providers
  PaaS (Platform as a Service)
- No servers, no software, no maintenance team no HVAC
  - Someone else handles platform you handle the development
- No direct control over data, people or infrastructure
- Trained security professionals watching your stuff
- Put building blocks together to develop app from whats available on platform Ex: Salesforce.com
  Cloud Responsibility Matrix



1.3 Introduction to IP

- Efficiently move large amounts of data (Use a shipping truck)
- Our network topology is the road
  - Ethernet, DSL, cable system
- The truck is the Internet Protocol (IP)
  - These roads were designed for this truck
- The boxes hold your data (Boxes of TCP and UDP)
- Inside the boxers are more thing (Application information)

Breakdown of Frame Structure



Top = Least Detail vs Bottom = Most Detail of where each data component/instruction is held

TCP and UDP

- Transported inside of IP (encapsulated by IP protocol)
- Two ways to move data across destinations
- OSI Layer 4 (Transport Layer)
- Multiplexing -> Transferring multiple applications simultaneously among multiple devices

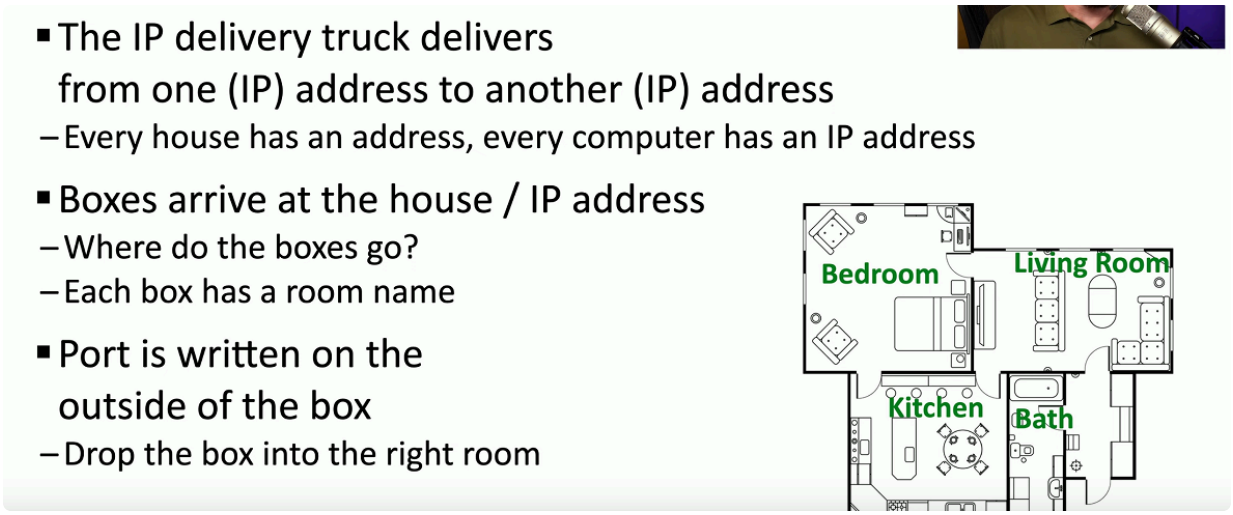
TCP - Transmission Control Protocol

- Connection-oriented -> Formal connection setup and close
- "Reliable" deliver
  - Recovery from errors
  - Can manager out of order messages or retransmissions
  - TCP Data sent, then TCP ACK response sent back when received

- Flow control -> Receiver can manage how much data is sent

UDP - User Datagram Protocol

- COnnectionless -> No formal open or close to the connection
- Packet after packet sent of UDP data without server acknowledgement of data being delivered.
- "Unreliable" delivery -> No error recovery or reordering of data or retransmissions
- No flow control -> Sender determines amount of data transmitted
  TCP/UDP Port Room Analogy

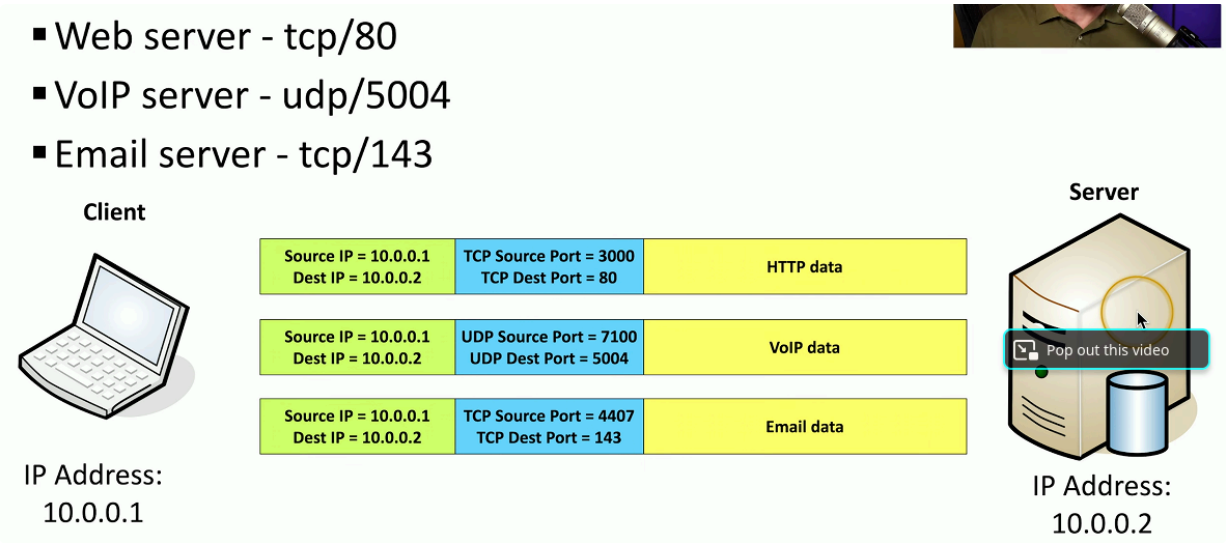


  Port written outside box will tell us which room to send to: Ex of ports = 80, 25, 123, 443

Ports

- IPv4 Sockets
  - Server IP address, protocol, server app port number
  - Client IP address, protocol, client port number
- Non-ephemeral ports = Permanent port number
  - Ports 0 through 1023
  - Usually on a server or service
- Ephemeral ports = Temporary port numbers
  - Ports 1024 through 65,535
- TCP and UDP Ports can be any number between 0-65,535
- Port numbers are for communication, not security
- Service port numbers need to be "well known"
  - Web servers expected to always use port 80 or 443

- TCP and UDP port numbers are not the same



1.4 Common Ports

FTP - File Transfer Protocol

- Transfers files between systems
  - Generic file transfer method, not specific to OS
- tcp/20 (active mode data), tcp/21 (control)
  - Authenticates with username and password
- full-featured functionality (list,add,delete, etc)

SSH - Secure Shell

- Text based console communication
- Encrypted communication link -> tcp/22

SFTP - Secure FTP

- Uses the SSH File transfer Protocol
  - SSH not just for console communication
- tcp/22
- Generic File transfer with security

Telnet - Telecommunication Network

- tcp/23
- Console access
- In the clear communication not the best choice for production systems.

SMTP - Simple Mail Transfer Protocol

- Server to server email transfer
- tcp/25 (SMTP w/ plaintext)
- tcp/587 (SMTP using TLS Encryption)

- Also used to send mail from a device to a mail server
  - Commonly configured on mobile devices and email cliednts
- Other protocols are used for clients to receive email (IMAP,POP3)

DNS - Domain Name System

- upd/53
- Large transfers may use tcp/53
- Converts names to IP addresses

DHCP - Dynamic Host COnfiguration Protocol

- Automated configuration of IP address, subnet mask and other options
- udp/67, udp/68
  - Requires DHCP server
  - Server, appliance, integrated into a SOHO router, etc.
- Dynamic/pooled
  - IP addresses are assigned in real time from a pool
  - Each system is given a lease, must renew at set intervals
- DHCP reservation

  - Addresses are assigned by MAC address in the DHCP server
  - Quickly manage addresses from one location

TFTP - Trivial File Transfer Protocol

- udp/69
- Very simple file transfer -> Read and write without authentication
- Useful when starting a system

HTTP and HTTPS

- HTTP = tcp/80
- HTTPS = tcp/443
- Hypertext Transfer Protocol

  - Communication in the browser and by other apps
  - In the clear or encrypted: SSL (Secure Socket Layer) or TLS (Transport Layer Security)

Protocol	Port	Name	Description
HTTP	tcp/80	Hypertext Transfer Protocol	Web server communication
HTTPS	tcp/443	HTTP over TLS or SSL	Web server communication with encryption

NTP - Network Time Protocol

- udp/123
- Switches,router,firewalls,server,workstations

  - Every device has its own clock

- Synchronizing clocks is critical -> Log files, authentication info, outage details
- Automatic updates also accurate to better than 1 millisecond on local network
- Flexible -> You control how clocks are updated

SNMP - Simple Network Management Protocol

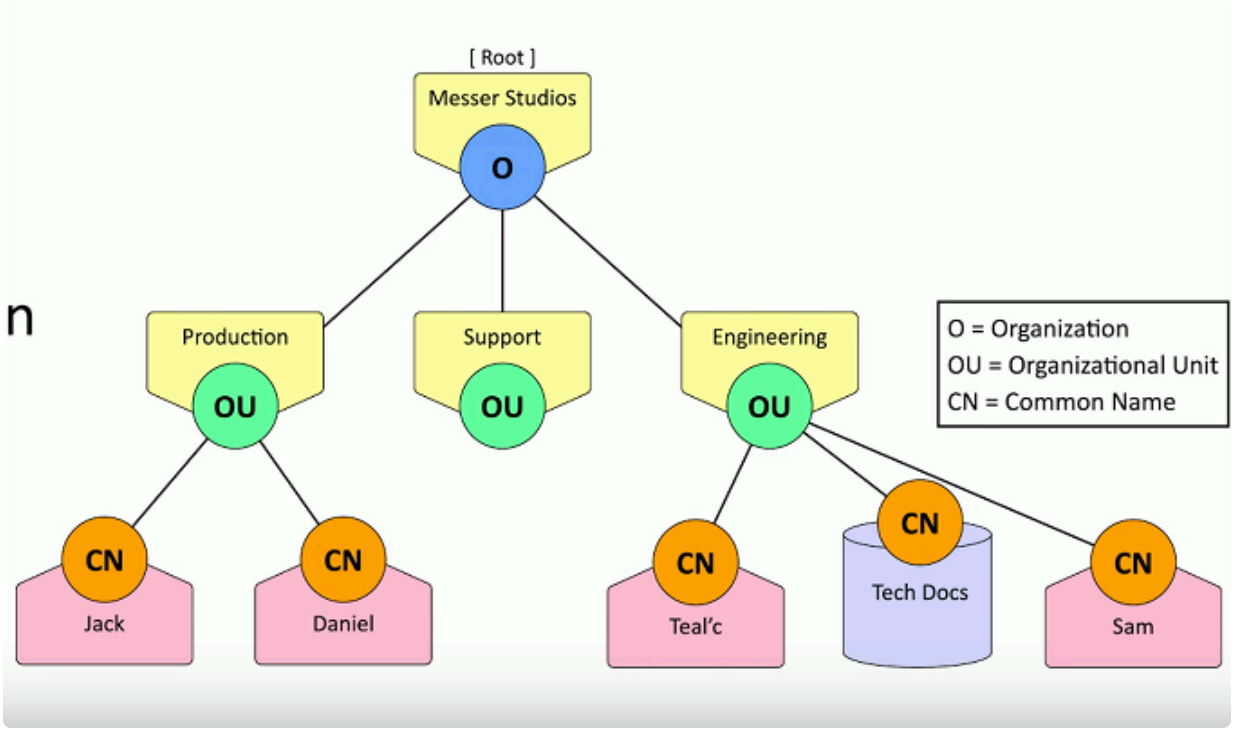
- udp/161
- Gather statistics from network devices
- v1- The original
  - Structured tables
- v2 - A good step ahead
  - Data type enhancements, bulk transfer
- All data however sent in the clear no encryption
- v3 - A secure standard
  - Message integrity, authentication and encryption
- SNMP traps

  - udp/162
  - Alerts and notifications from the network devices

LDAP/LDAPS (Lightweight Directory Access Protocol) and LDAPS -> LDAP(Secure)

- LDAP tcp/389
- Store and retrieve info in a network directory
- LDAPS tcp/636

  - Non standard implementation of LDAP over SSL



SMB - Server Message Block

- Direct over tcp/445 (NetBIOS-less)

    - Direct SMB communication over tcp
- Protocol used by Microsoft Windows
  - File sharing, printer sharing
  - Also called CIFS (Common Internet File System)
  - Integrated into the OS

  Syslog
- udp/514
- Standard for message logging
    - Diverse systems, consolidated log
- Usually a central log collector
  - Integrated into the SIEM (Security Information and Event Manager)
  - Requires a lot of disk space (Data storage from many devices over an extended timeframe)

  Databases
- Microsoft SQL Server tcp/1433
- MS-SQL (Microsoft structured Query Language)
- Collection of information -> Many different types of data but one common method to store and query (SQL)
- SQL -> A standard language across database servers

  `SELECT * FROM Customers WHERE Last_Name='Messer';`

  RDP - Remote Desktop Protocol
- Share desktop over remote location tcp/3389
- Connect to entire desktop or applicatioin

  SIP - Session Initiation Protocol
- Voice over IP (VoIP) signaling tcp/5060, tcp/5061
- Setup and manage VoIP session->Call ring, play busy signal, hang up
- Extend voice communications ->File transfer, video conferencing, messaging

1.4 Other Useful Protocols

ICMP - Internet Control Message Protocol

- "Text messaging" for your network devices
- Another protocol carried by IP -> Not used for data transfer
- Devices can request and reply to admin requests
    - Hey are you there? / Yes Im right here
- Devices can send msgs when things don't go well
  - That network you're trying to reach is not reachable from here

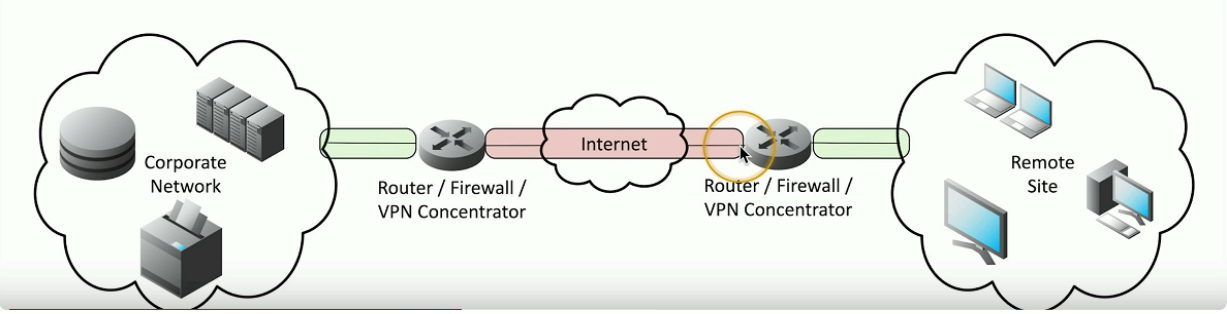
- Your TTL (Time to live) expired just letting you know

GRE - Generic Routing Encapsulation

- The tunnel between two endpoints
- Encapsulate traffic inside of IP

  - Two endpoints appear to be directly connected to each other
  - No built in encryption

  Site-to-site VPN
- Always-on (Or almost always)
- Firewalls often act as VPN concentrators



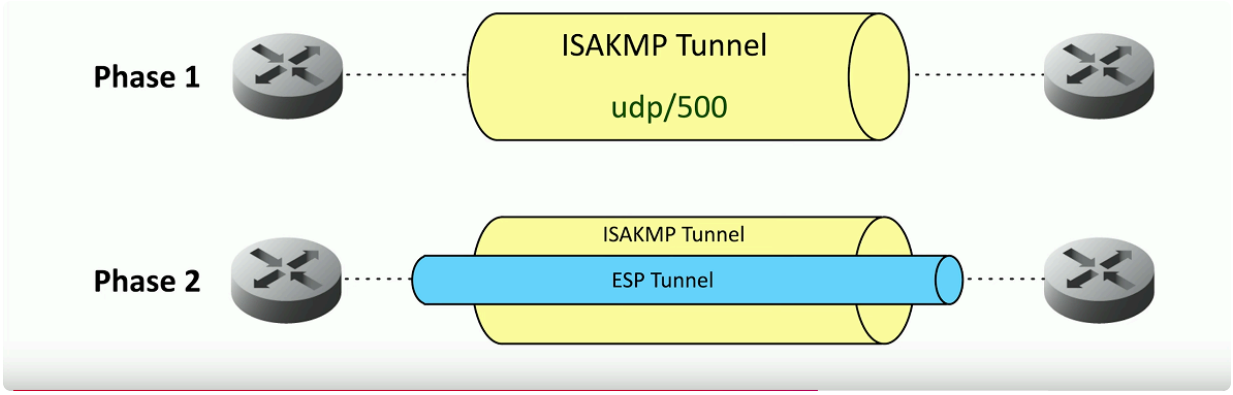
IPSec (Internet Protocol Security)

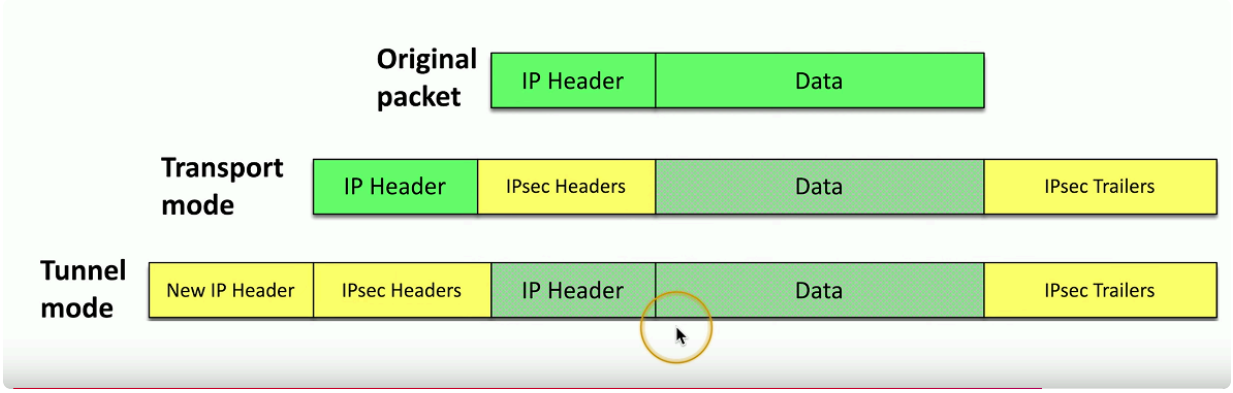
- Security for OSI layer 3
  - Authentication and encryption for every packet
  - Confidentiality and integrity/anti-replay through encryption and packet signing
  - Very standardized -> Common to use multi-vendor implementations
- Two core IPSec Protocols

  - Authentication Header (AH)
  - Encapsulation Security Payload (ESP)

  Internet Key Exchange (IKE)
- Agree on encryption/decryption keys without sending the key across the network
- Builds a Security Association (SA)
- Phase 1
  - Use Diffie-Hellman to create a shared secret key
  - udp/500
  - ISAKMP (Internet Security Association and Key Management Protocol)
- Phase 2

  - Coordinate ciphers and key sizes
  - Negotiation an inbound and outbound SA for IPsec

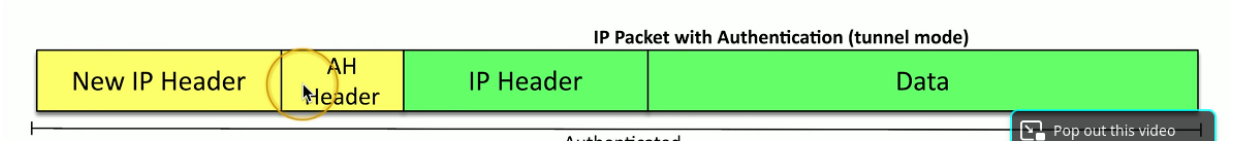




Tunnel mode is most preferred as IP Header and Data are Encrypted where as in Transport Mode the IP Header is not and therefore information about where the data is intended to go can be extracted

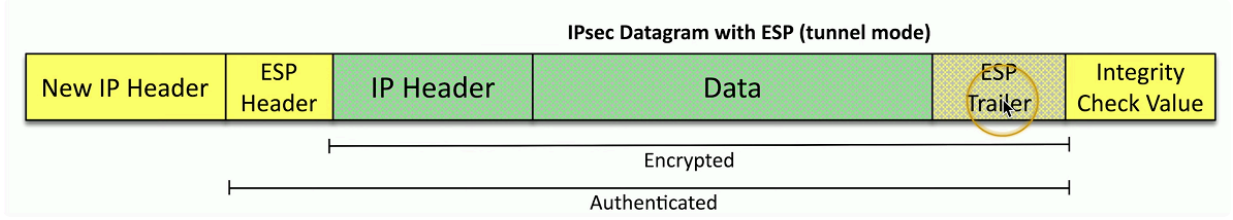
Authentication Header (AH)

- Hash of the packet and a shared key
  - MD5- SHA-1 or Sha-2 are common
  - Adds the AH to the packet header



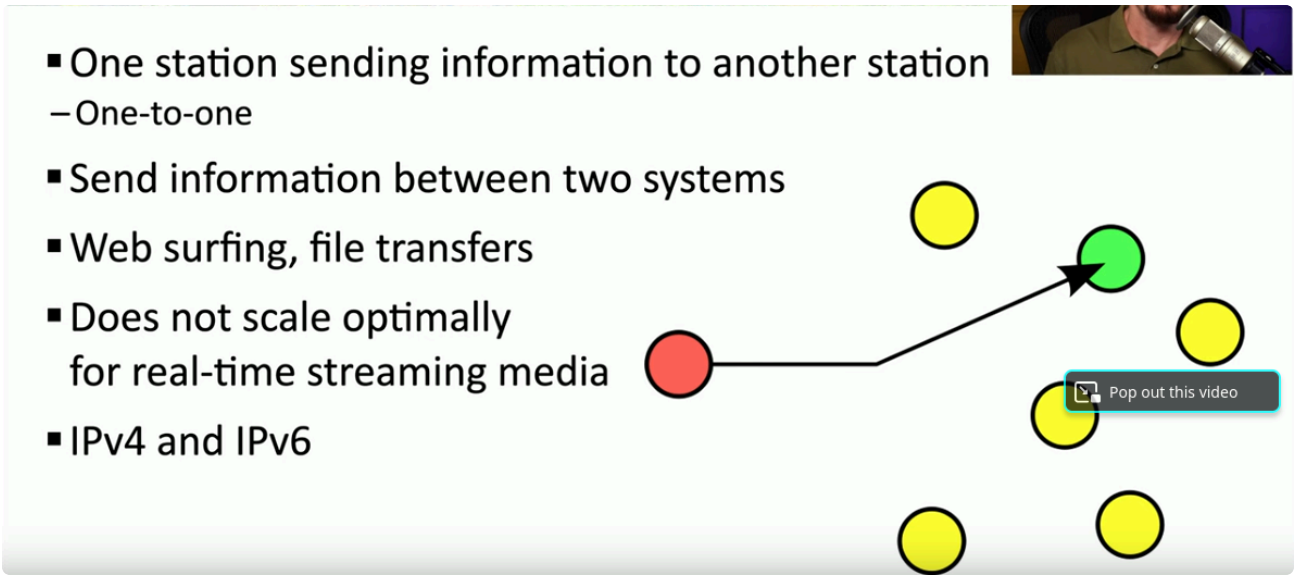
Encapsulation Security Payload (ESP)

- Encrypts the packet
  - MD5, SHA-1 or SHA-2 For Hash
  - 3DES or AES for encryption
- Adds a header, a trailer and an Integrity Check Value

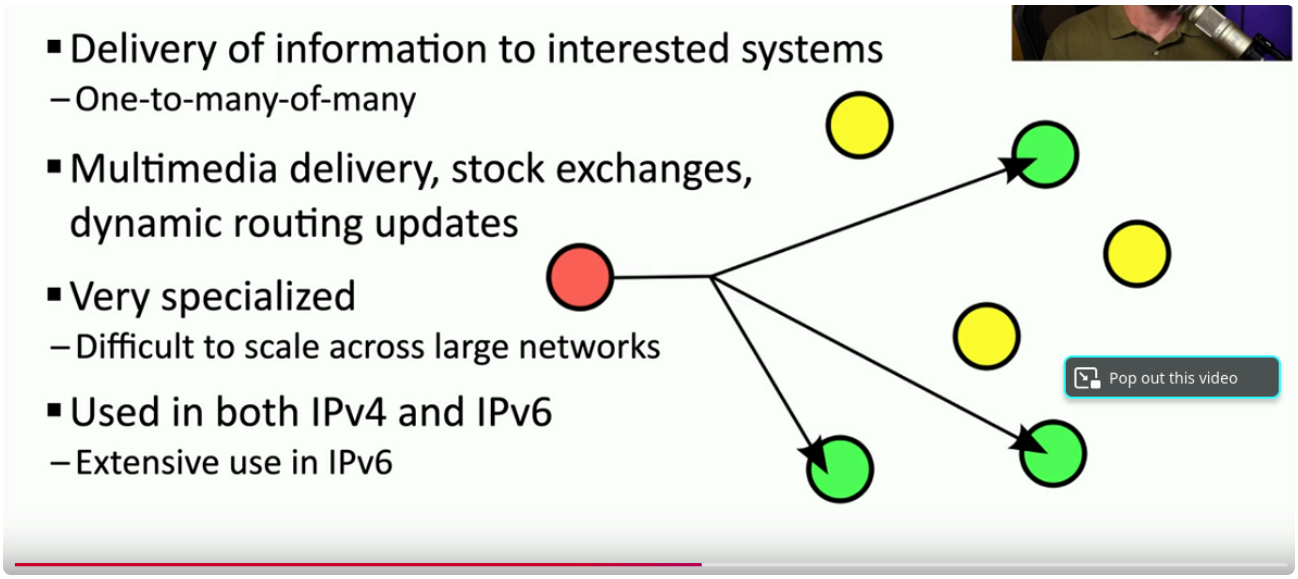


1.4 Network Communication

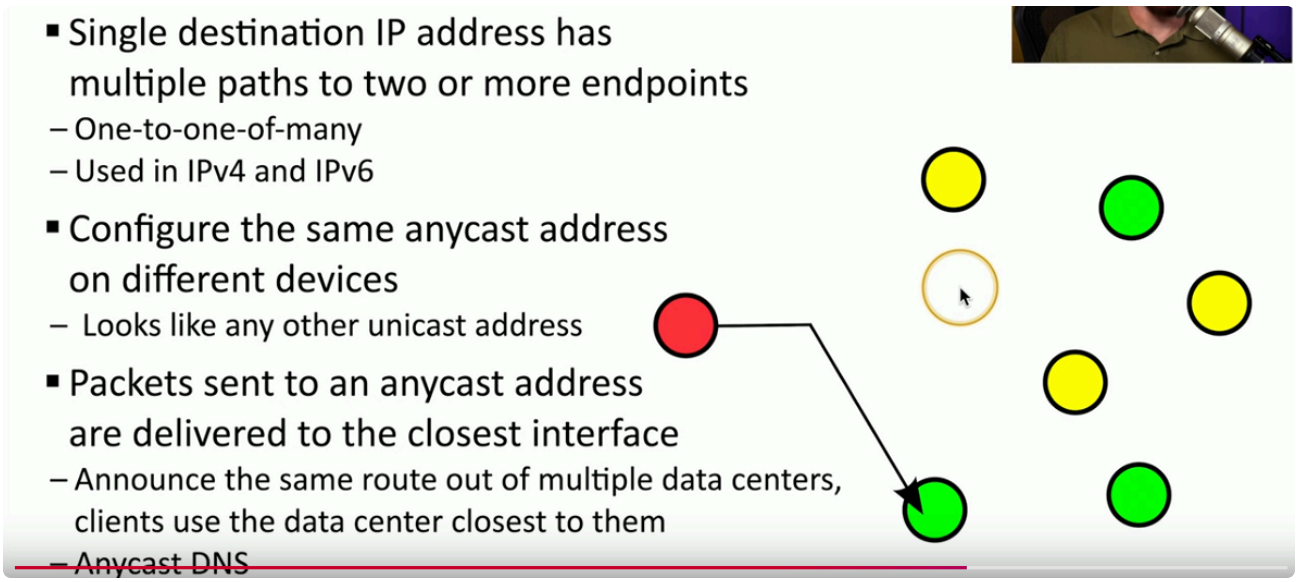
Unicast:



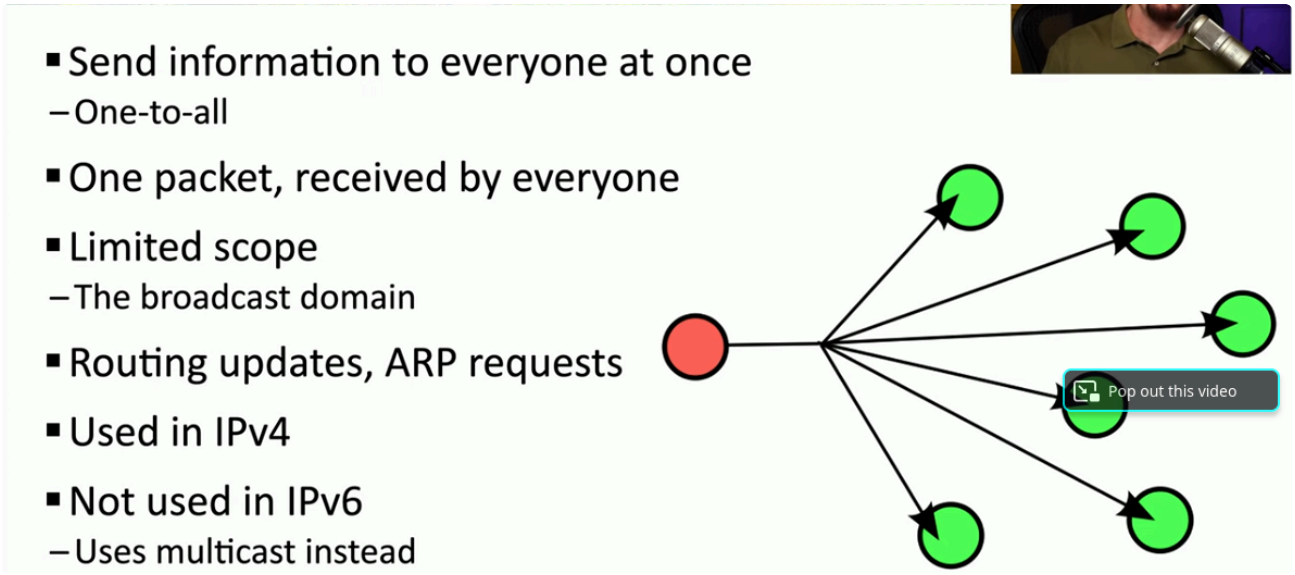
Multicast:



Anycast:



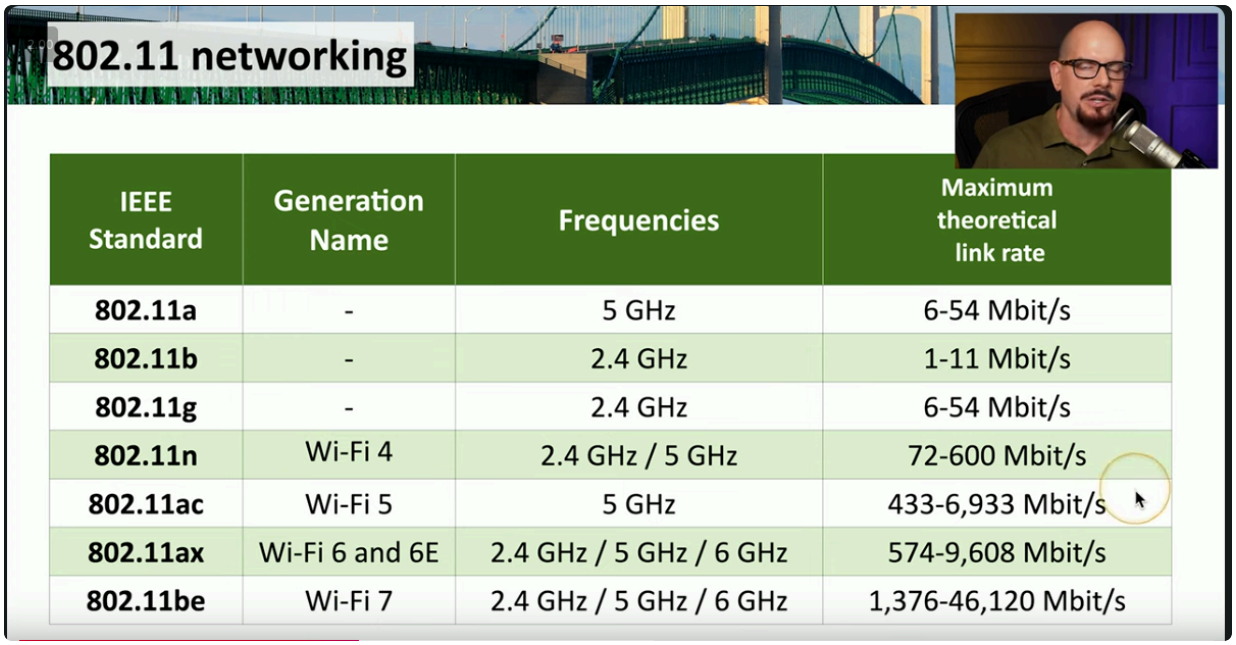
Broadcast:



1.5 Wireless Networking

Wifi

- Wireles networking (802.11)
  - Managed by the IEEE LAN/MAN Standards Committee (IEEE 802)



IEEE Standard	Generation Name	Frequencies	Maximum theoretical link rate
802.11a	-	5 GHz	6-54 Mbit/s
802.11b	-	2.4 GHz	1-11 Mbit/s
802.11g	-	2.4 GHz	6-54 Mbit/s
802.11n	Wi-Fi 4	2.4 GHz / 5 GHz	72-600 Mbit/s
802.11ac	Wi-Fi 5	5 GHz	433-6,933 Mbit/s
802.11ax	Wi-Fi 6 and 6E	2.4 GHz / 5 GHz / 6 GHz	574-9,608 Mbit/s
802.11be	Wi-Fi 7	2.4 GHz / 5 GHz / 6 GHz	1,376-46,120 Mbit/s

  4G and LTE
- Long Term Evolution (LTE)
  - A "4G" technology
  - Converged standard (GSM and CDMA providers)
  - Based on GSM and EDGE (Enhance Data Rates for GSM Evolution)
  - Standard supports download of 150 Mbit/s

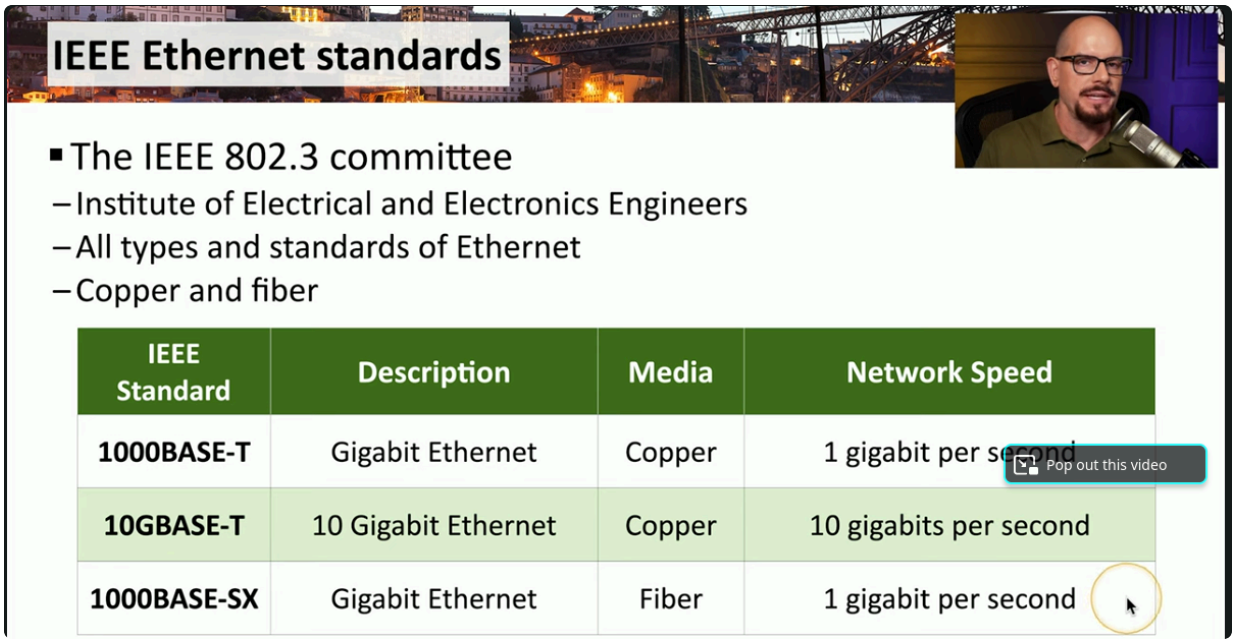
- LTE-A (LTE Advanced)
  - Standard supports download rates of 300 Mbit/s

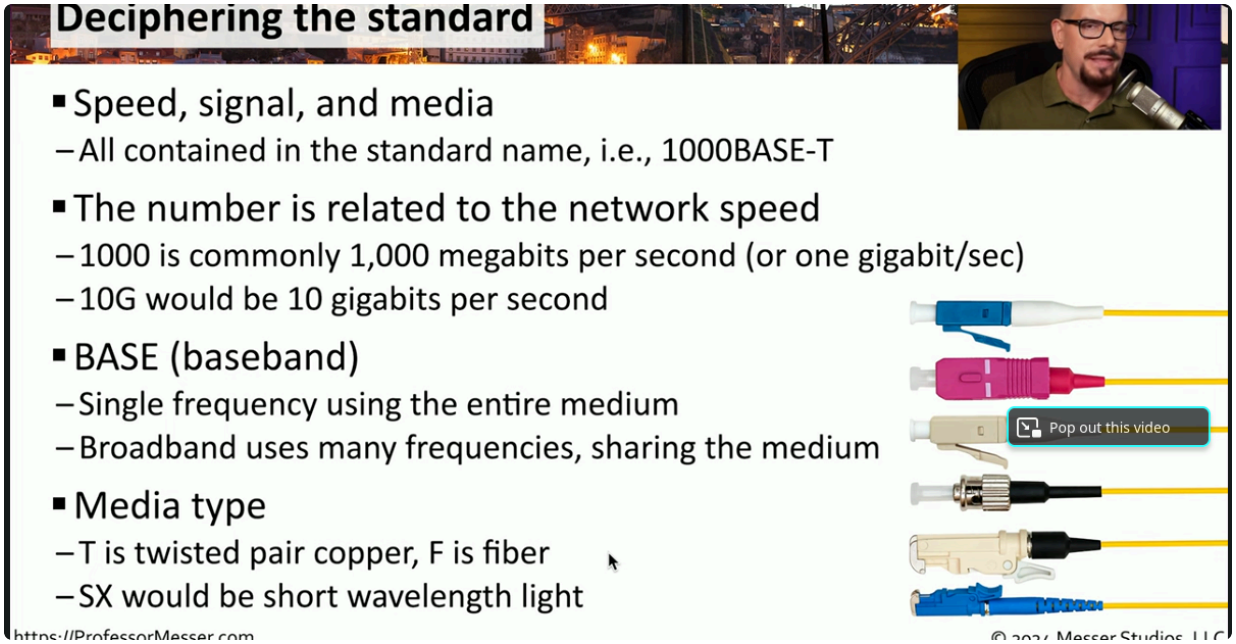
  5G
- Fifth generation cellular networking ->Launched Worldwide in 2020
- Performance improvements -> At higher frequencies, eventually 10 gigabits/s
  - Slower speeds from 100-900 Mbit/s
- Significant IoT (Internet of Things) impact
  - Bandwidth less of constraint, larger data transfers, additional cloud processing, faster monitoring and notification

  Satellite networking
- Communication to a satellite
  - Non terrestrial communication
- High cost relative to terrestrial networking
  - 100 Mbit/s down, 5 Mbit/s up is common
  - Remote sites, difficult to network sites
  - Relatively high latency -> 250ms up 250ms down
  - Starlink advertises 40ms and is working 20ms
- High frequencies - 2GHz
  - Need line of sight and suffers to rain fade

1.5 Ethernet Standards

- Different types: Speeds, cabling, connectors, equipment
- Modern uses: Twisted pair copper or fiber
  - Standard defines the media



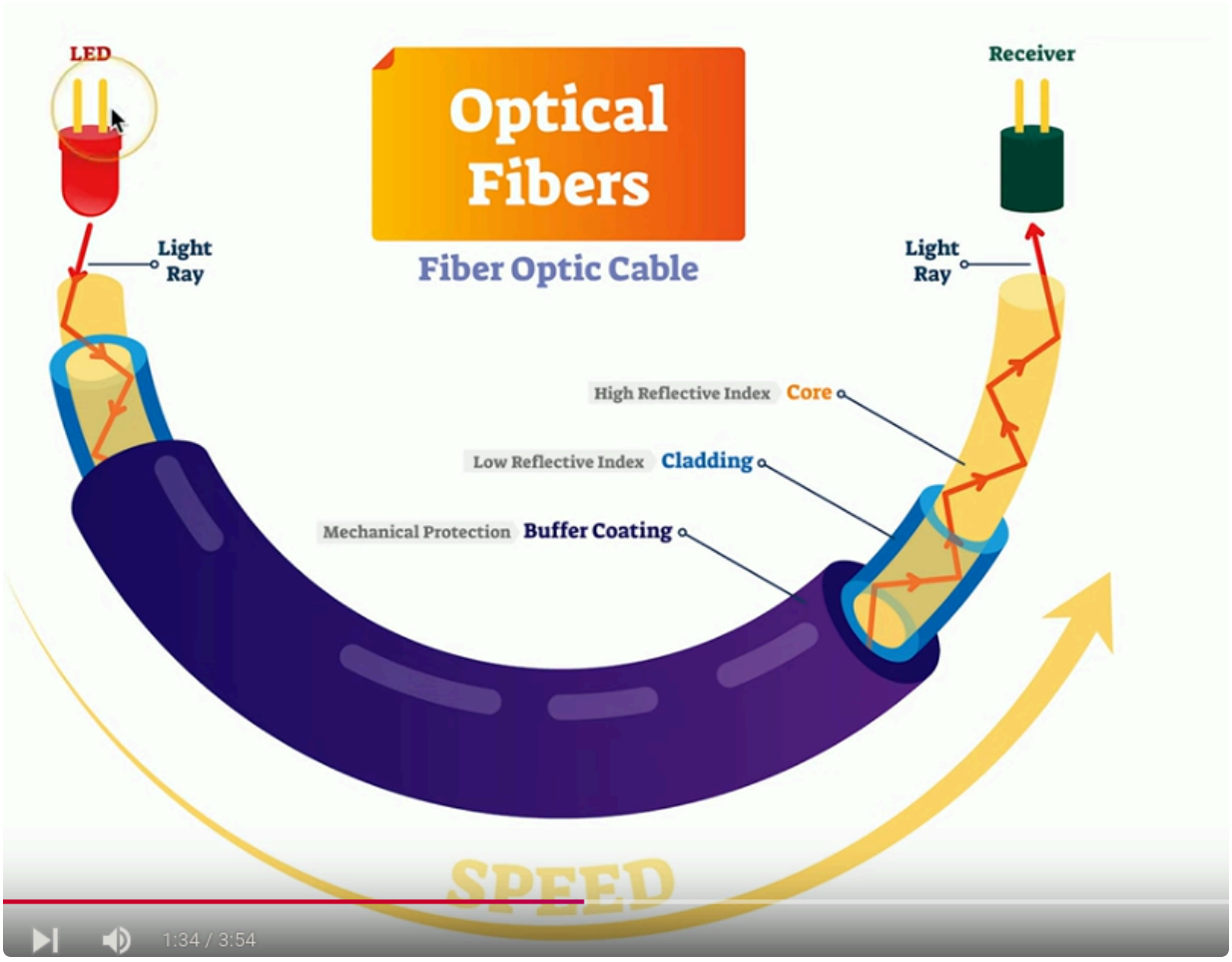


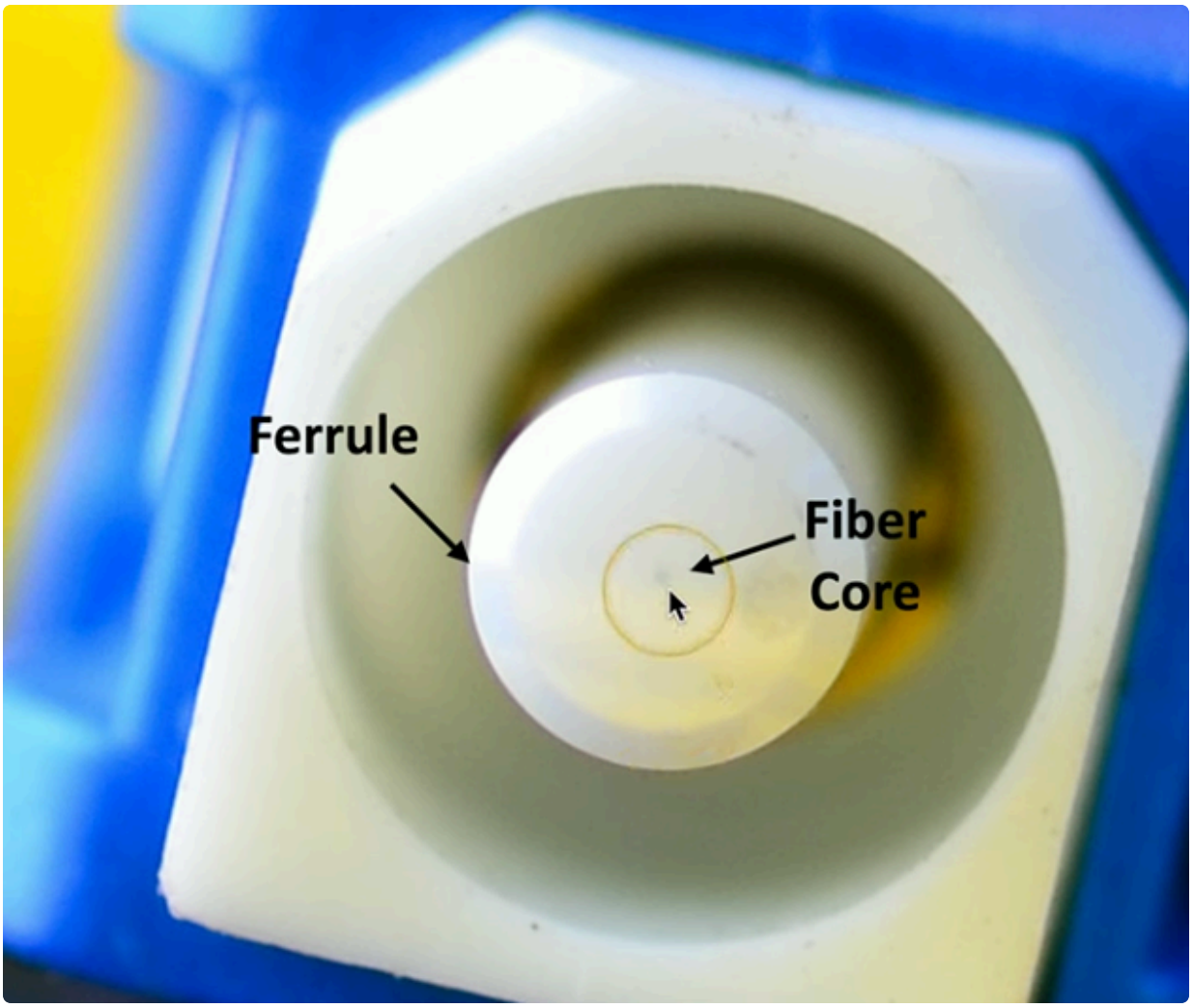
1.5 Optical Fiber

Fiber Communication

- Transmission by light -> visible spectrum
- No RF signal -> Very difficult to monitor or tap
- Signal slow to degrade -> Transmission over long distances
- Immune to radio interferance

Anatomy of Fiber Optic Cable


LED
Optical Fibers
Receiver
Light Ray
Fiber Optic Cable
Light Ray
High Reflective Index
Core
Low Reflective Index
Cladding
Mechanical Protection
Buffer Coating
SPEED
1:34 / 3:54

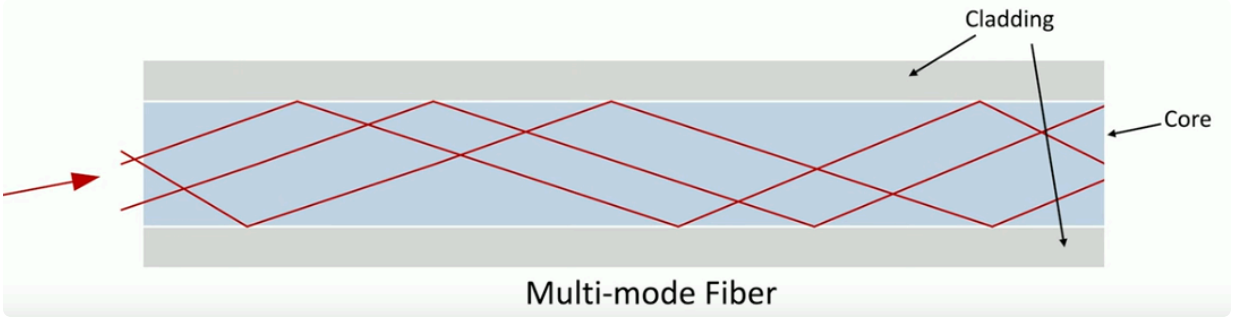


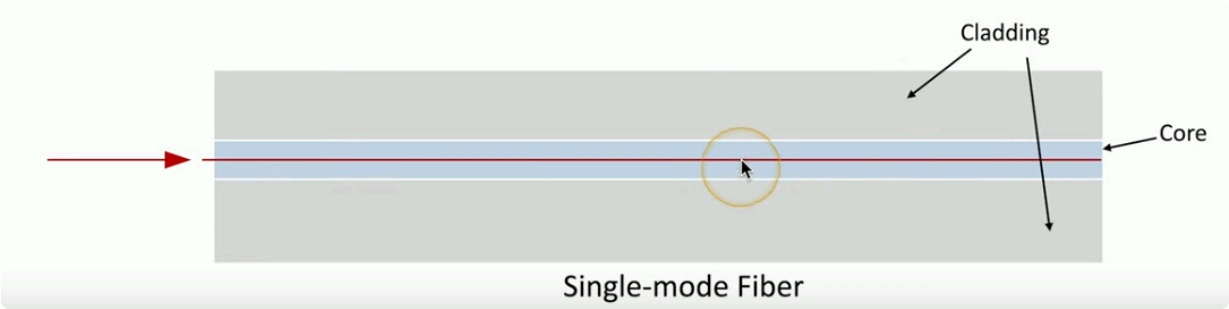
Multimode Fiber

- Short range communication -> Up to 2km
- Inexpensive light source -> Ex: LED

Single-mode Fiber

- Long range communication -> Up to 100km without processing
- Expensive light source -> Laser beams





1.5 Copper Cabling
https://www.youtube.com/watch?v=zoefzxHIfPc&list=PLG49S3nxzAnl_tQe3kvnmeMid0mjF8Le8&index=14

1.5 Network Transceivers
Transceiver

- Transmitter and receiver -> Usually in a single component
- Provides a modular interface -> Add the transceiver that matches your network
- Diff types -> Ethernet or Fibre Channel (Not compatible with each other)
  SFP and SFP+
- Small Form-factor Pluggable (SFP)
  - Commonly used to provide 1Gbit/s fiber
- Enhanced Small Form-factor Pluggable (SFP+)
  - Exactly same physical size SFP's
  - Data rates up to 16Gbit/s, common with 10 Gigabit Ethernet
  QSFP
- Quad Small Form-factor Pluggable
  - 4 Channel SFP = Four 1Gbit/s = 4Gbit/s
  - QSFP+ is a four channel SFP+ Four 10 Gbit/sec = 40Gbit/sec

1.5 Fiber Connectors
https://www.youtube.com/watch?v=PNoqhs5QvFw&list=PLG49S3nxzAnl_tQe3kvnmeMid0mjF8Le8&index=16

1.5 Copper Connectors
RJ11 Connector

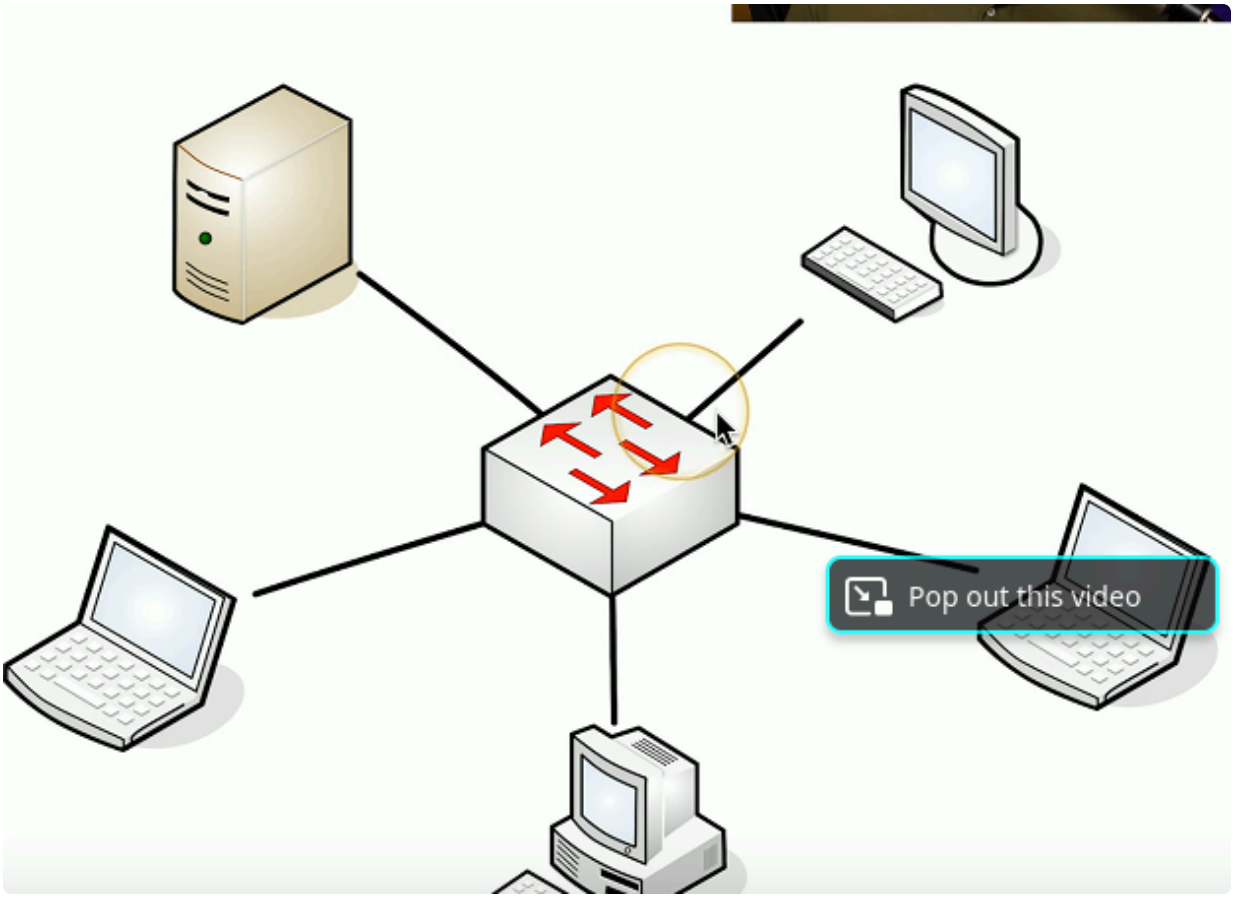
- Registered Jack type 11
  - 6 Position , 2 Conductor (6P2C)

- Telephone & DSL Connection
  RJ45 Connector
- Registed Jack Type 45
- 8 Position, 8 Conductor (8P8C) -> Modular Connector, Ethernet
  F-Connector
- Coaxial cable
  - Standard connector type, threaded connector
- Cable television infrastructure
  - Cable modem
  - DOCSIS (Data Over Cable Service Interface Specification)
  BNC Connector
- Bayonet Neill-Concelman
- Another common coaxial cable connector
  - Secure due to twist and lock in place
  - Common with twinax and DS3 WAN Link
  - Video connections

1.6 Network Topologies

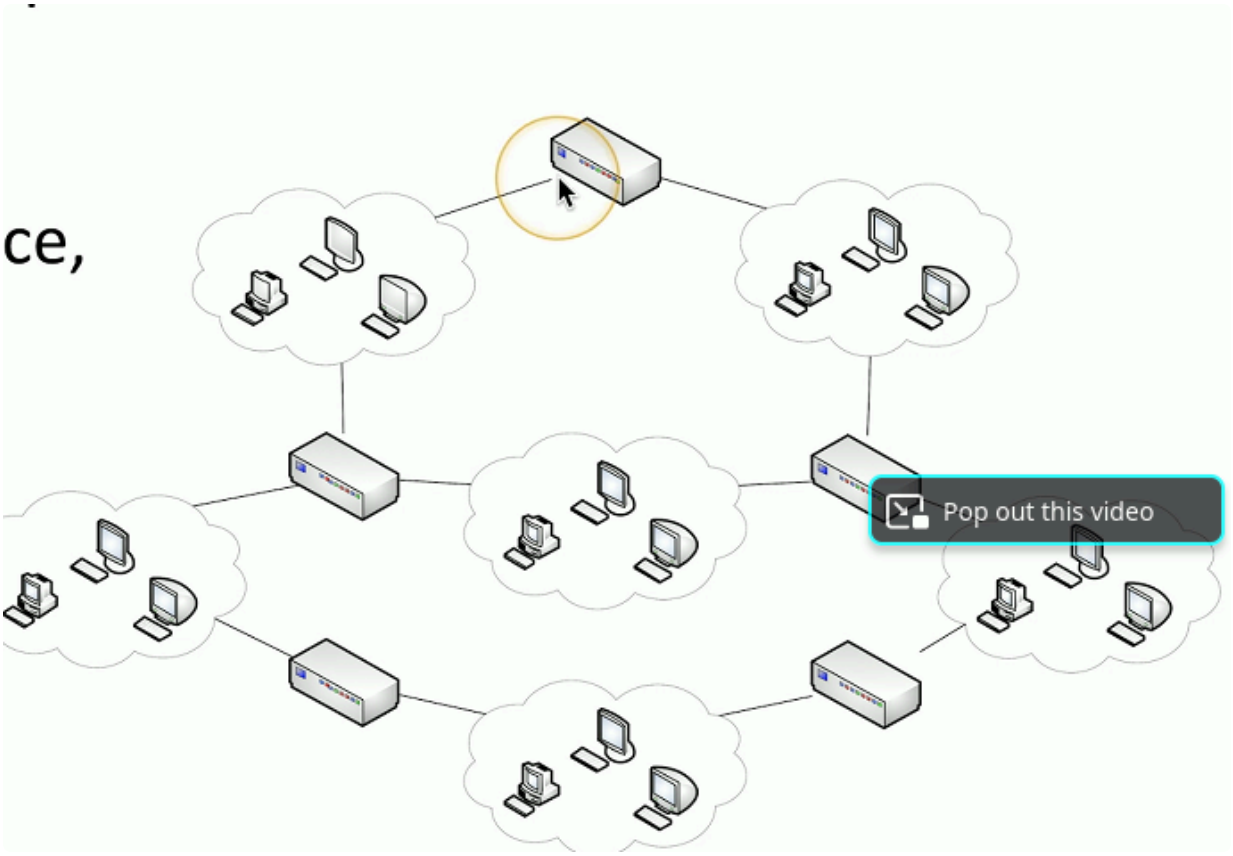
- Useful in planning a new network
  - Analogy -> Physical layout of a building or campus
- Assists in understanding signal flow and troubleshooting problems
  Star/Hub and spoke
- Used in most large and small networks
- All devices are connected to a central device

- Switched Ethernet networks -> The switch is in the middle



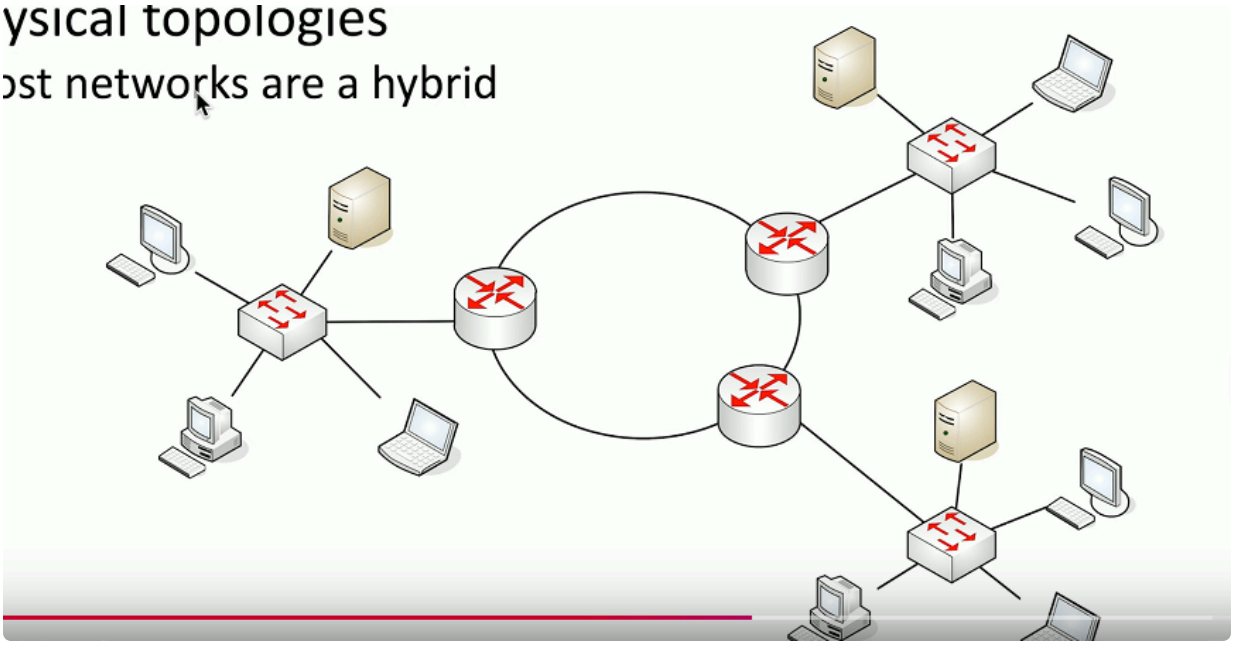
Mesh Network

- Multiple Links to same place
  - Fully connected or partially connected
- Redundancy, fault tolerance, load balancing
- Used in Wide Area Networks (WAN's)
  - Fully meshed and partially meshed



Hybrid

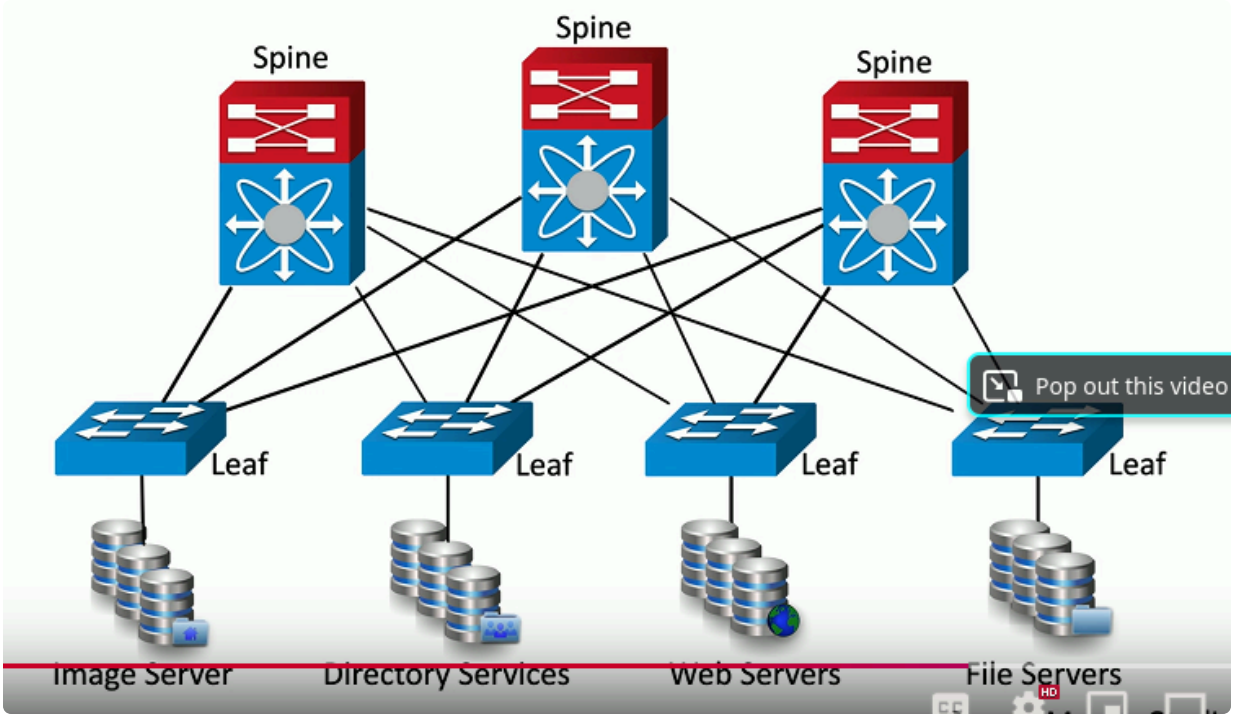
- A combination of one or more physical topologies
- Most networks are a hybrid



Spine and Leaf Architecture

- Each leaf switch connected to each spine switch
  - Each spine switch connects to each leaf switch
- Leaf switches do not connect to each other and spine switches do not connect to each other

- Top-of-rack switching
  - Each leaf is on the "top" of a physical network rack
  - May include a group of physical racks
  - Advantages: Simple cabling, redundant, fast
  - Disadvantages: Additional switches may be costly



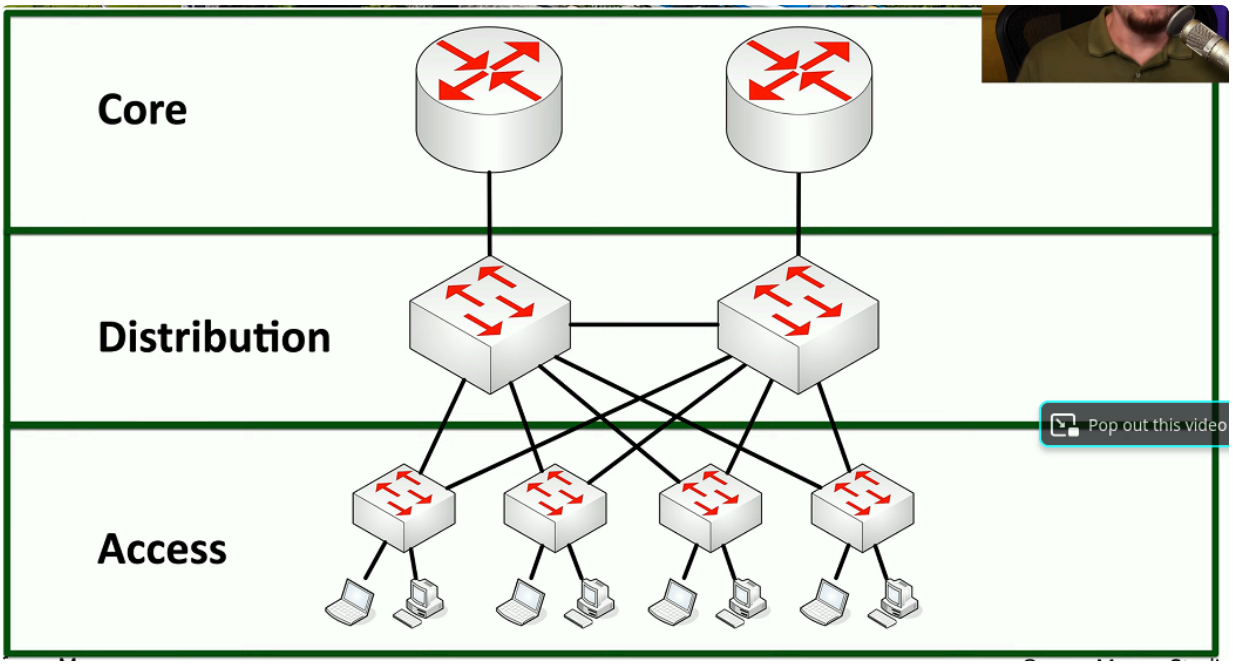
Point-to-point

- One-to-one connection
- Older WAN link
  - Point-to-point T-1
- Connections between buildings on campus

1.6 Network Architectures

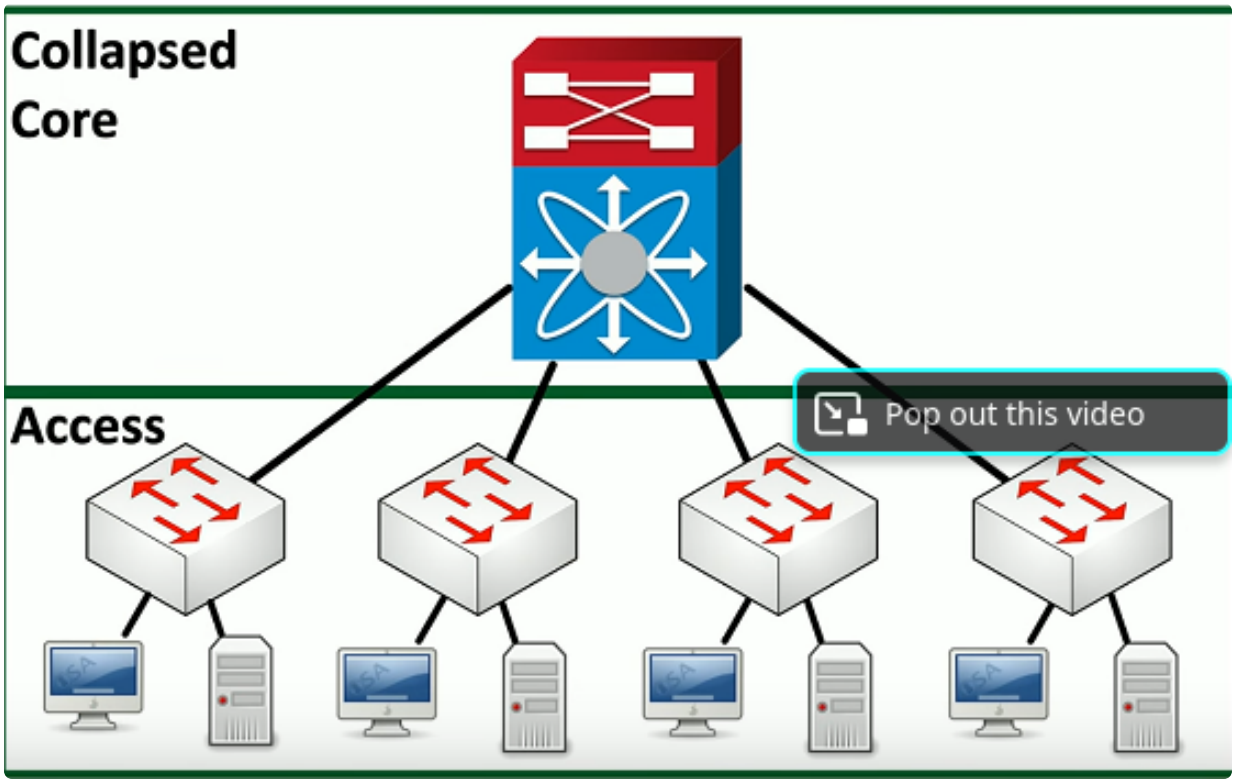
Three tier architecture

- Core
  - "Center" of network
  - Web servers, databases, applications
  - Many people need access tot his
- Distribution
  - Midpoint between the core and the users
  - Communication between access switches
  - Manage path to the end users
- Access
  - Where users connect -> End stations, printers etc



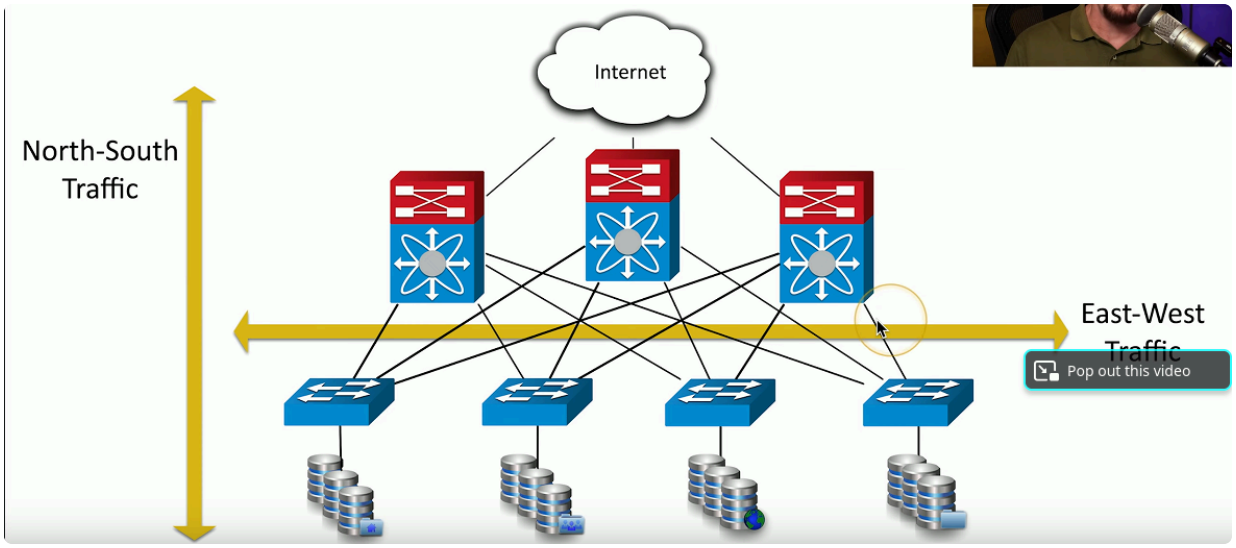
Collapsed core

- A two tier model
  - Simply the three-tier architecture
  - Good for smaller organizations
- Combine Core and Distribution Layer -> Collapse together
- Differences over three tier:
  - Simpler to design and support
  - Less expensive to implement
  - Not as resilient



Traffic Flows

- Traffic flows withing a data center
  - Important to know where traffic starts and ends
- East-west
  - Traffic between devices in the same data center
  - Relatively fast response times
- North-south traffic
  - Ingress/egress to an outside device
  - A different security posture than east-west traffic



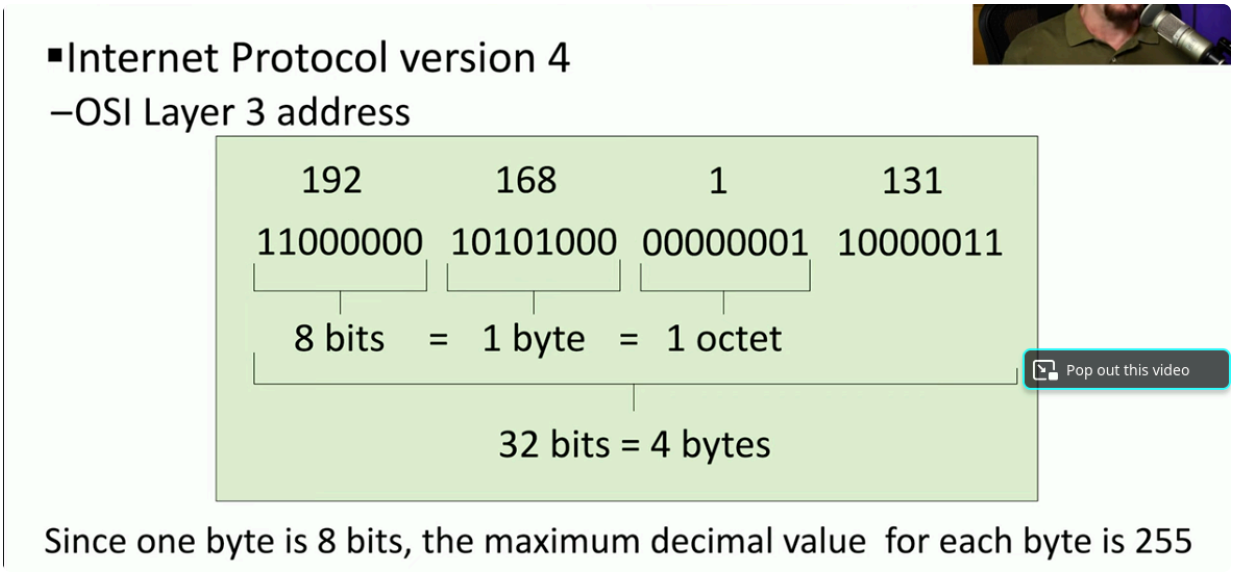
1.7 Binary Math

https://www.youtube.com/watch?

v=94dcHJfEAIo&list=PLG49S3nxzAnl_tQe3kvnmeMid0mjF8Le8&index=20

1.7 IPv4 Addressing

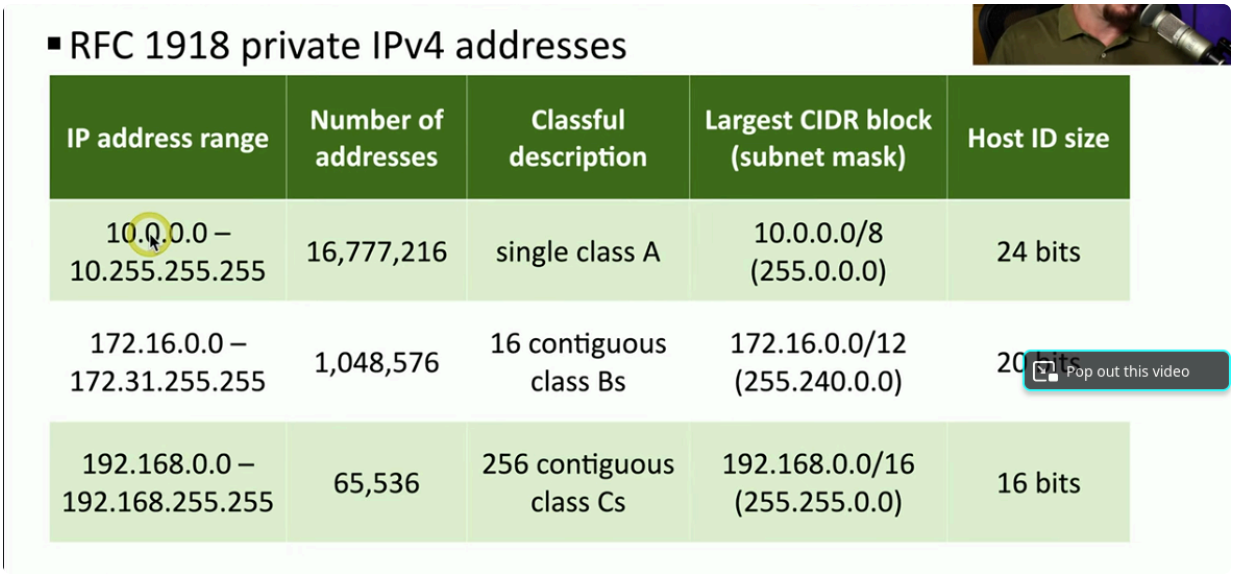
- IP Address, e.g, 192.168.1.165
  - Every device needs a unique IP address
- Subnet mask, e.g, 255.255.255.0
  - Used by local device to determine what subnet it's on
  - Not usually transmitted across the network
- Default gateway, e.g, 192.168.1.1
  - The router that allows you to communicate outside of your local subnet
  - The default gateway must be an IP address on the local subnet
- Loopback address
  - An address to yourself-> Ranges from 127.0.0.1 through 127.255.255.254
  - Easy way to self reference is to -> ping 127.0.0.1
- Reserved addresses
  - Set aside for future use or testing
  - 240.0.0.1 through 254.255.255.254
  - All "Class E" Addresses
- Virtual IP addresses (VIP)
  - Not associated with a physicial network adapter
  - Virtual machine, internal router address



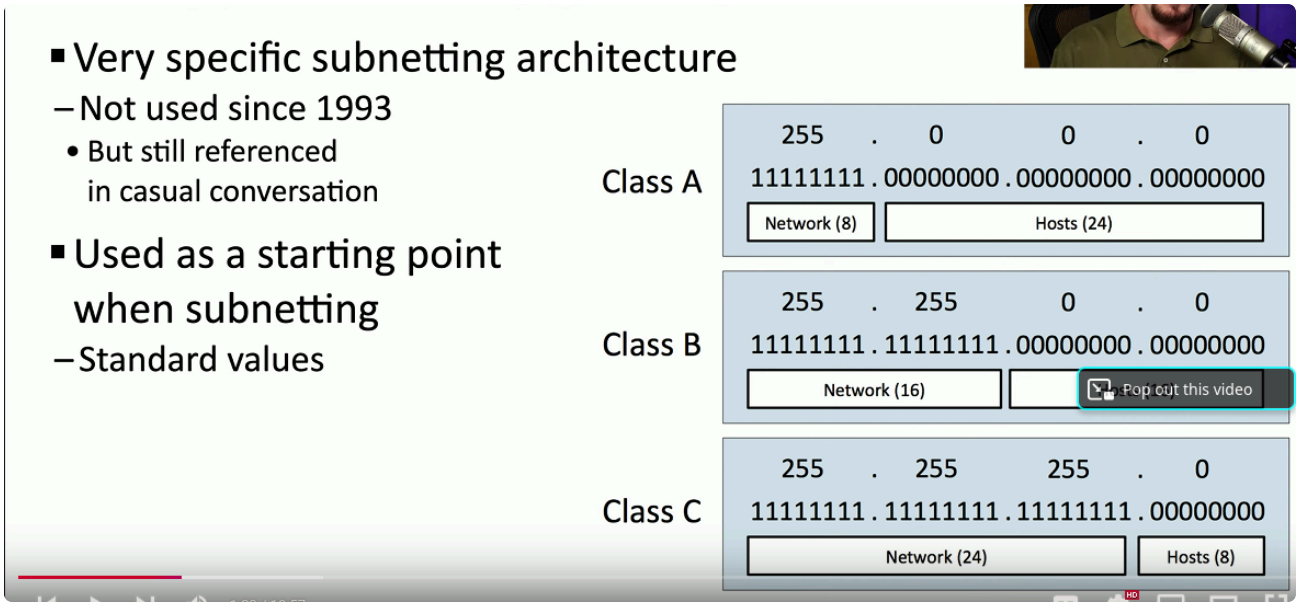
DHCP

- IPv4 address config used to be a manual process
  - IP address, subnet mask, gateway, DNS servers, NTP servers, etc

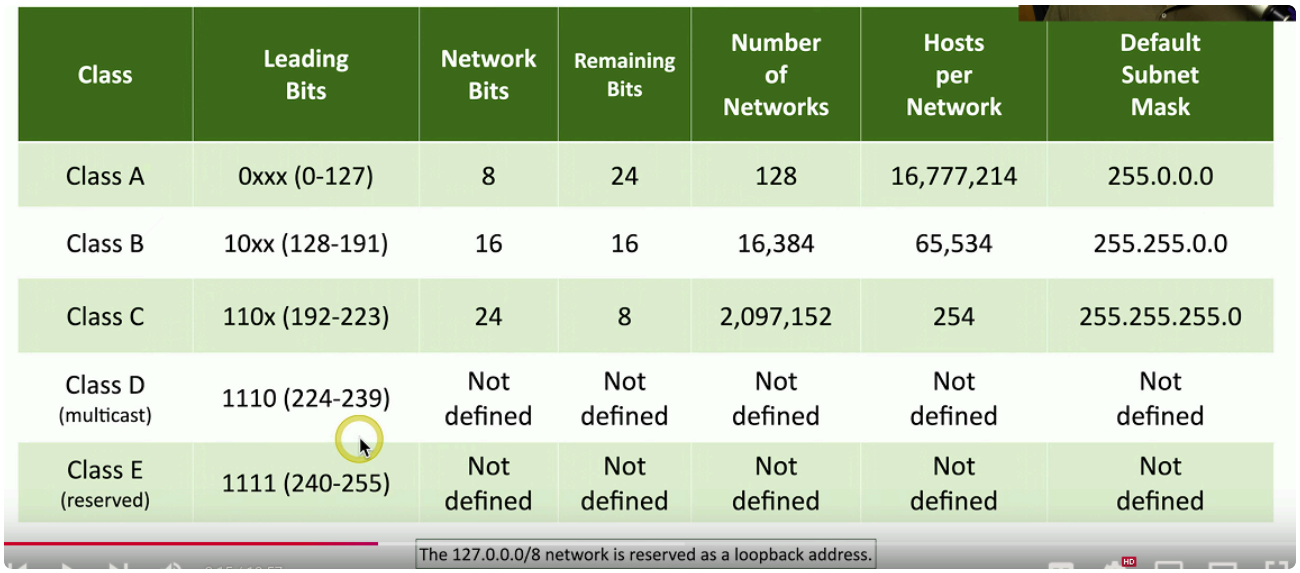
- DHCP (Dynamic Host Configuration Protocol) automatically provides addresses and IP configurations for almost all devices
  Automatic Private IP Addressing (APIPA)
- A link-local address
  - Can only communicate to other local devices
  - No forwarding by routers
- IETF has reserved 169.254.0.1 through 169.254.255.254
  - First and last 256 addresses are reserved
  - Functional block of 169.254.1.0 through 169.254.254.255
- Automatically assigned -> Uses ARP to confirm address isn't currently in use
  Private IP Address
- Can not be routed on the internet
- Can only be used inside the local network
- Private IP addresses allow for more public IP addresses
- We can connect to internet with private IP through the help of NAT (Network Address Translation), which translates our private IP to a public IP



1.7 Classful Subnetting



Subnet Classes

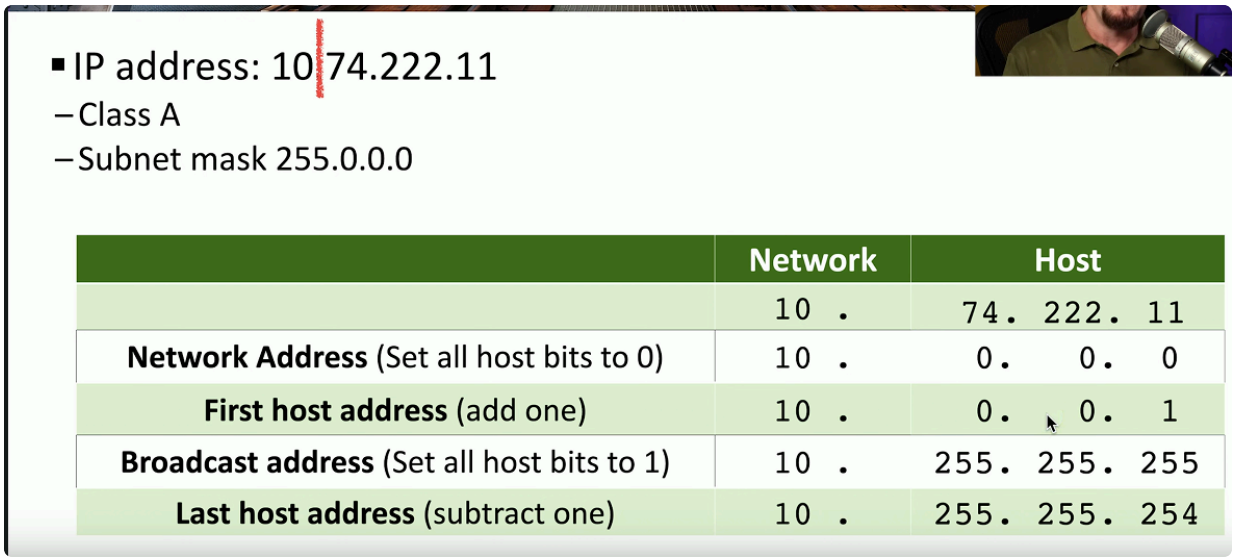


Class	Leading Bits	Network Bits	Remaining Bits	Number of Networks	Hosts per Network	Default Subnet Mask
Class A	0xxx (0-127)	8	24	128	16,777,214	255.0.0.0
Class B	10xx (128-191)	16	16	16,384	65,534	255.255.0.0
Class C	110x (192-223)	24	8	2,097,152	254	255.255.255.0
Class D (multicast)	1110 (224-239)	Not defined	Not defined	Not defined	Not defined	Not defined
Class E (reserved)	1111 (240-255)	Not defined	Not defined	Not defined	Not defined	Not defined

Construction of a Subnet

- Network address
  - First IP address of a subnet
  - Set all host bits to 0 (0 Decimal)
- First usable host address
  - One number higher than the network address
- Network broadcast address
  - Last IP address of a subnet
  - Set all host bits to 1 (255 decimal)
- Last usable host address
  - One number lower than the broadcast address

Subnet Calculations



Through first octets decimal value we can classify as Class A. This lets us know the subnet mas is 255.0.0.0, In order to get our network address we must take our first octet value and then set the remaining to 0 decimal giving us 10.0.0.0.

1.7 IPv4 Subnet Masks

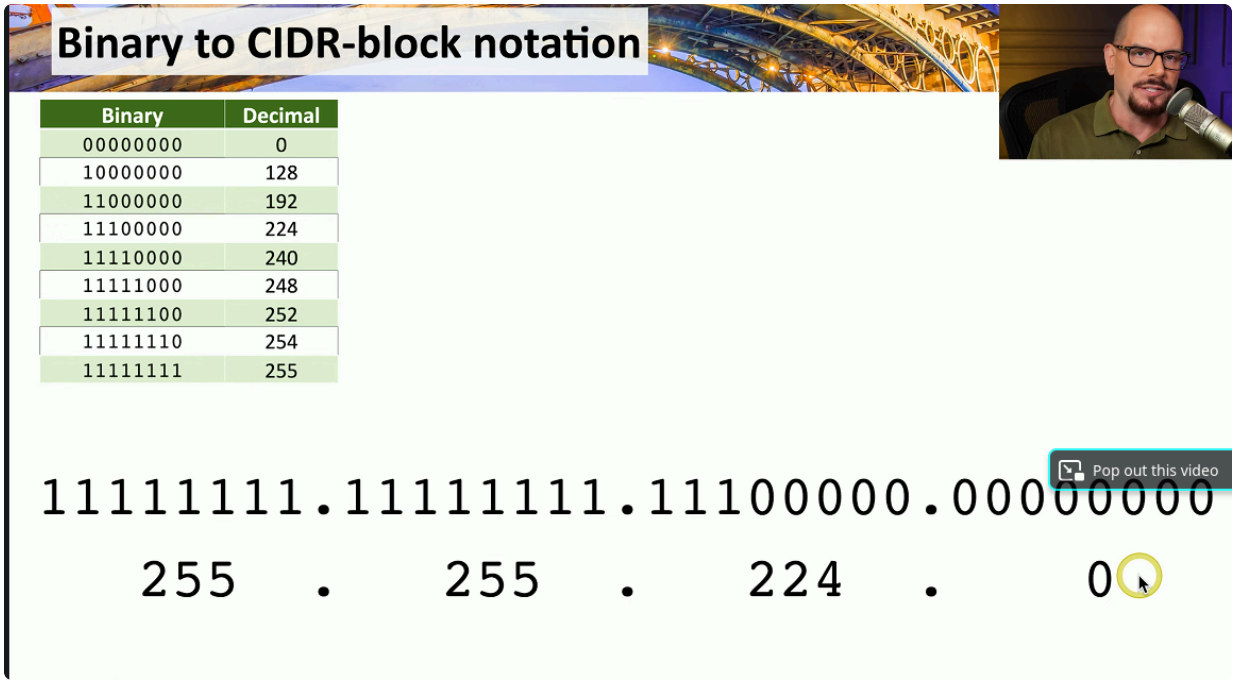
- CIDR (Classless Inter-Domain ROuting)
  - Created around 1993, Removed restrictions created by classful subnet masks
  - "Cider" block notation

Binary	Decimal	CIDR
11111111.00000000.00000000.00000000	255.0.0.0	/8
11111111.11111111.00000000.00000000	255.255.0.0	/16
11111111.11111111.11111111.00000000	255.255.255.0	/24

Ex: 255.0.0.0 = /8 in Cider notation

- Subnet masks can be expressed as decimal or in CIDR notation
  - IP address, slash, number of subnet bits.
    - 192.168.1.44/24
- You are usually provided an IP address, subnet mask, default gateway, and DNS server
  - Some OS are expecting decimal marks other are expecting CIDR notation marks
- /8 would indicate 8 network bits and 24 host bits

- 1's on left indicate num of network bits



1.7 Calculating IPv4 Subnets and Hosts

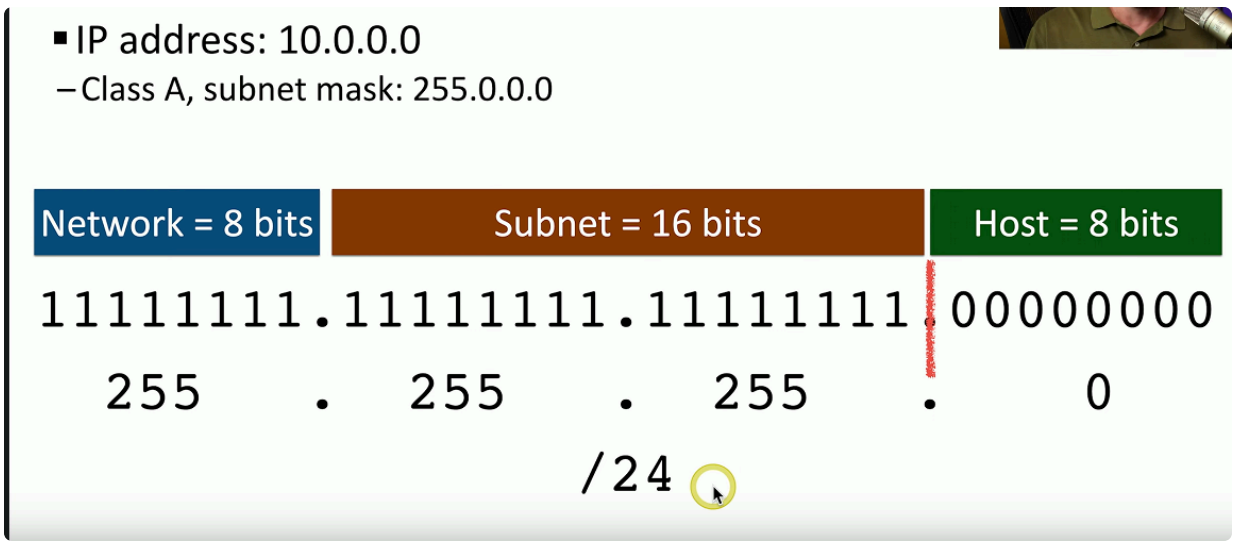
VLSM (Variable Length Subnet Masks)

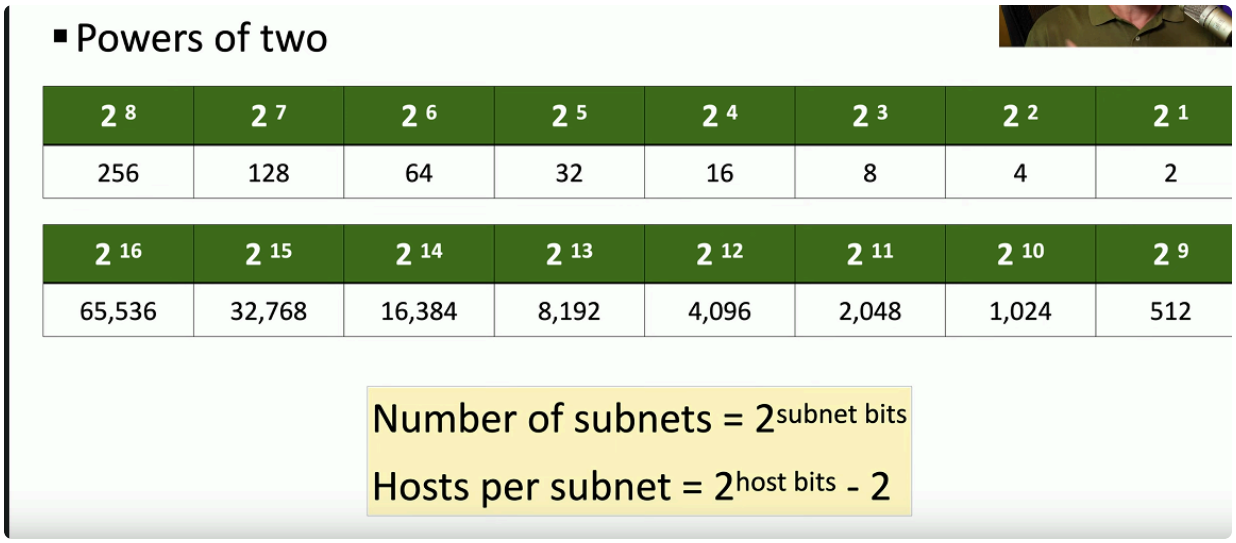
- Class-based networks are inefficient
- VLSM allows network admins to define their own masks
  - Customize subnet mask to specific network requirements
- Use different subnets masks in the same classful network

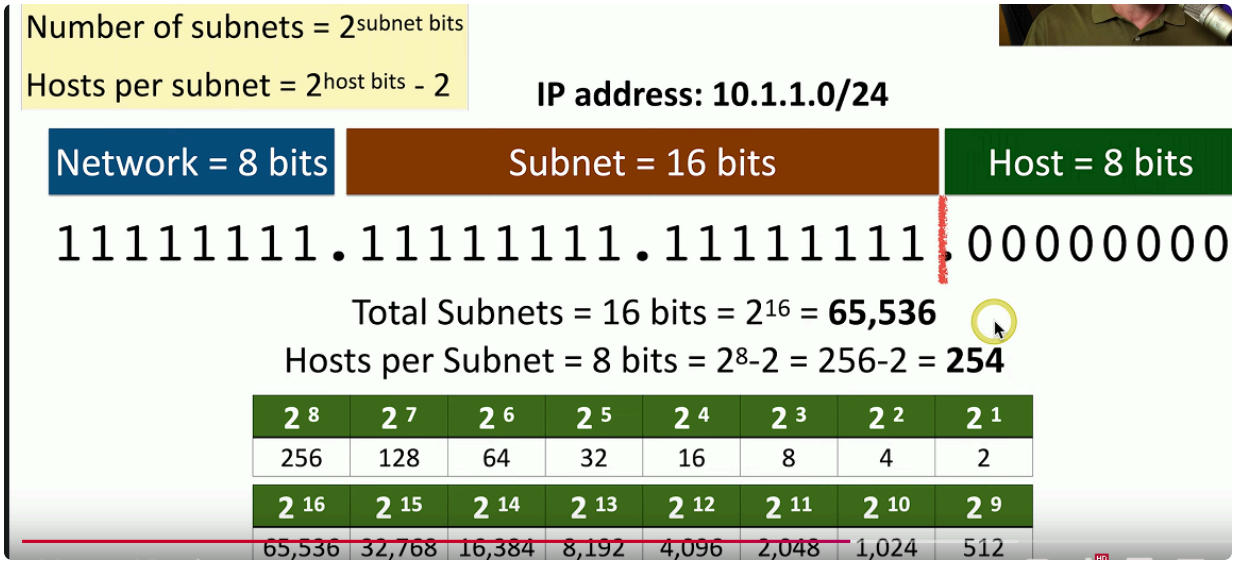
  - 10.0.0.0/8 is the class A network

  - 10.0.1.0/24 and 10.0.8.0/26 would be VLSM

Defining Subnets

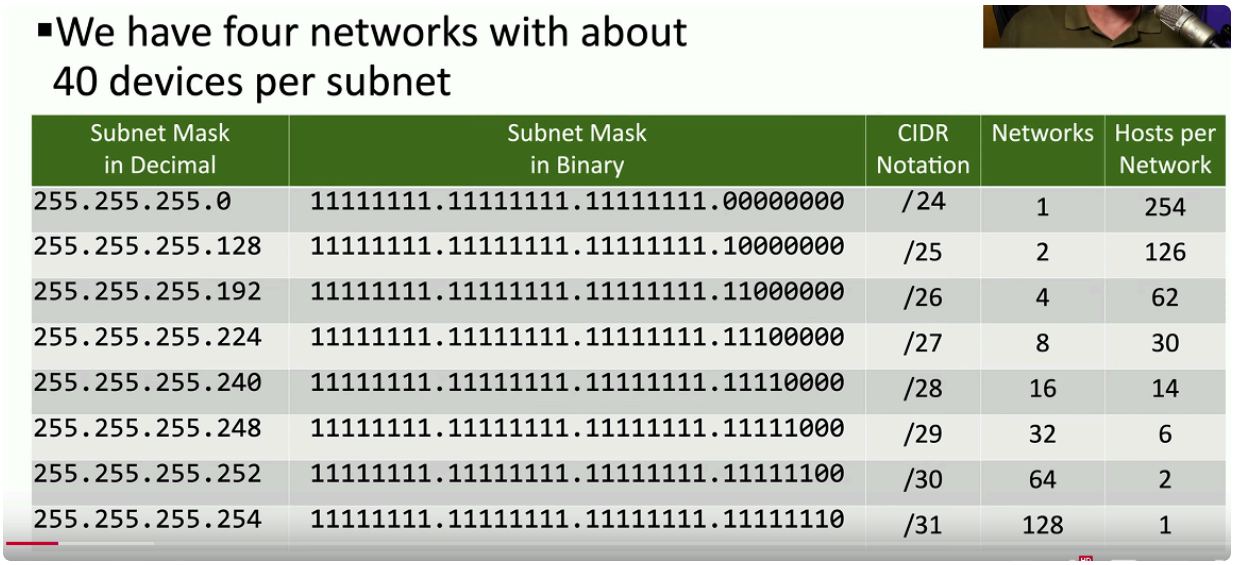






1.7 Magic Number Subnetting

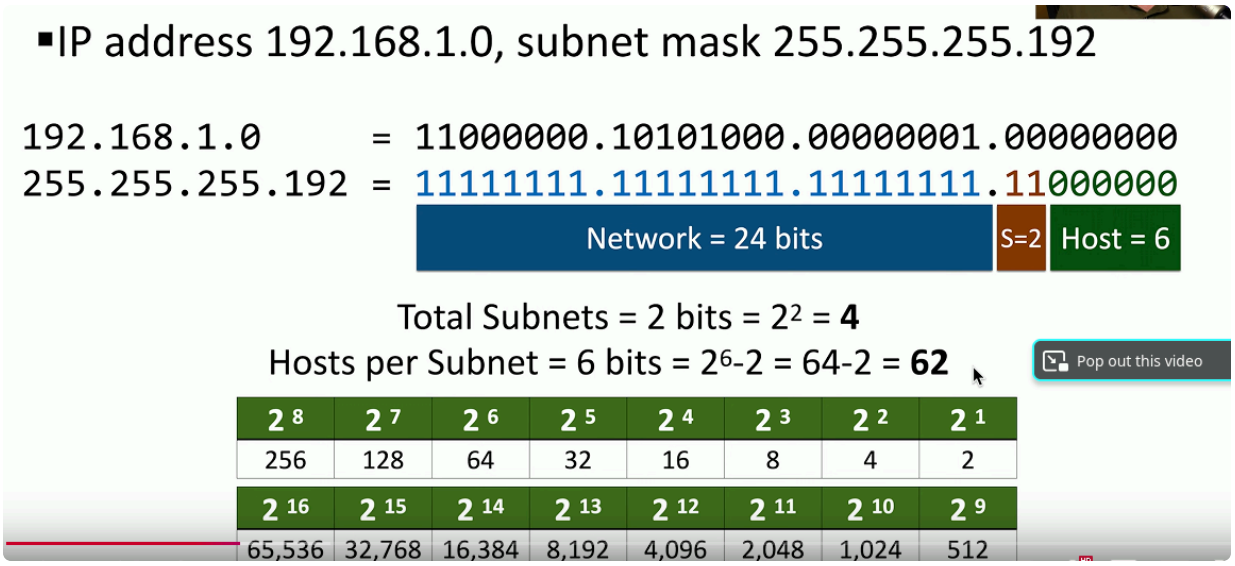
- Say we have IP address assignment
  - Network: 192.168.1.0/24
- We need an IP addressing scheme with more than one network address that can supports 40 devices per subnet



Subnet Mask in Decimal	Subnet Mask in Binary	CIDR Notation	Networks	Hosts per Network
255.255.255.0	11111111.11111111.11111111.00000000	/24	1	254
255.255.255.128	11111111.11111111.11111111.10000000	/25	2	126
255.255.255.192	11111111.11111111.11111111.11000000	/26	4	62
255.255.255.224	11111111.11111111.11111111.11100000	/27	8	30
255.255.255.240	11111111.11111111.11111111.11110000	/28	16	14
255.255.255.248	11111111.11111111.11111111.11111000	/29	32	6
255.255.255.252	11111111.11111111.11111111.11111100	/30	64	2
255.255.255.254	11111111.11111111.11111111.11111110	/31	128	1

IP address = 192.168.1,9 == 11000000.10101000.00000001.00000000
Subnet mask = 255.255.255.192 = 11111111.11111111.11111111.11000000

- We can see why we chose this subnet mask from the diagram above which shows that when choosing /26 Subnet mask we get 4 networks and 62 hosts per network which is closest to our 40 devices per subnet and number of networks.
  - Also note how as networks increase hosts per network decrease (inverse)



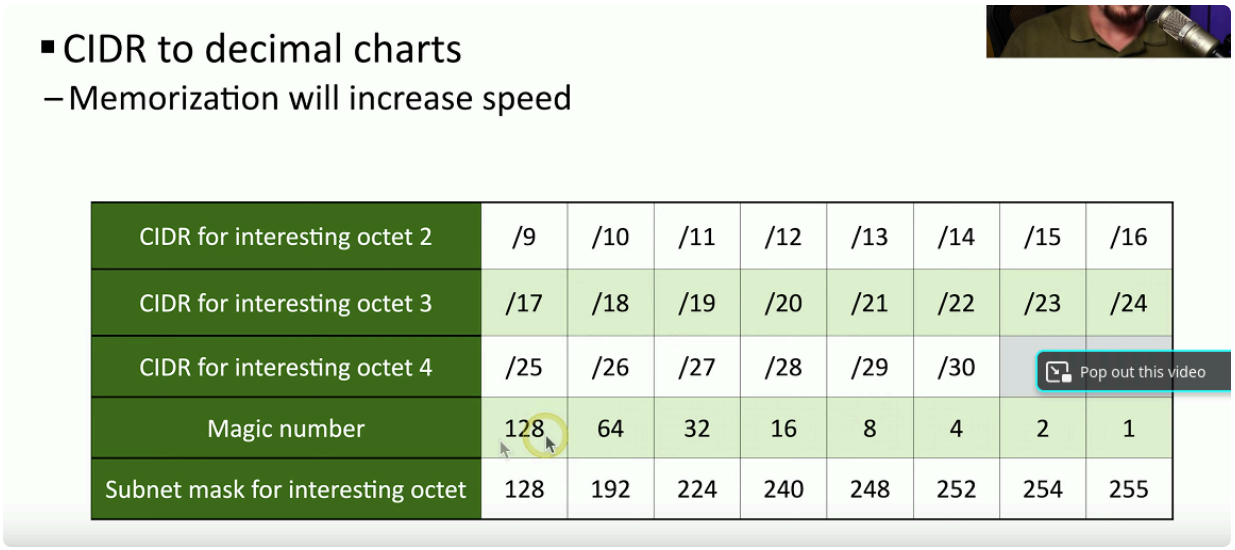
2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1
256	128	64	32	16	8	4	2

2^{16}	2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^9
65,536	32,768	16,384	8,192	4,096	2,048	1,024	512

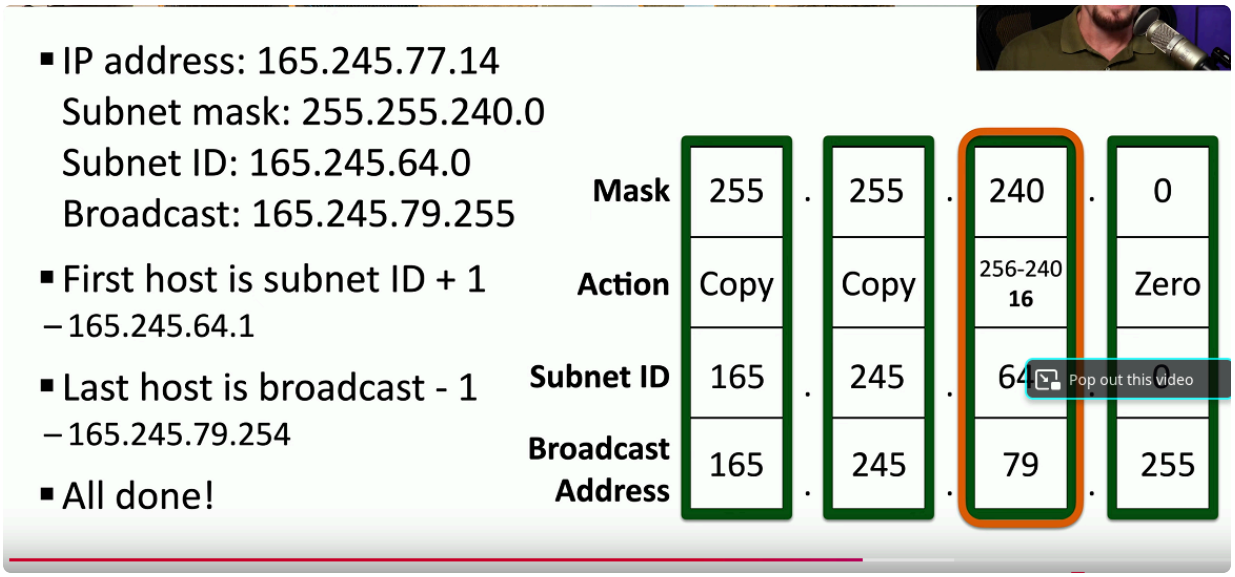
Wanted Addresses :

- Network address/subnet ID -> First address in the subnet
- Broadcast address -> Last address in the subnet
- First available host address -> Network address + 1
- Last available host address -> Broadcast address -1

Magic Number Chart:

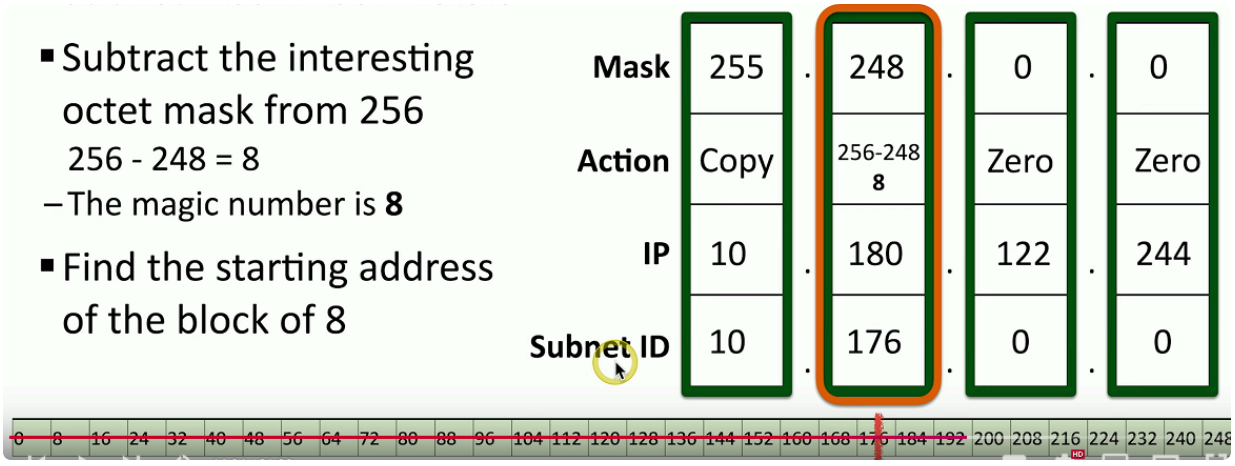


CIDR for interesting octet 2	/9	/10	/11	/12	/13	/14	/15	/16
CIDR for interesting octet 3	/17	/18	/19	/20	/21	/22	/23	/24
CIDR for interesting octet 4	/25	/26	/27	/28	/29	/30		
Magic number	128	64	32	16	8	4	2	1
Subnet mask for interesting octet	128	192	224	240	248	252	254	255

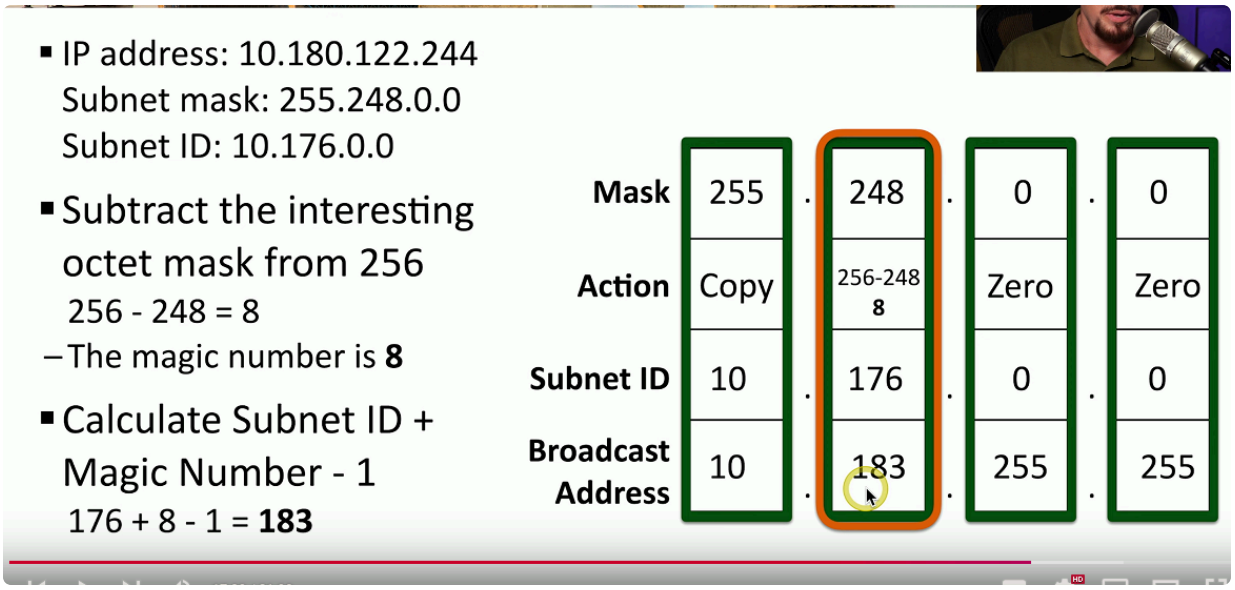


For broadcast - subtract our mask non 255 number from 256 and then take our magic number and add it to the corresponding subnet ID - 1 -> So 16+64-1 = 79

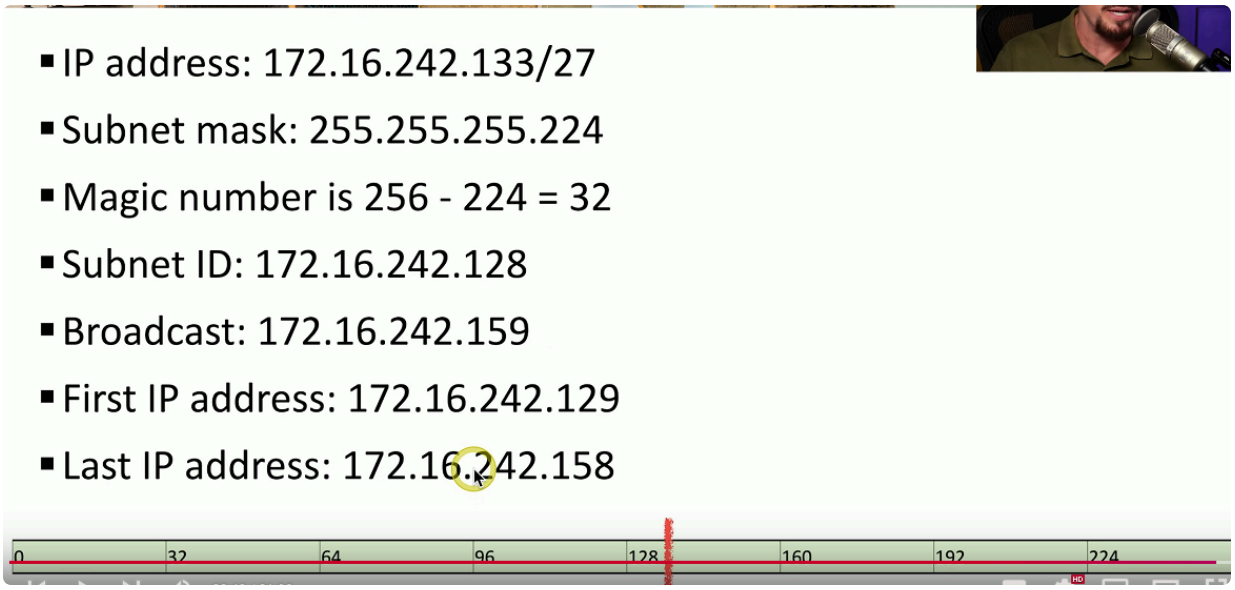
- For 255 in Mask we Copy the IP val to Subnet ID and for any zeroes we place zeros in same corresponding location
- However for calculating broadcast we replace 0 vals with 255



180 corresponds to octet block start at 176 so starting address would be 176



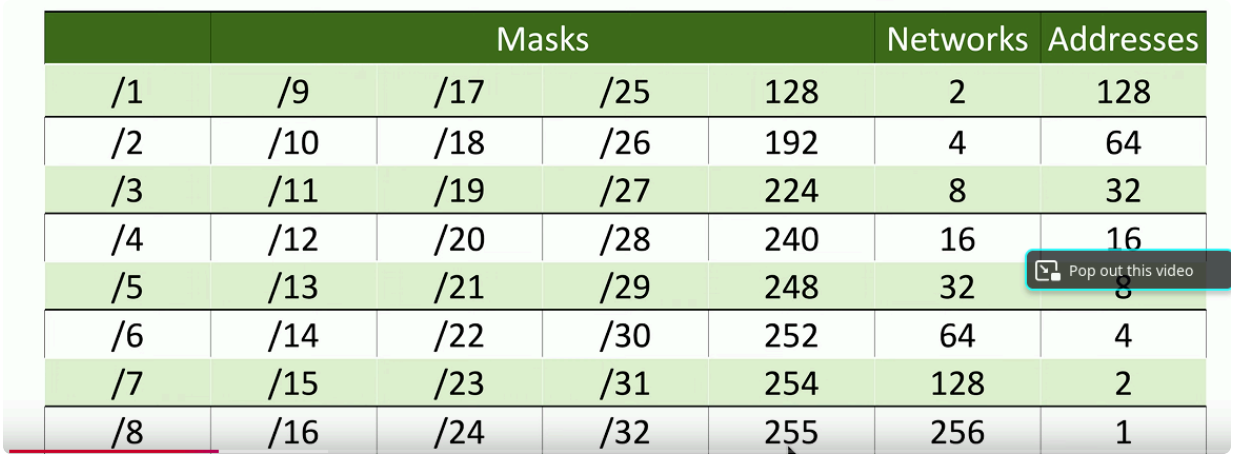
Faster process using CIDR Block Interesting Octet Chart



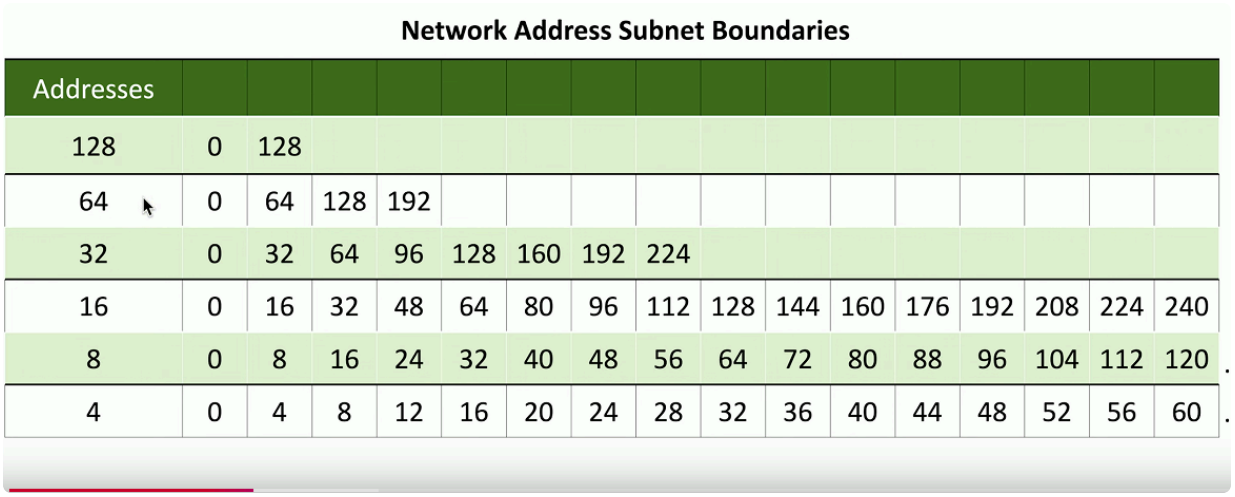
- From /27 we know we are in look for interesting octet 4 and for 27 this is 224
  - So subnet = 255.255.255.224 <- Interesting octet 4
  - 256-224 = 32 Gives us our magic number, we use this to see how we split our ranges from 0-255, 133 clearly in 128 range so we use starting val 128 for our Subnet ID : 172.16.242.128
  - Broadcast ID Value 4 = Subnet ID interesting val + Magic Number - 1
    - 128+32-1 = 159
  - From there on we simply add 1 to subnet ID for first address and remove 1 from broadcast ID for last address

1.7 Seven Second Subnetting

- Designed for exams -> Fast subnetting -> No second guessing

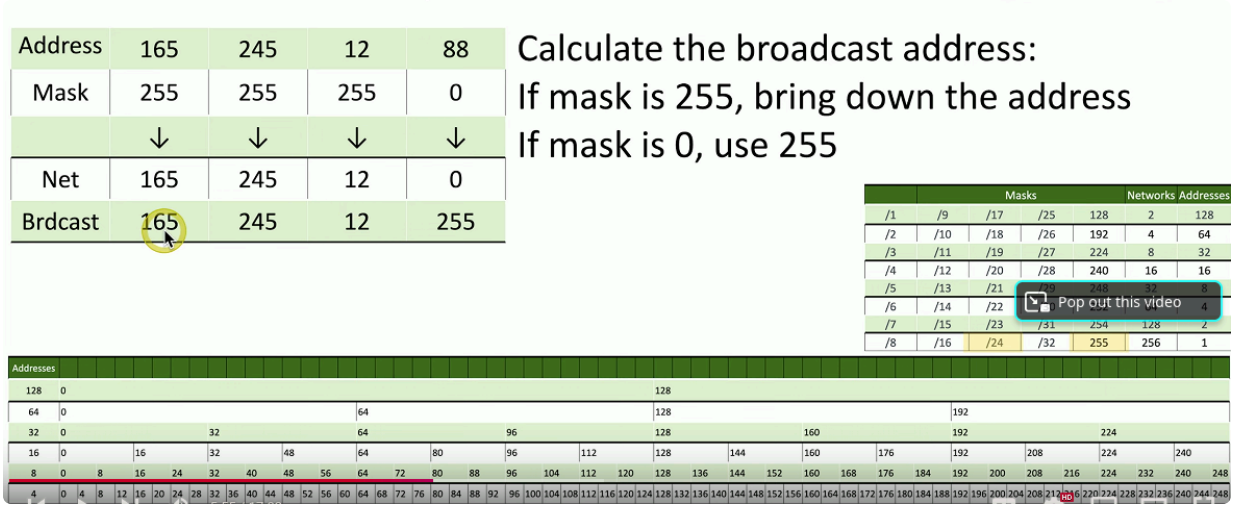


	Masks				Networks	Addresses
/1	/9	/17	/25	128	2	128
/2	/10	/18	/26	192	4	64
/3	/11	/19	/27	224	8	32
/4	/12	/20	/28	240	16	16
/5	/13	/21	/29	248	32	8
/6	/14	/22	/30	252	64	4
/7	/15	/23	/31	254	128	2
/8	/16	/24	/32	255	256	1



Network Address Subnet Boundaries

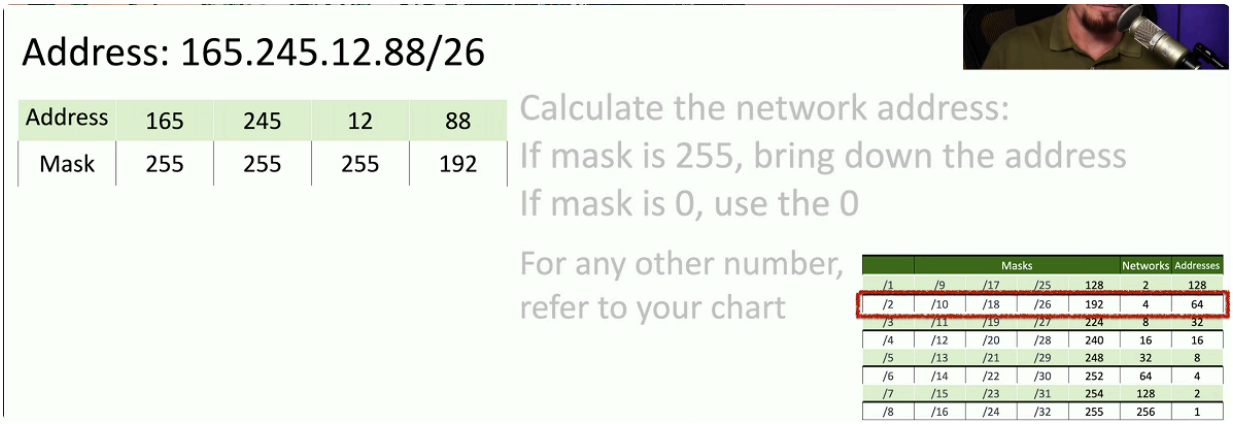
Addresses																
128	0	128														
64	0	64	128	192												
32	0	32	64	96	128	160	192	224								
16	0	16	32	48	64	80	96	112	128	144	160	176	192	208	224	240
8	0	8	16	24	32	40	48	56	64	72	80	88	96	104	112	120
4	0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60



Address	165	245	12	88
Mask	255	255	255	0
	↓	↓	↓	↓
Net	165	245	12	0
Brdcast	165	245	12	255

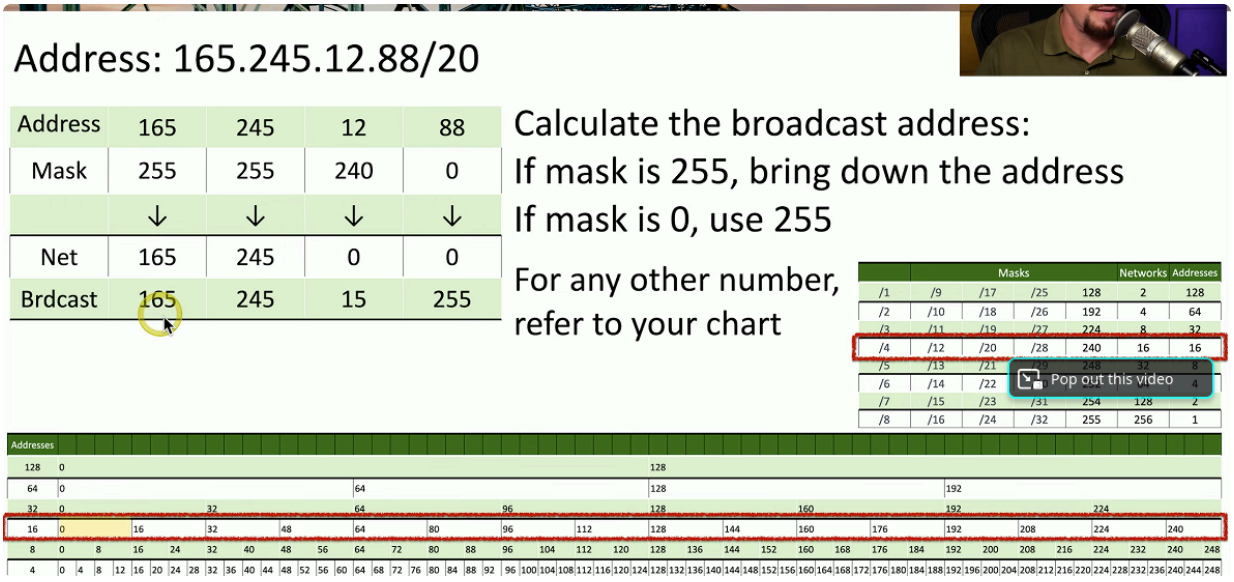
Calculate the broadcast address:
If mask is 255, bring down the address
If mask is 0, use 255

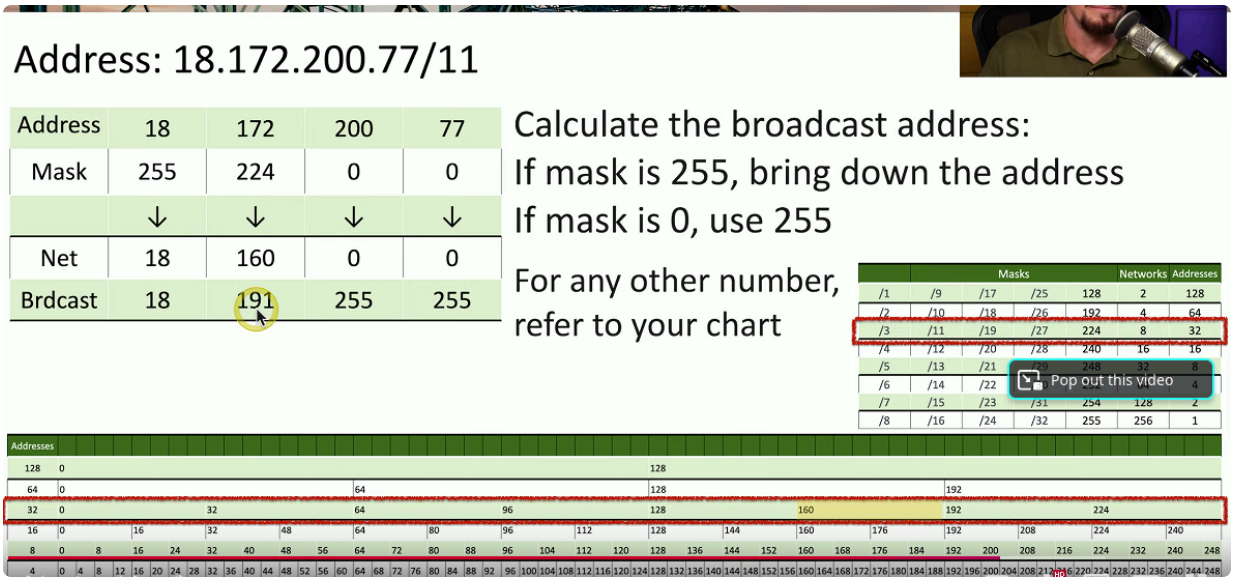
- First IP is Net address +1 -> Last IP is Broadcast address -1



- /26 so we refer to chart -> Here we see we are looking for interesting octet 4 and value is 192 as said in chart
  - Therefore we bring 255 down for first 3 octets and then 192 for the interesting octet in order to obtain our subnet mask
- For Net address bring original IP down for all sections with 255 in it, for the area in the interesting octet refer to the address section of the chart. We are given 64 and our original IP is 88, this clearly corresponds to starting address 64 as seen here. So Net IP -> 165.245.12.64

- For broadcast instead we see that 88's next starting block would be 128, so we do 128-1 to obtain our broadcast addresses last value
  - Broadcast IP -> 165.245.12.127





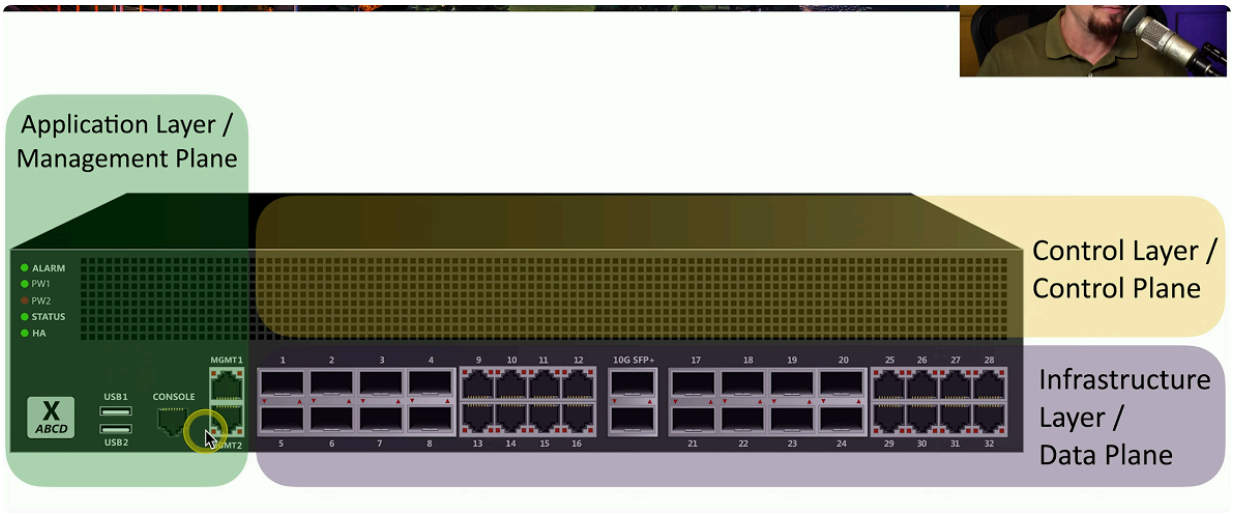
Note how for CDIR /11 we are interested in octet 2 (172), this tells us to use 224 as its subnet mask value, and all others become 0'sa

- Same chart tells use to use 32 Address blocks, 172 is contained by the 160 block so we use 160 for our net value of octet 2 and bring the zeros down
- Lastly Broadcast is next CIDR block starting point -1, as we see this would be 192 for CIDR /11. So we get 192-1 = 191 for our second octet value and then 255 for octet 3 and 4 as 0's in subnet mask become 255 on broadcast address.

1.8 Software Defined Networking (SDN)

- Infrastructure layer/ Data plane (Ex: switch/router)
  - Process the network frames and packets
  - Forwarding, trunking, encrypting, NAT
- Control layer/ Control plane
  - Manages the actions of the data plane
  - Routing tables, session tables, NAT tables
  - Dynamic routing protocol updates
- Application layer/ Management plane
  - Configure and manage the device
  - SSH, browser, API

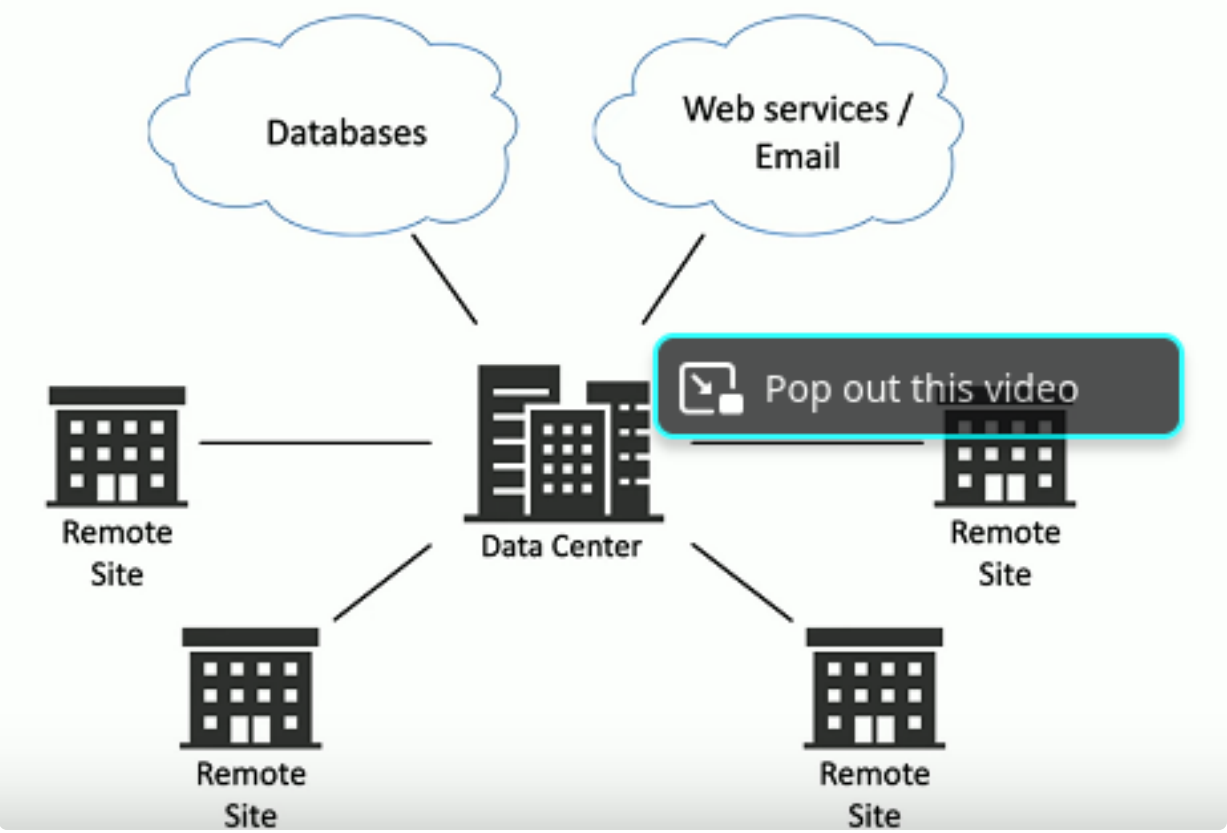
Firewall Example of Physical Architecture



SD-WAN (Software Defined Networking in a Wide Area Network)

- A WAN built for the cloud
- The data center used to be in one place but cloud changed everything
- Cloud-based applications communicate directly to the cloud
  - No need to hop through central point
- Application aware
  - WAN knows which app is in use
  - Routing decisions based on application data
- Zero touch provisioning
  - Remote equipment is automatically configured
  - App traffic uses the most optimal path

- Can change based on traffic patterns and network health



- Transport agnostic
  - Underlying network can be any type
    - Cable modem, DSL, fiber-based, 5G, etc
    - Pick best choice for location
- Central policy management
  - Management and config in a single console
  - One device to configure then changes pushed to SD-WAN routers

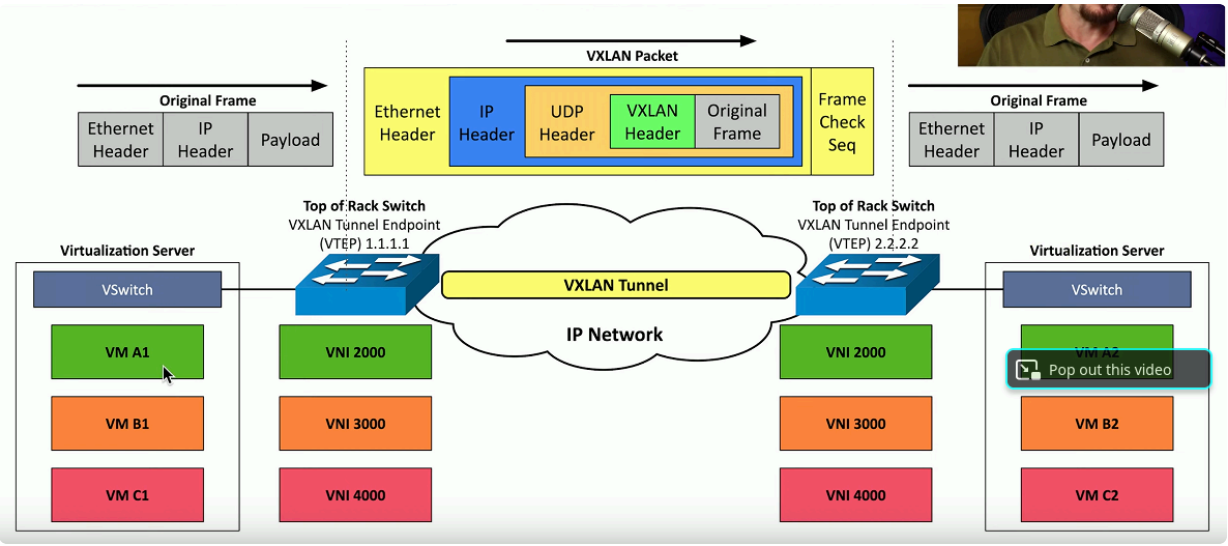
1.8 Virtual Extensible LAN

Data Center Interconnect (DCI)

- Connect multiple data centers together
  - Seamlessly span across these geographic distances
- Connect and segment different customer networks
  - Across multiple data centers
  - All customers share the same core network
- Distribute applications everywhere
  - Increase uptime and availability
  - Workload can be moved to the best location

Scaling Across Data Centers

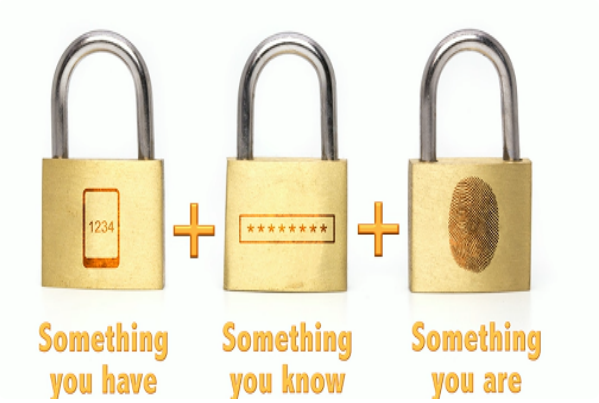
- IP addressing is different across data centers
  - Challenging to manage dynamically created virtual systems
- Centers can be connected in different ways -> MPLS, high speed optical, Metro Ethernet, etc.
- Apps shouldn't have to worry about IP addressing, routing or connectivity -> They should work regardless of physical location
- Extend networks across physical locations
  - Encapsulate, send the data ,decapsulate
  - Tunnel the data.
  Solution = Virtual Extensible Lan (VXLAN)
- Designed for large service providers -> Hundreds or thousands of tenants
- VLAN's
  - Max of about 4000 possible virtual networks
  - Fixed Layer 2 Domain (Layer 2 = Data Links Layer)
  - Not designed for large scale and dynamic movement of VM's
- VXLAN support
  - Over 16 million posible virtual networks
  - Tunnel frames across a layer 3 network (Layer 3 = Network Layer)
  - Built to accommodate large environments
  VXLAN Encapsulation



1.8 Zero Trust

- Many networks are relatively open on the inside
  - Once through firewall there are few security controls
- Zero trust is a holistic approach to network security
  - Covers every device, process and person

- Everything must be verified -> No inherent trust
  - MFA, encryption, system permissions, additional firewalls, monitoring and analytics etc...



Policy Based Authentication

- Adaptive identity
  - Consider the source and the requested resources
  - Multiple risk indicators -> relationship to org, physical location, type of connection , IP address, etc.
  - Make the authentication stronger, if needed
- Policy driven access control
  - Combine adaptive identity with predefined set of rules
  - Eval each access decision based on policy and other info
  - Grant, deny or revoke access

Authorization

- After authentication is complete -> We can trust your identity
- Authorization process is also required -> Determine which applications and data are accessible
- Different rights depending on the user
  - Can include other criteria -> Location, device certificate validation, time of day, etc

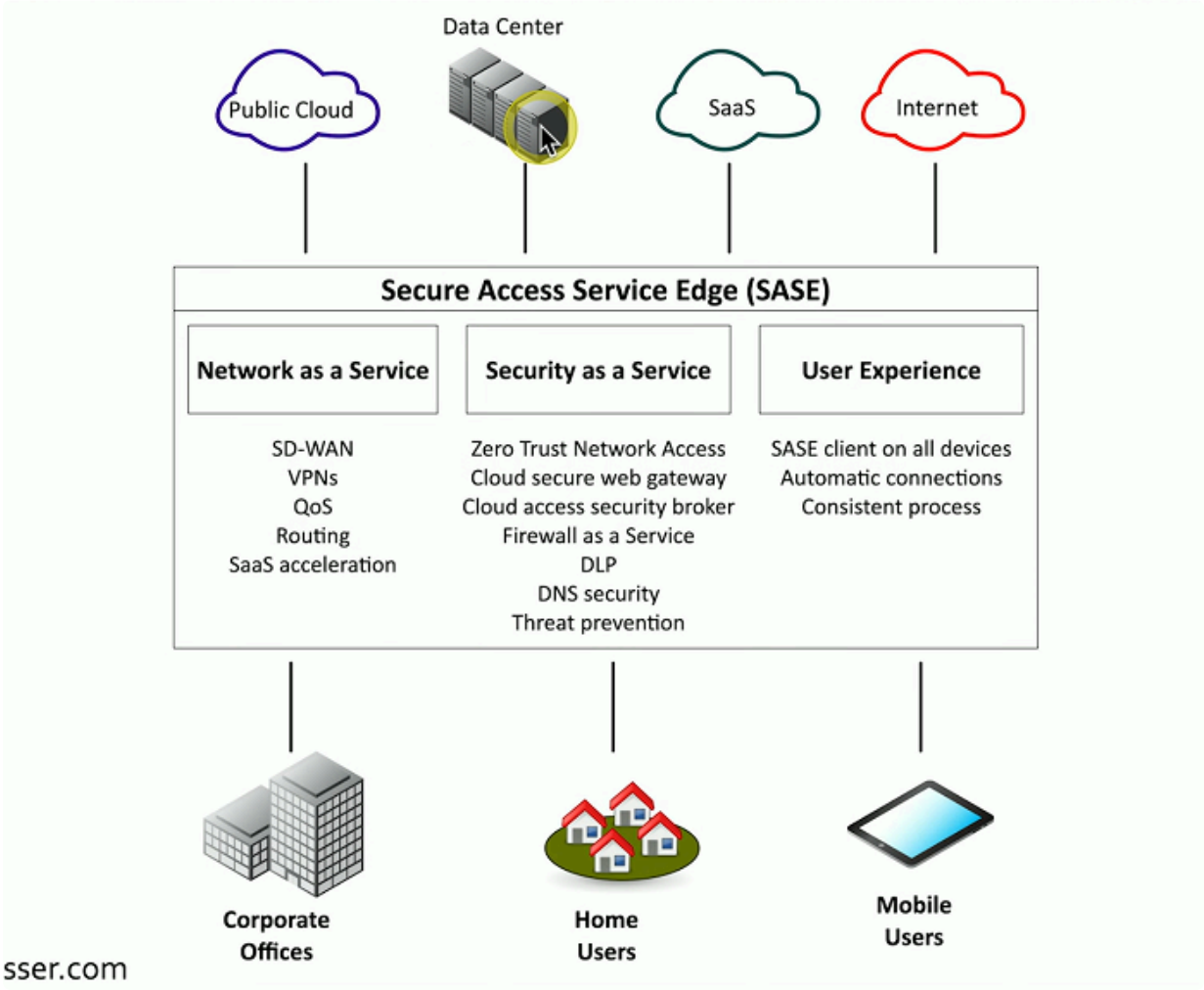
Least Privilege Access

- Good IT Practice -> Rights and permissions should be set to the bare minimum
- You only get exactly what's needed to complete your objective
- All user accounts must be limited -> Apps should run with min privileges
- Don't allow users to run with admin privileges -> Limits scope of malicious acts

Secure Access Service Edge (SASE)

- Update secure access for cloud services
  - Securely connect from different locations
- A "next generation" VPN
- Security tech are in the cloud -> Located close to existing cloud services

- SASE clients on all devices -> Streamlined and automatic



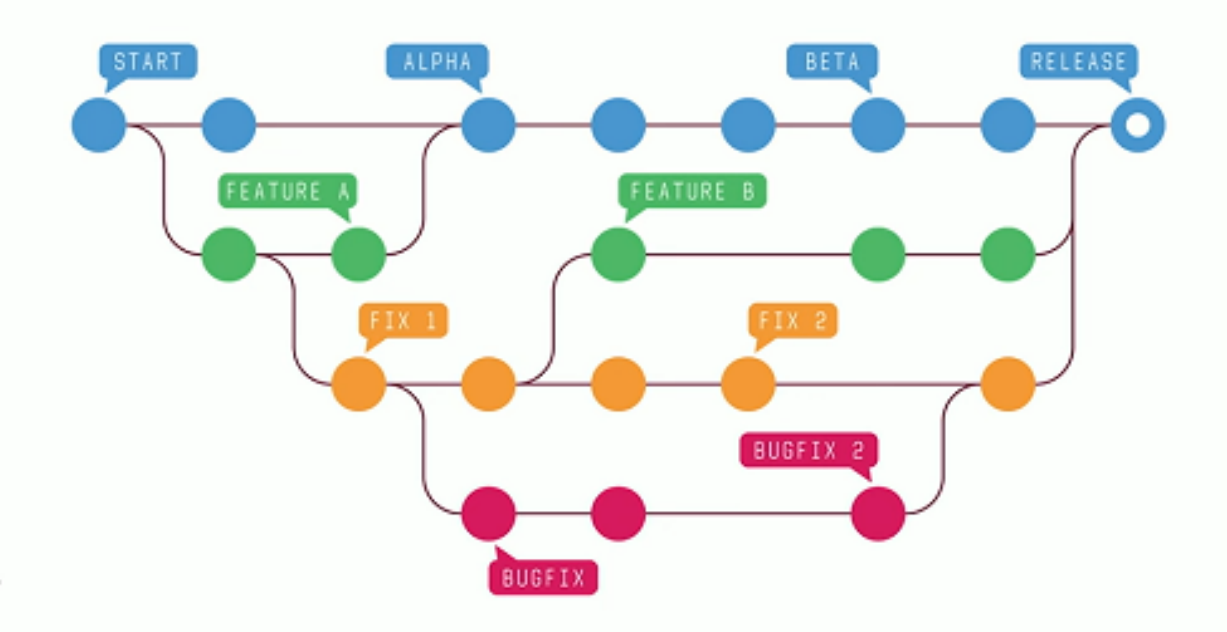
1.8 Infrastructure as Code

- Describe an infrastructure
  - Define servers, network and applications as definition files
- Modify the infrastructure and create versions
  - Same way you version application code
- Use the description (code) build other application instances
  - Build it same way every time
  - Important concept for cloud computing -> Build perfect version every time

  Playbooks
- Conditional steps to follow -> A broad process
  - Investigate a data breach, recover from ransomware
- Reusable template -> Can be used to automate activities
- Integrated with a SOAR platform -> Security Orchestration, Automation and Response
  - Integrate third-party tools and data sources

  Automation Use Cases

- Configuration drift/compliance
  - Ensure same configs for all systems
  - The config used in testing should be the same in production
  - IaC provides identical deployment
- Upgrades -> Change config with a single line of code
  - Modify config and software
- Dynamic inventories -> Query devices in real-time -> Manage based on results
  Source control
- Managing change
  - Developers create the infrastructure requirements
  - Build and public the definition files
- Manage ongoing changes to the code -> Version control system (Ex: Git)
- Track changes across multiple updates
- Central repo. -> All changes are tracked and merged together
  - Everyone can participate without causing issue with the code



Controlling Source Code

- Conflict identification
  - Some code can't be merged
  - Multiple versions could be modifying same line of code
- Which one wins? Determined automatically or may require manual intervention
- Branching
  - Move away from the main line of development
  - Work without making changes to main code base
  - Branch and merge, branch and merge

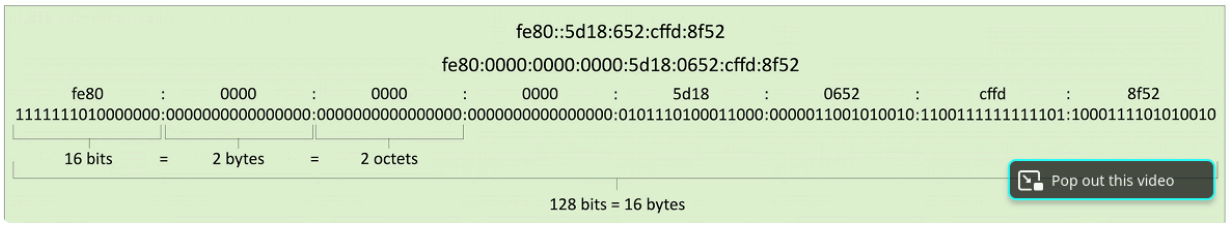
1.8 IPv6 Addressing

IPv4 Address Exhaustion

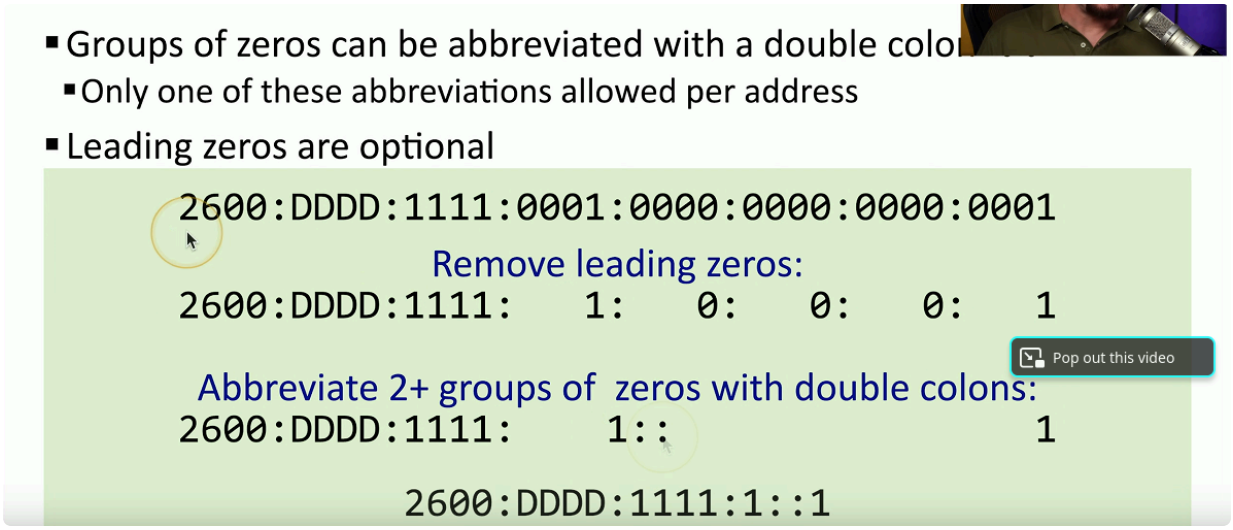
- There are an estimated 20B devices connected to internet and growing
  - IPv4 Supports around 4.29B addresses
- The address space for IPv4 is exhausted -> None available to assign
- IPv4 and NAT is a workaround -> Can be challenging with certain protocols
- IPv6 provides a larger address spaces

  IPv6 Addresses
- Internet Protocol v6 - 128-bit address (16 bytes)
  - 16 bits = 2 bytes = 2 octets for each section of address
- 340 Undecillion addresses

  - Each grain of sand on earth could have 45 quintilion unique IPv6 Addresses



IPv6 Address Compression



In this case group 0: 0: 0: becomes ::

Ex: Given IP 2601:04C3:4002:BE00:0000:0000:0000:0066

First step-> Remove Leading 0's

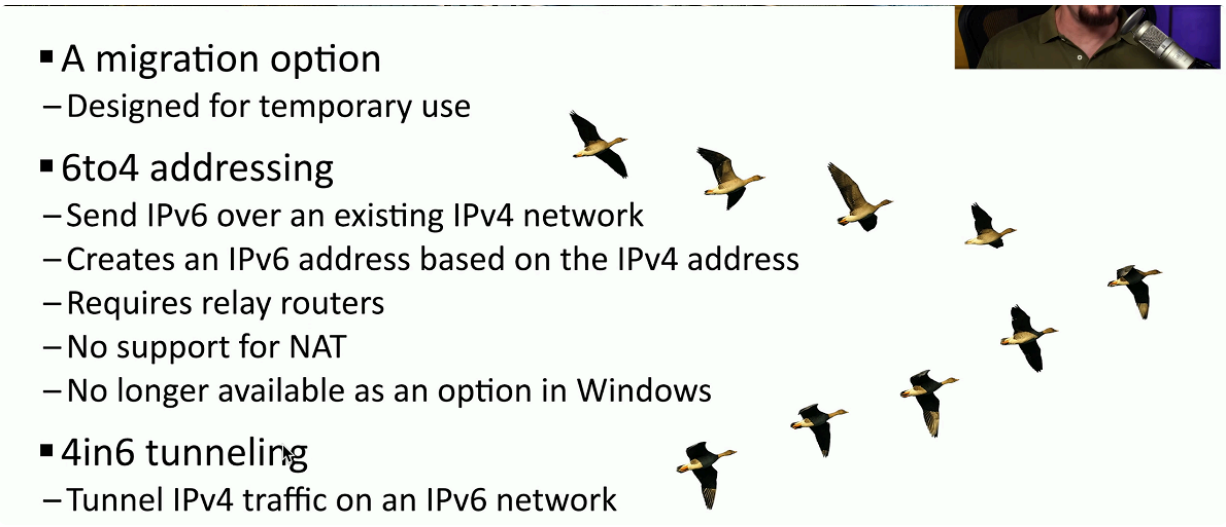
- 2601:4C3:4002:BE00:0:0:0:66

  Second step-> Abbreviate group of zeroes
- 2601:4C3:4002:BE00::66

  Communicating between IPv4 and IPv6
- Not all devices can talk IPv6
  - Legacy devices, embedded systems, etc.

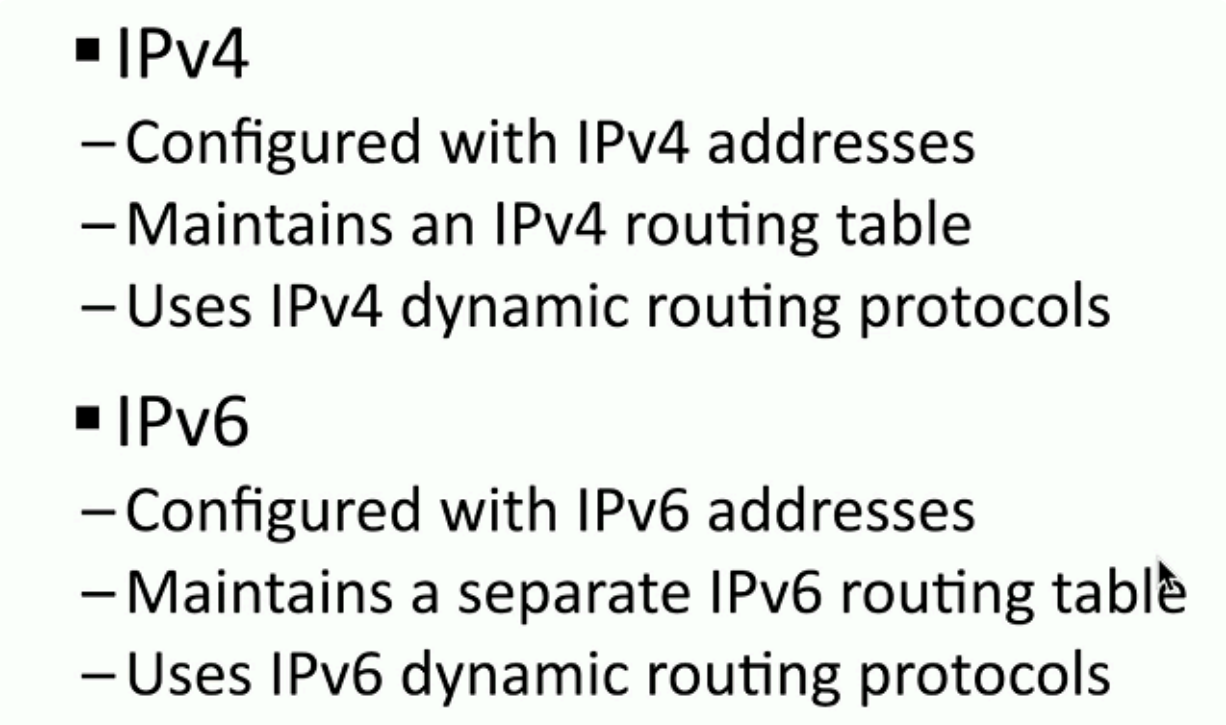
    - How can IPv4 device talk to an IPv6 Server?
    - Can IPv6 device communicate with legacy IPv4 Server?
- Requires alternate form of communication
    - Tunnel: Encapsulate one protocol within another
    - Dual-stack: Have the option to use both v4 and v6
    - Translate: Convert between IPv4 and IPv6
- Short term strategies -> Long term = complete migration to IPv6

Tunneling IPv6



Dual-Stack Routing

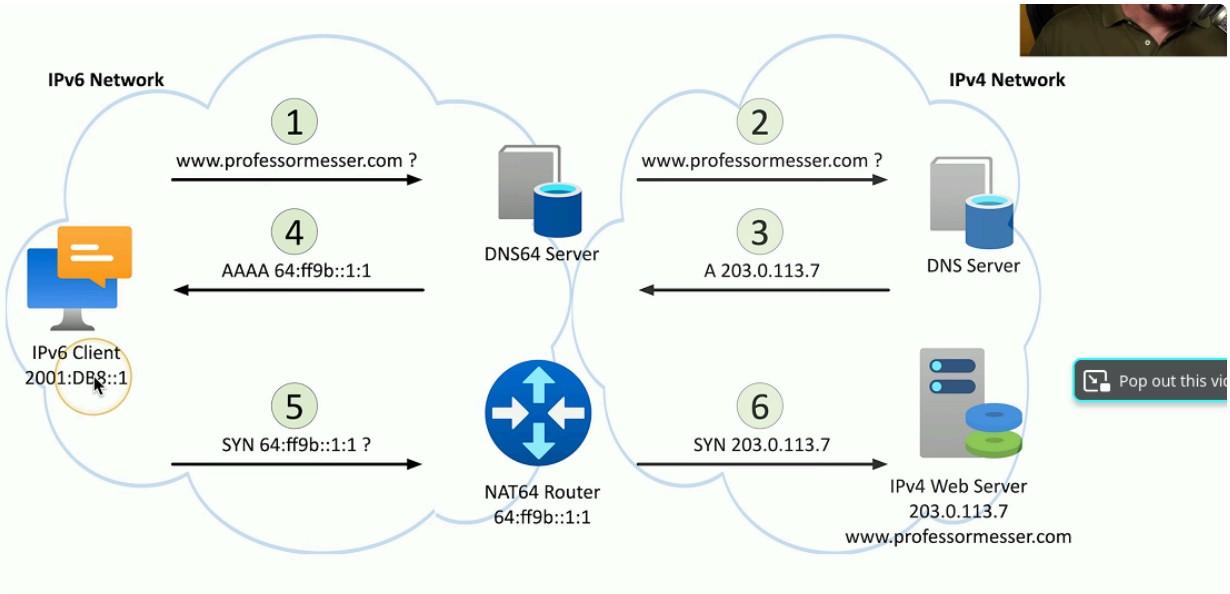
- Dual-stack v4 and v6 -> Run both at same time -> Interfaces assigned multiple address types



Translating between IPv4 and IPv6

- Network address translation using NAT64

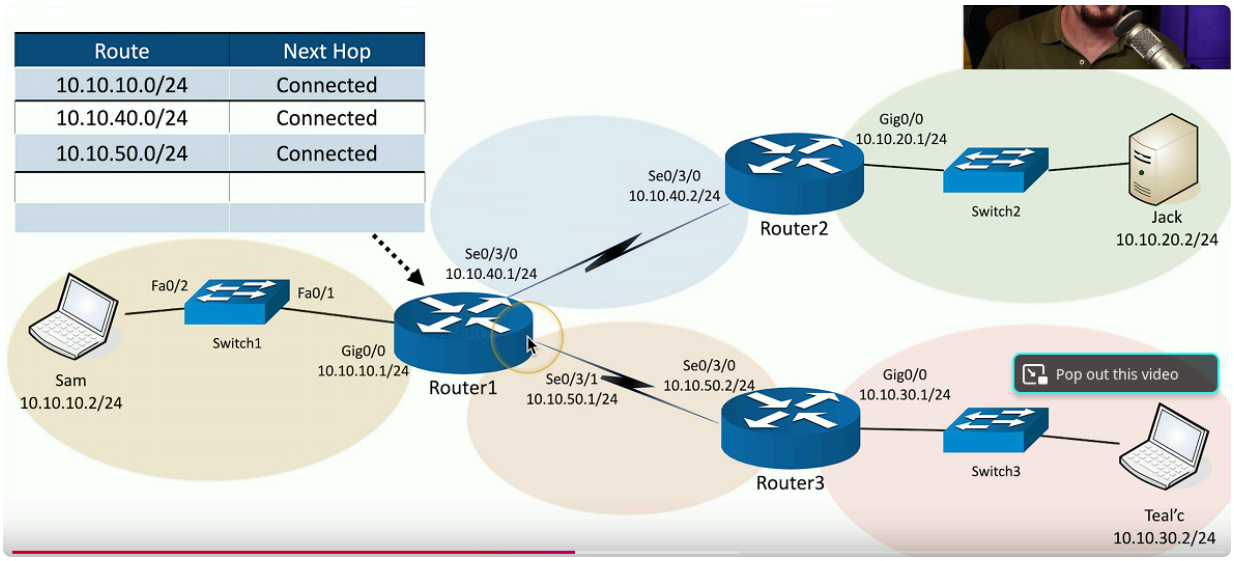
    - Translate between v4 and v6 -> Seamless to the end User
- Requires something in the middle to translate
    - IPv6 not backwards compatible w/ IPv4
    - Use a NAT64 capable router
- Works with DNS64 server
  - Translate the DNS requests



2.1 Static Routing

Routing Tables

- Router has relatively simple job -> Underlying tech is relatively complex
- Identify the destination IP address -> It's in the packet
- If destination IP is on a locally connected subnet-> Forward packet to local device
- If destination IP address on remote subnet-> Forward to next-hop router/gateway
  - This "map" of forwarding locations is the routing table



Static Routing

- Administratively define the routes ->You're in control
- Advantages:
  - Easy to config and manage in smaller networks
  - No overhead from routing protocols (CPU,memory,bandwidth)
  - Easy to configure on stub networks (only one way out)

References

https://www.youtube.com/watch?v=k7IOn3TiUc8&list=PLG49S3nxzAnl_tQe3kvnmeMid0mjF8Le8