Network+ N10-009 Notes

Ioritz Eguileor

2024-11-26

Status: #complete

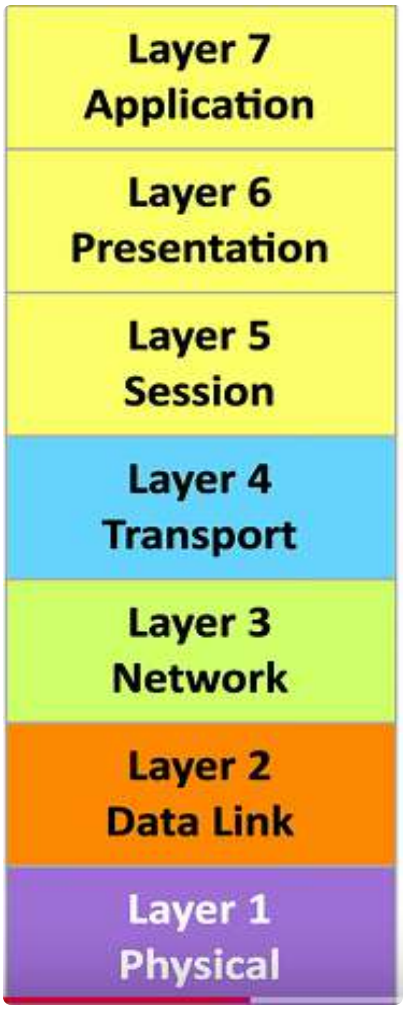
Tags: networking network+

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

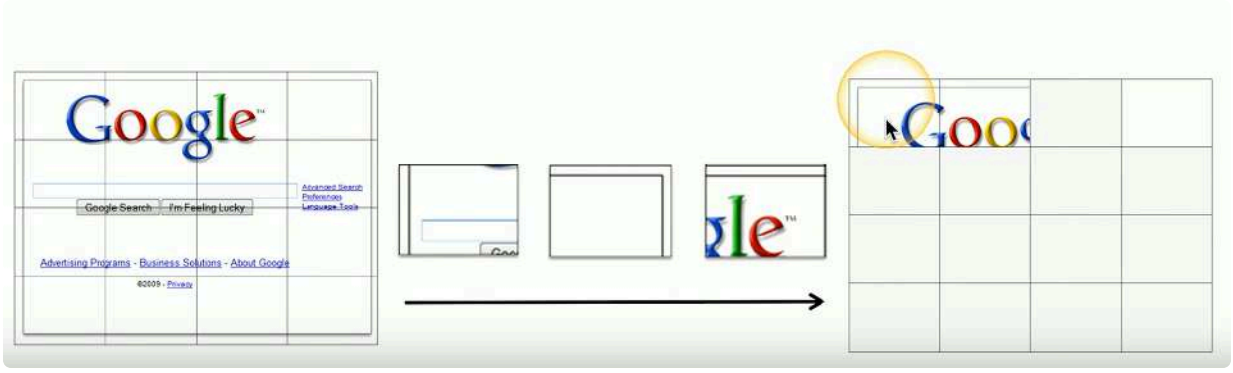
- The physics of the network
  - Signaling, cabling, connectors
  - This layer is not about protocols (Very Hardware Heavy)
- "You have a physical layer problem"
  - Fix your cabling, punch-downs etc
  - Run loopback tests, test/replace cables, swap adapter cards

  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)

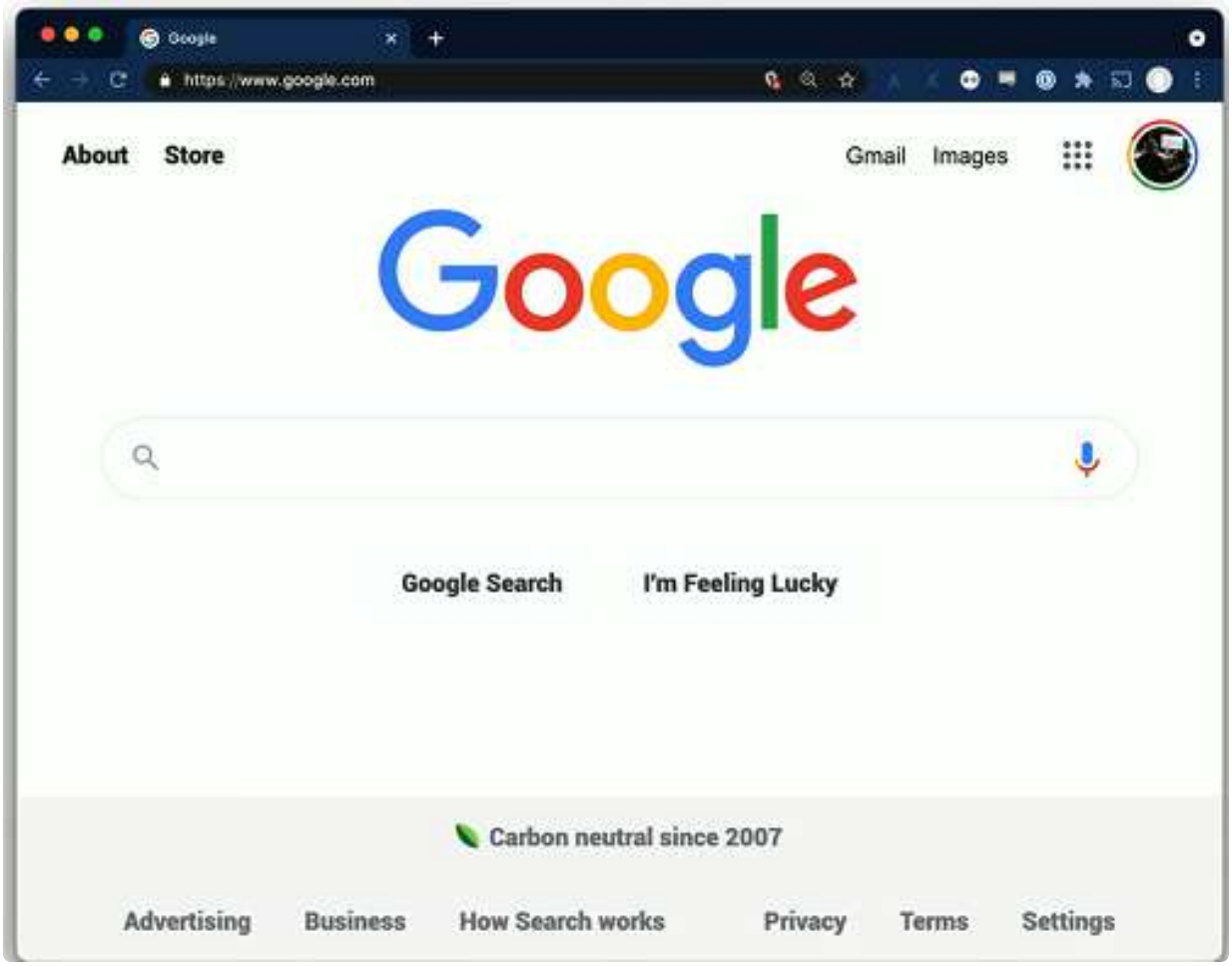


  Layer 5 - Session Layer
- Communication management between devises
  - Start, stop, restart
- Control protocols, tunneling protocols

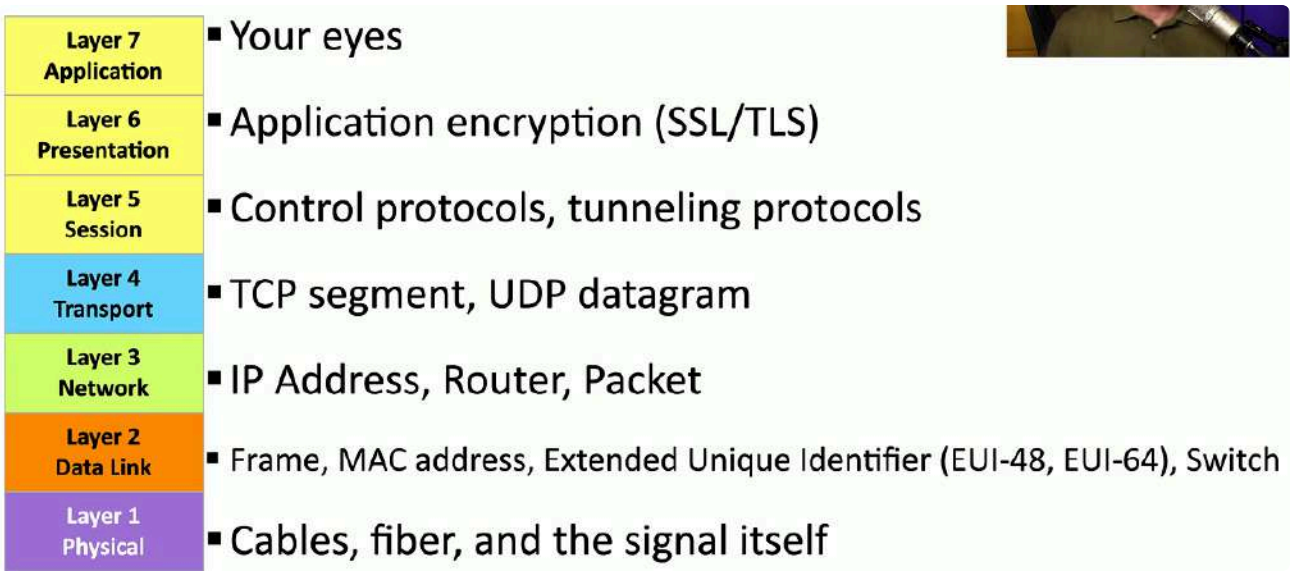
  Layer 6 - Presentation Layer
- Character encoding
- Application encryption
- Often combined with Application Layer

  Layer 7 - Application Layer

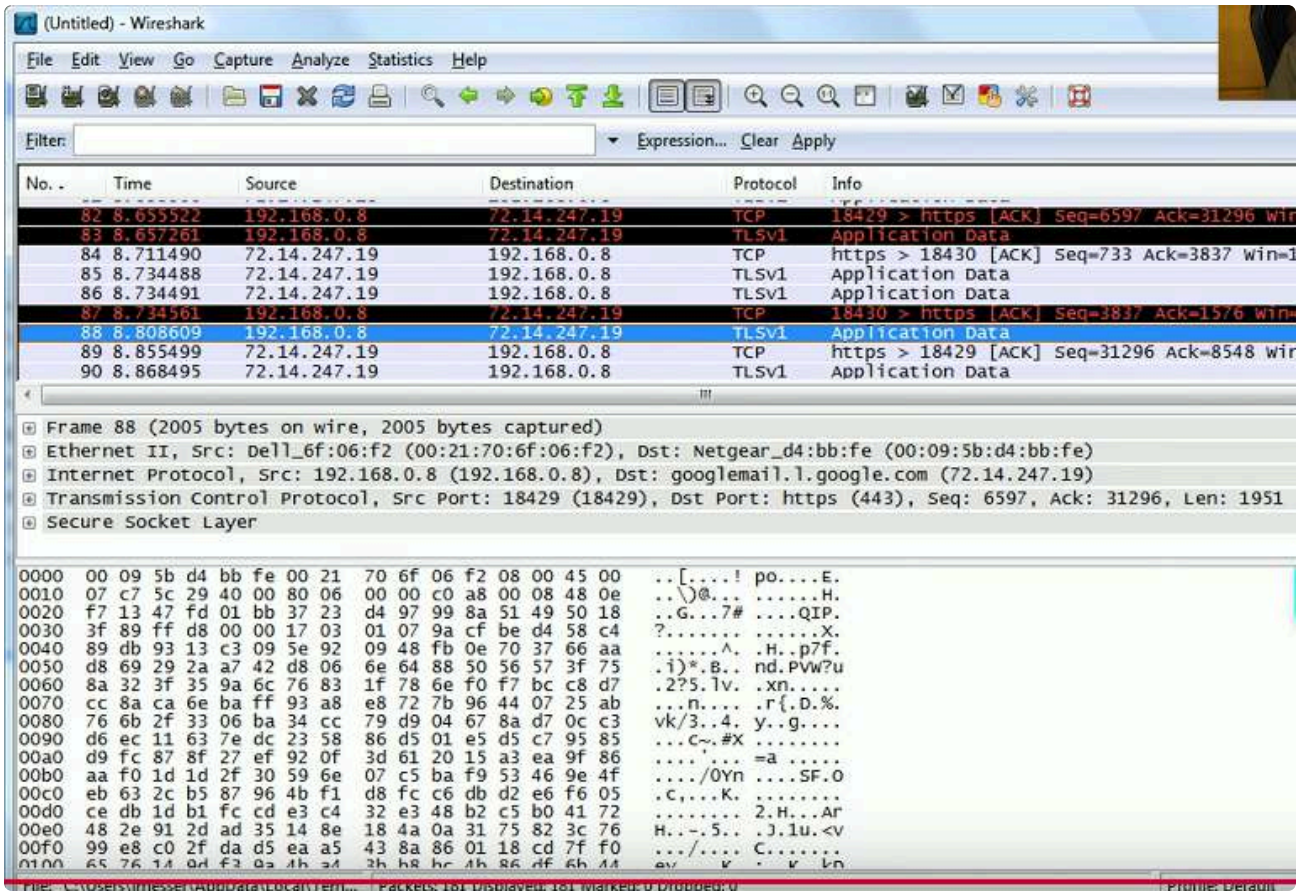
- The layer we see

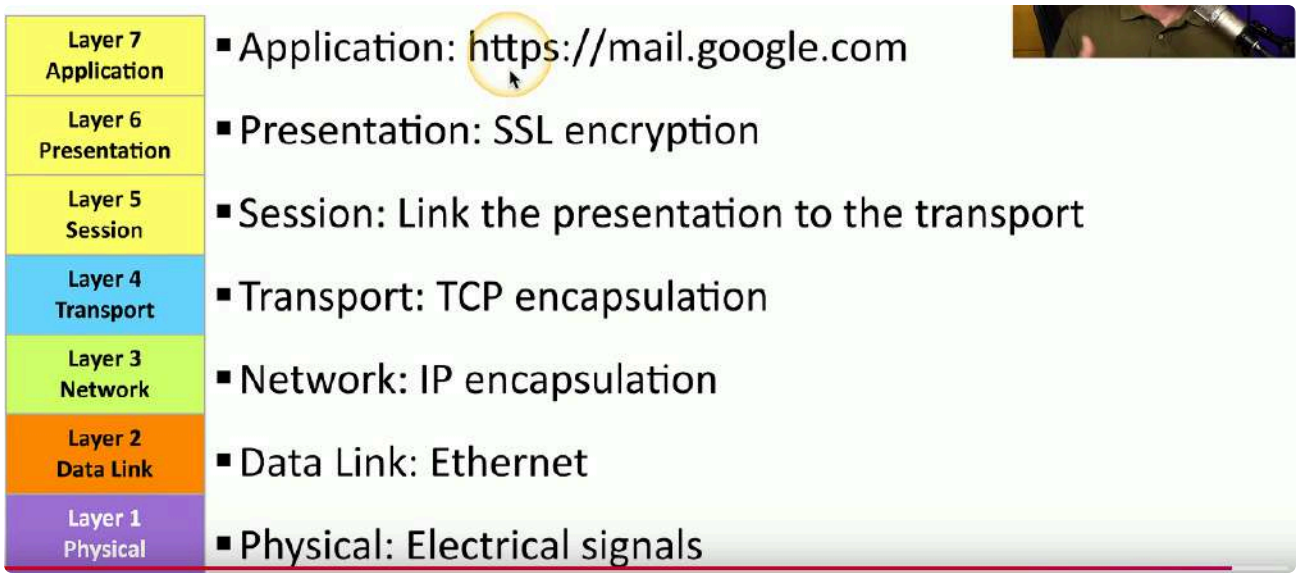


Real World To OSI Model Application:



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

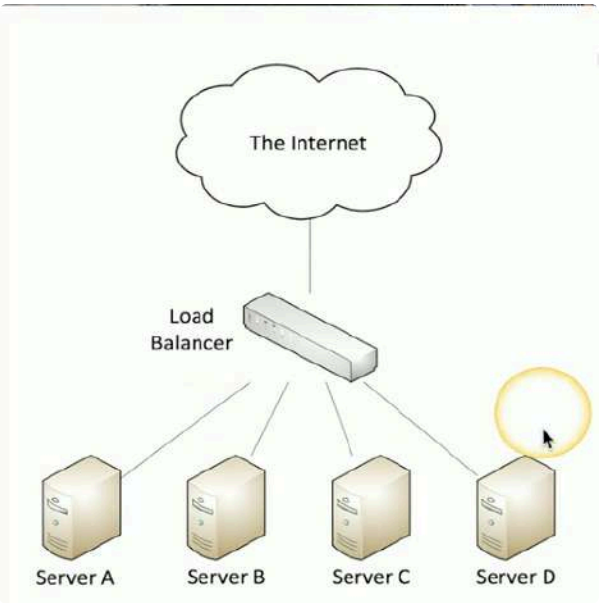
  Switch:
- Bridging done in hardware
  - Application-specific integrated circuit (ASIC)
- OSI layer 2 Device (L2 = Data Link Layer)
  - Forwards traffic based on data link address (MAC Address for example)
- Many ports and features
  - Core of enterprise network
  - May provide Power over Ethernet (PoE)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

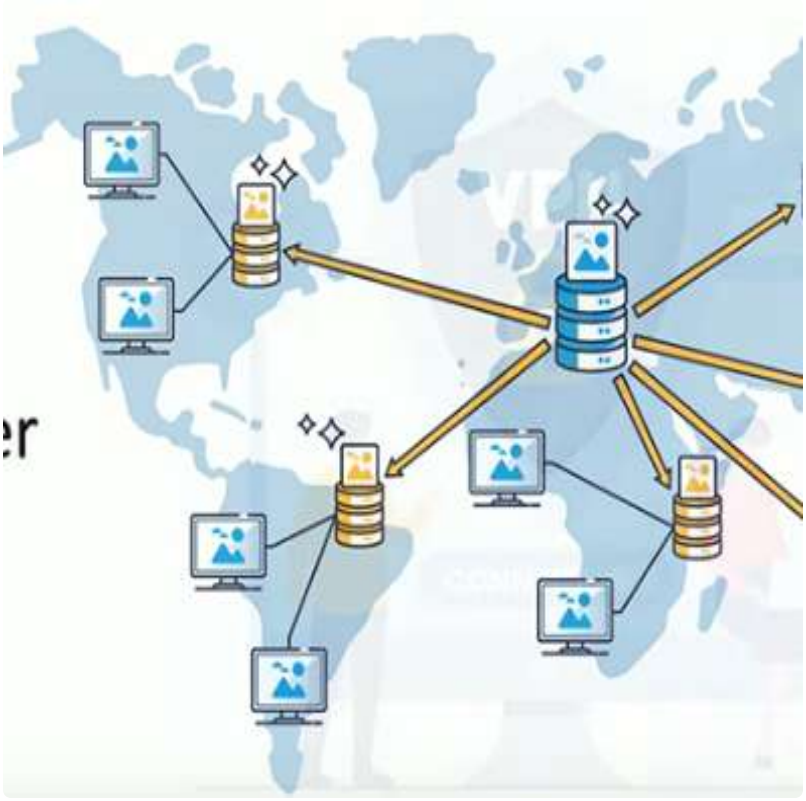
- Storage Area Network (SAN)
  - Looks and feels like a local storage device
  - Block level access (more efficient than file-level)
    - Only write and read changes of block rather than entire file
- Both require large bandwidth so they often use isolated network and high speed network technologies
  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

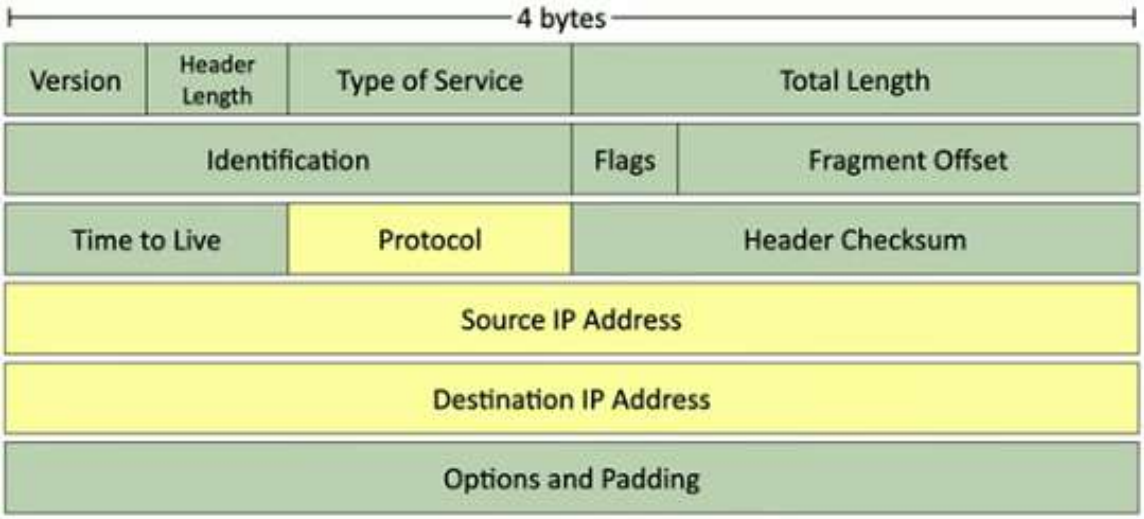
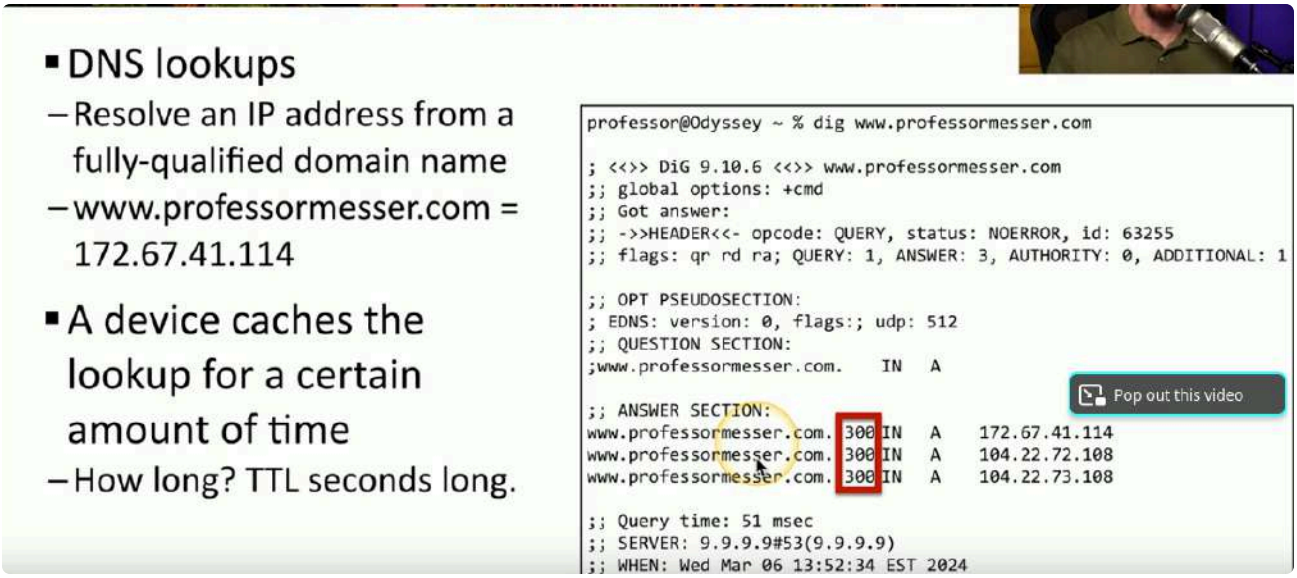


Image shows where TTL is stored

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

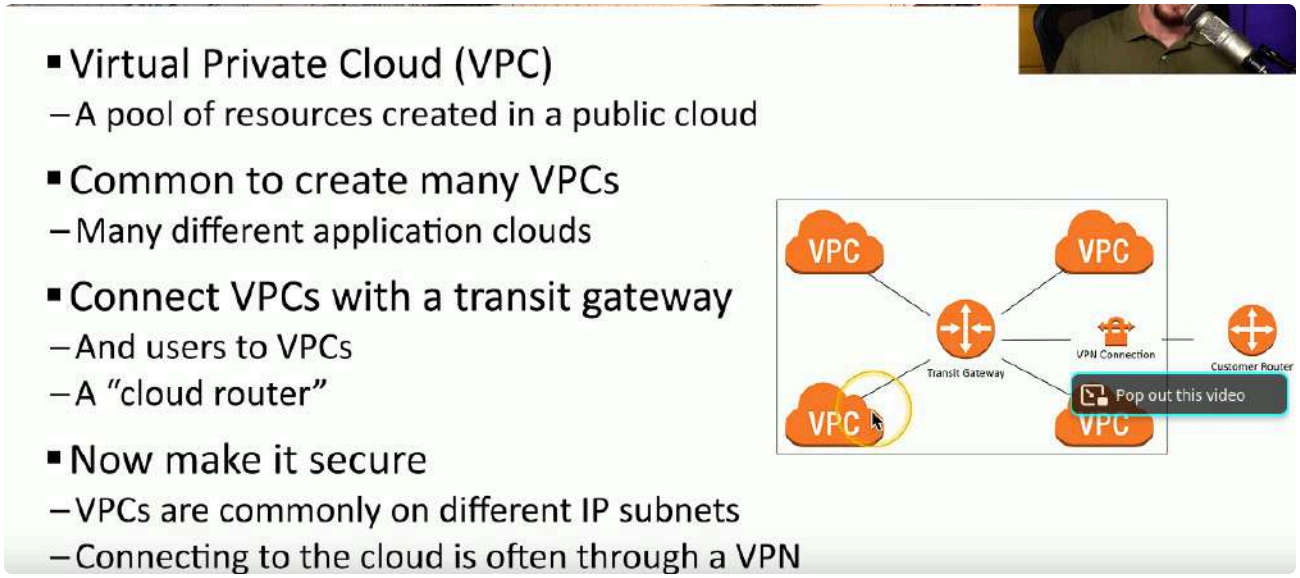
Virtual Network

- 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?

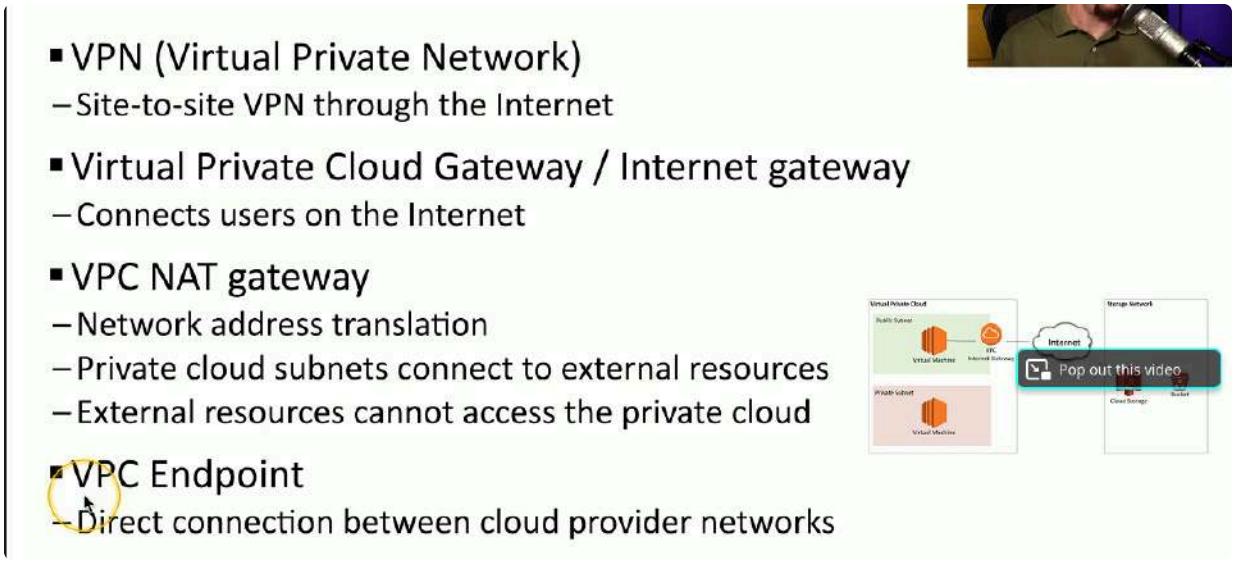
Network Function Virtualization (NFV)

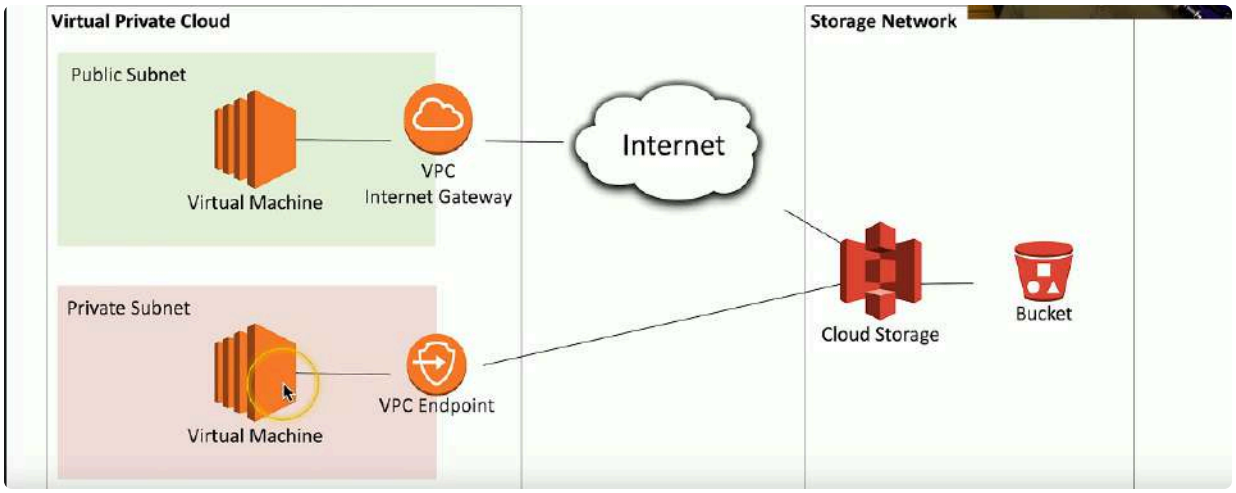
- Replace physical network devices with virtual version
  - Manged from the hypervisor
- Same functionality as previous physical device
  - Routing,switching, load balancing, firewalls etc...

Connecting to the Cloud:



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





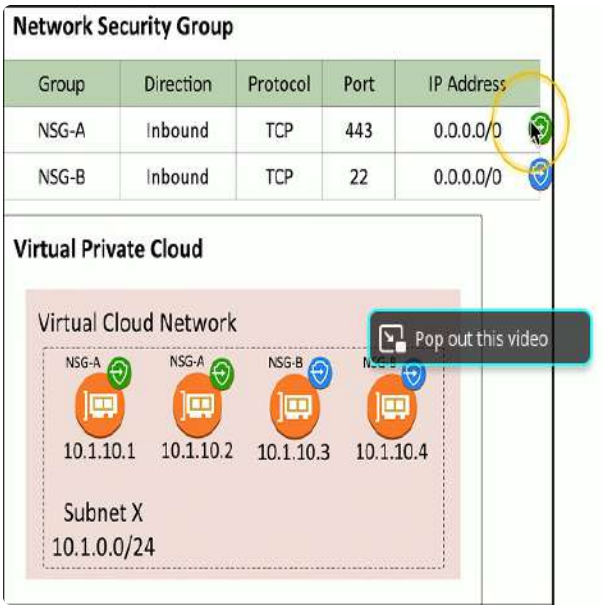
Security Groups and Lists (Like Firewall for the Cloud)

- 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



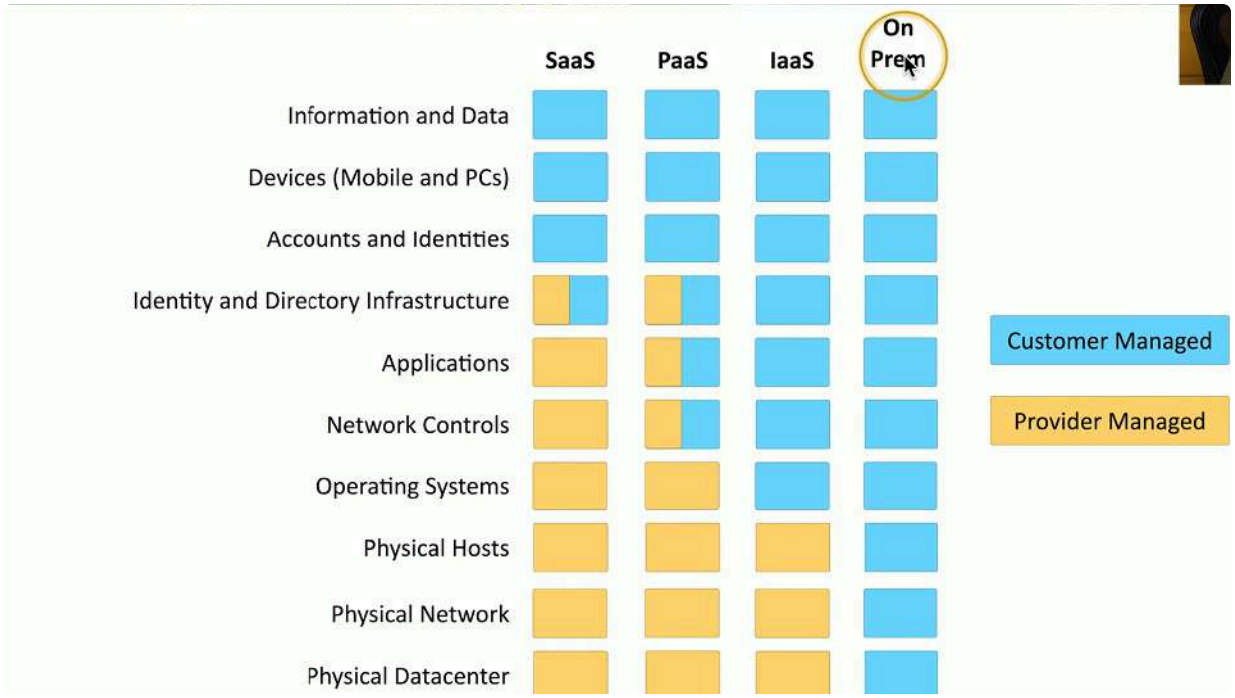
Note how although all devices are in the same Subnet X (10.1.0.0/24) they are separated by group NSG-A and NSG-B

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)

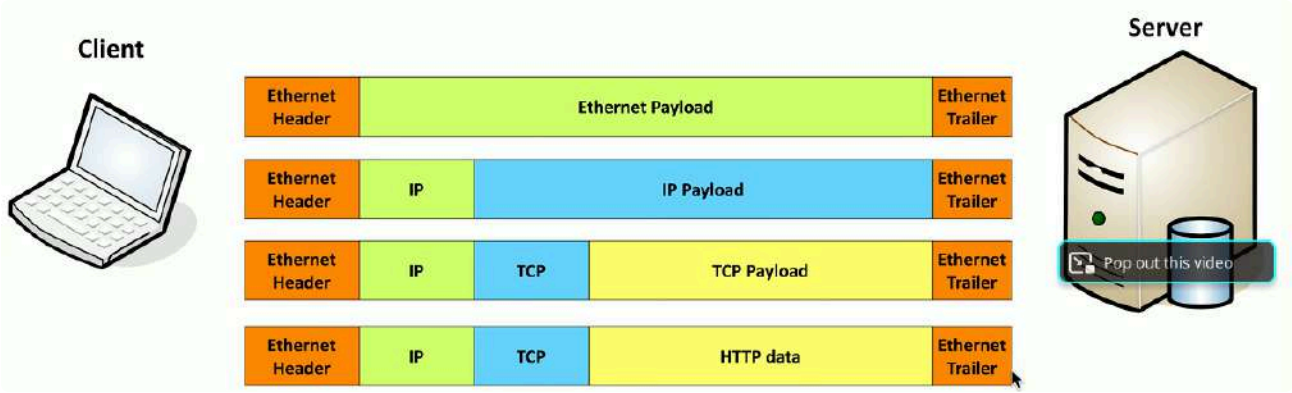
- On demand software
- No local installation
- Central management of data and applications
- No dev work required
  - Google Mail, Office 365
  IaaS (Infrastructure as a Service)
- Outsource your equipment
- Still responsible for management and security
- Data still out there but more control
- Web server 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

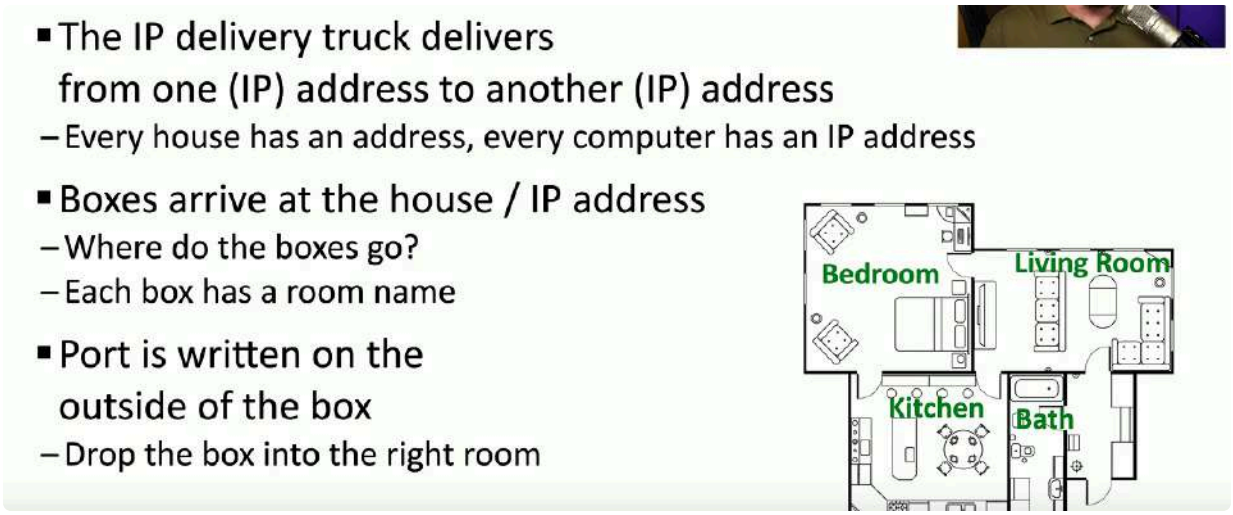
TCP - Transmission Control Protocol

- 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

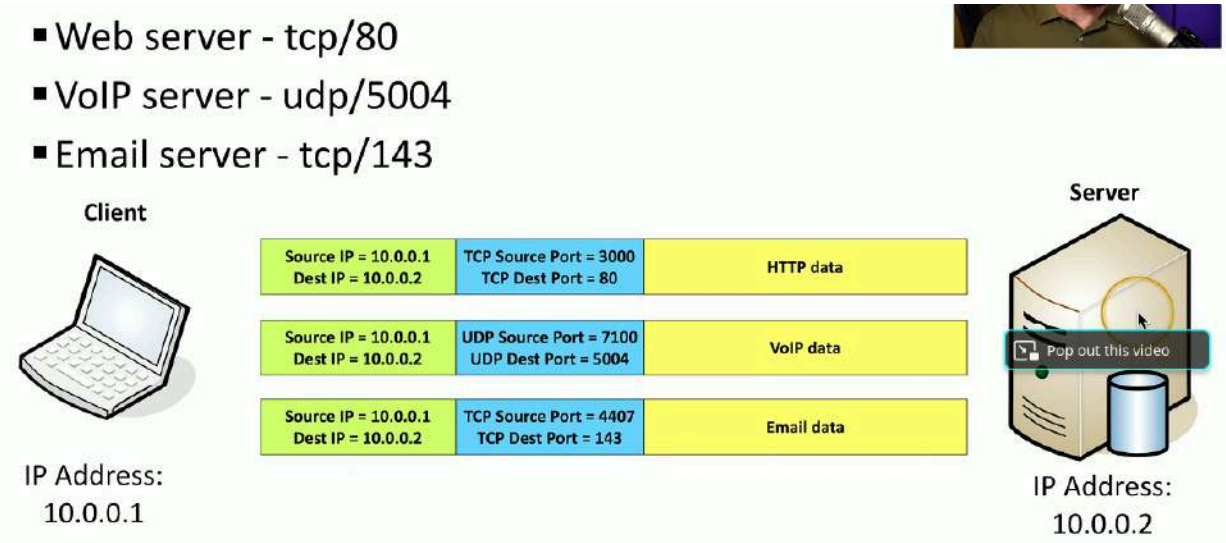


  Port written outside box will tell us which room to send to: Ex of ports = 80, 25, 123, 443

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

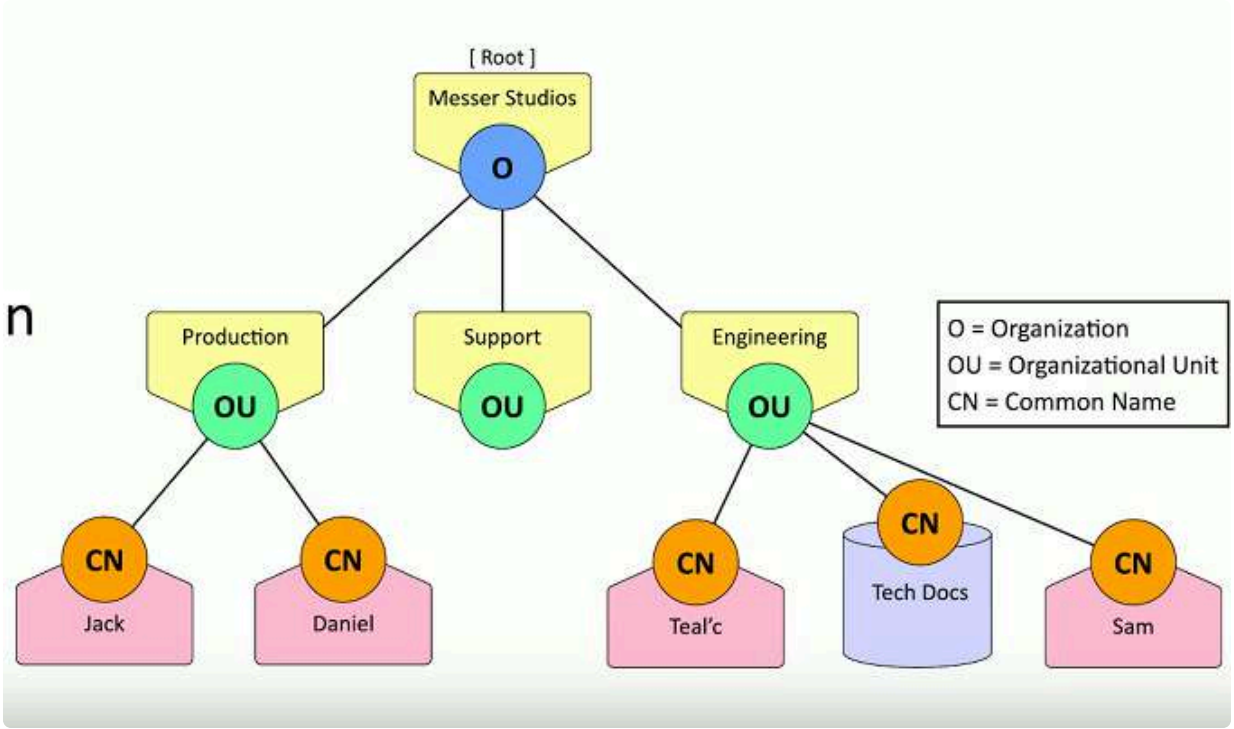
- udp/161
- Gather statistics from network devices
- v1- The original
  - Structured tables
- v2 - A good step ahead
  - Data type enhancements, bulk transfer
- All data however sent in the clear no encryption
- v3 - A secure standard
  - Message integrity, authentication and encryption
- SNMP traps

  - 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

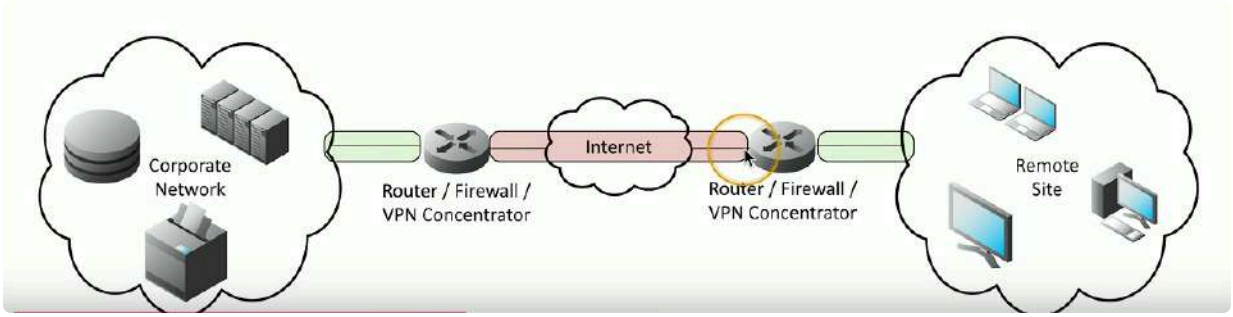
- Your TTL (Time to live) expired just letting you know

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



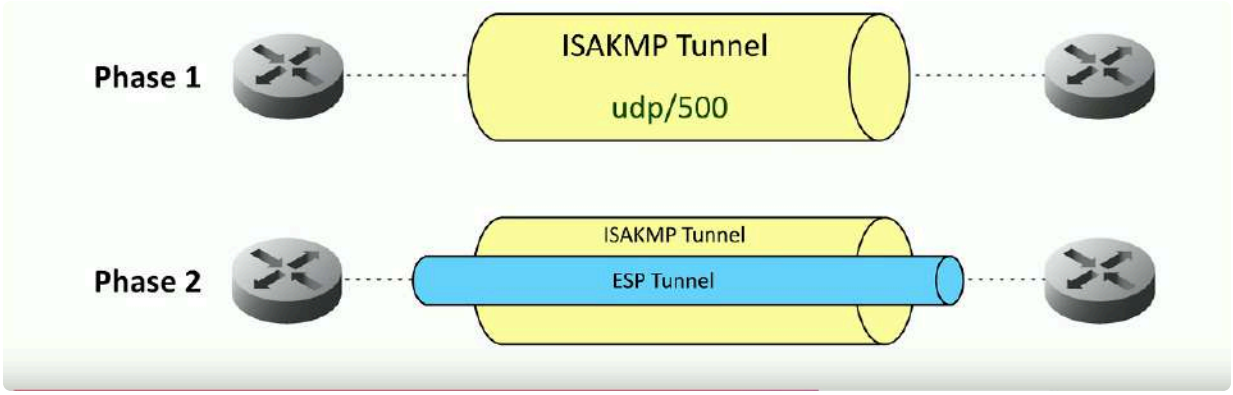
IPSec (Internet Protocol Security)

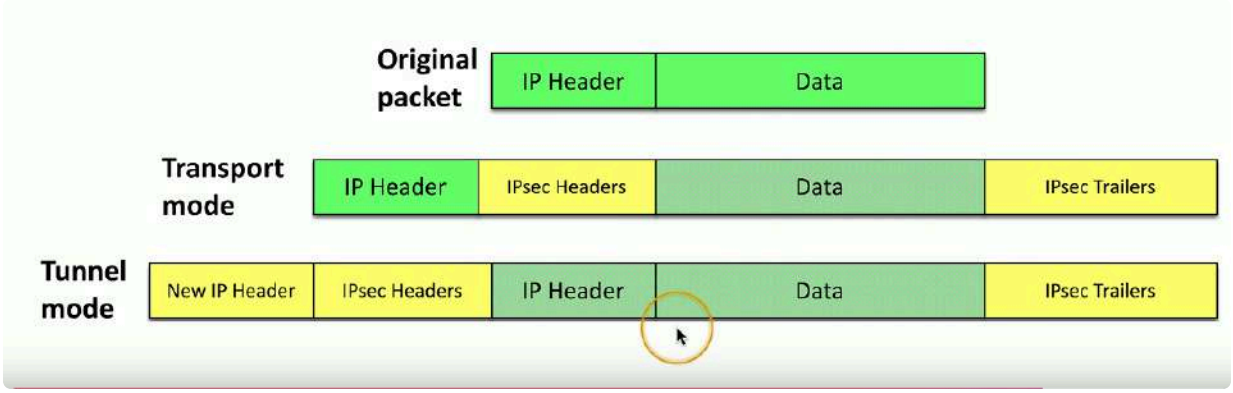
- Security for OSI layer 3
  - Authentication and encryption for every packet
  - Confidentiality and integrity/anti-replay through encryption and packet signing
  - Very standardized -> Common to use multi-vendor implementations
- Two core IPSec Protocols

  - 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

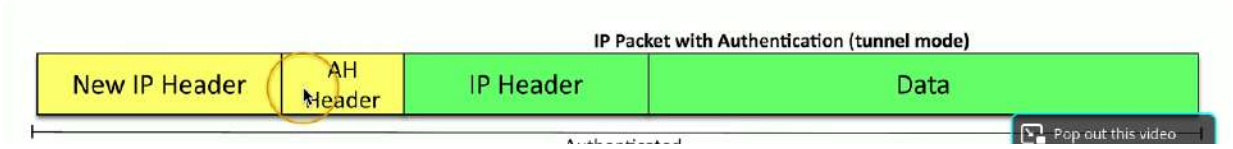




Tunnel mode is most preferred as IP Header and Data are Encrypted where as in Transport Mode the IP Header is not and therefore information about where the data is intended to go can be extracted

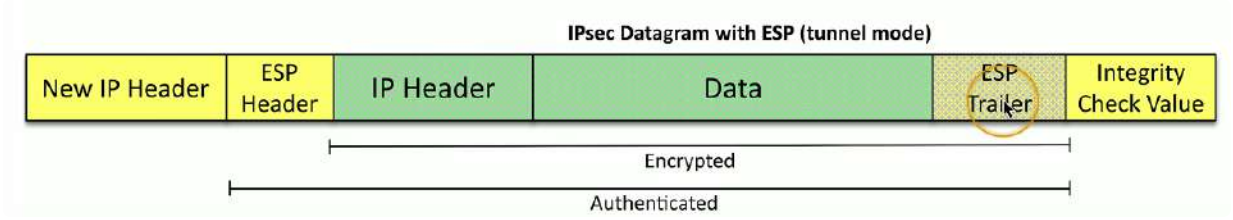
Authentication Header (AH)

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



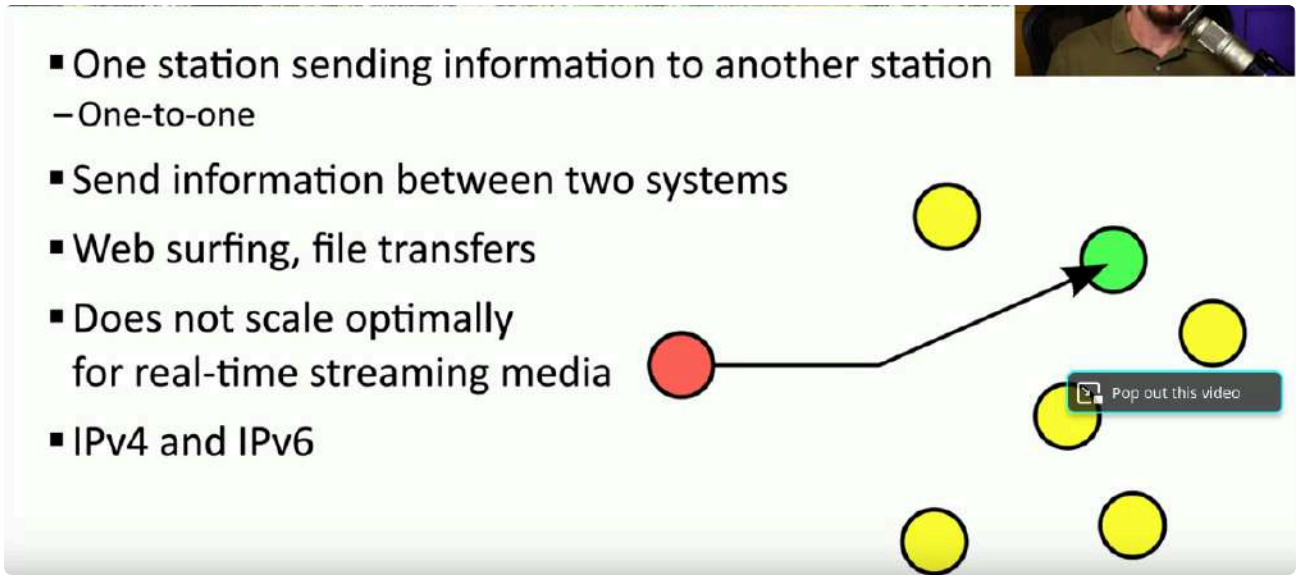
Encapsulation Security Payload (ESP)

- 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

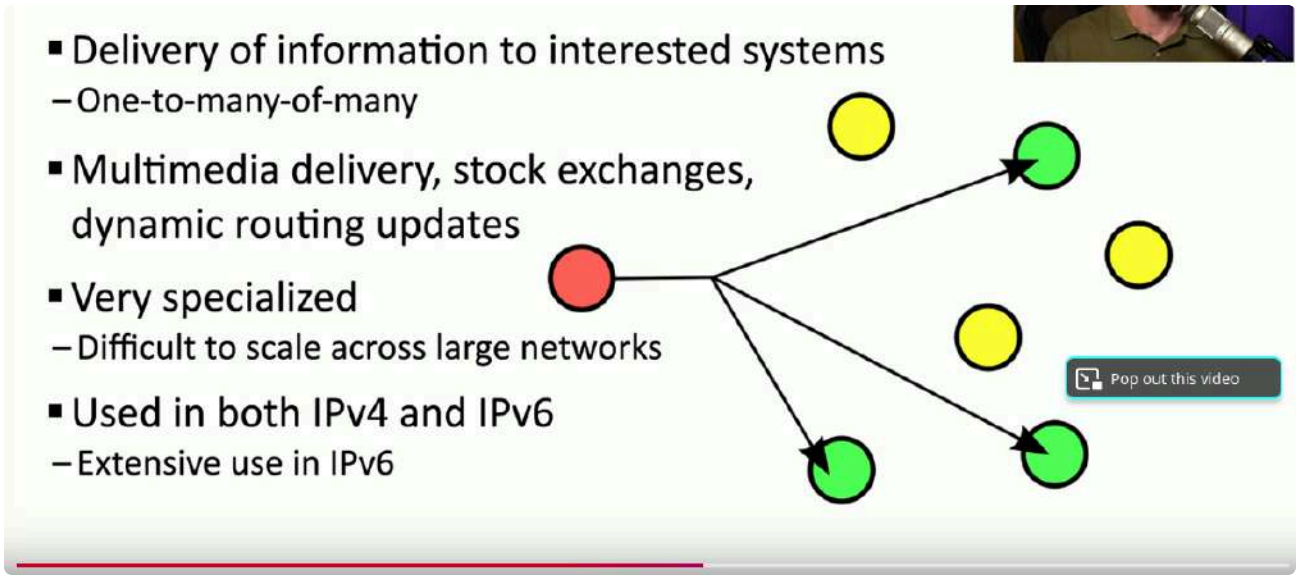


1.4 Network Communication

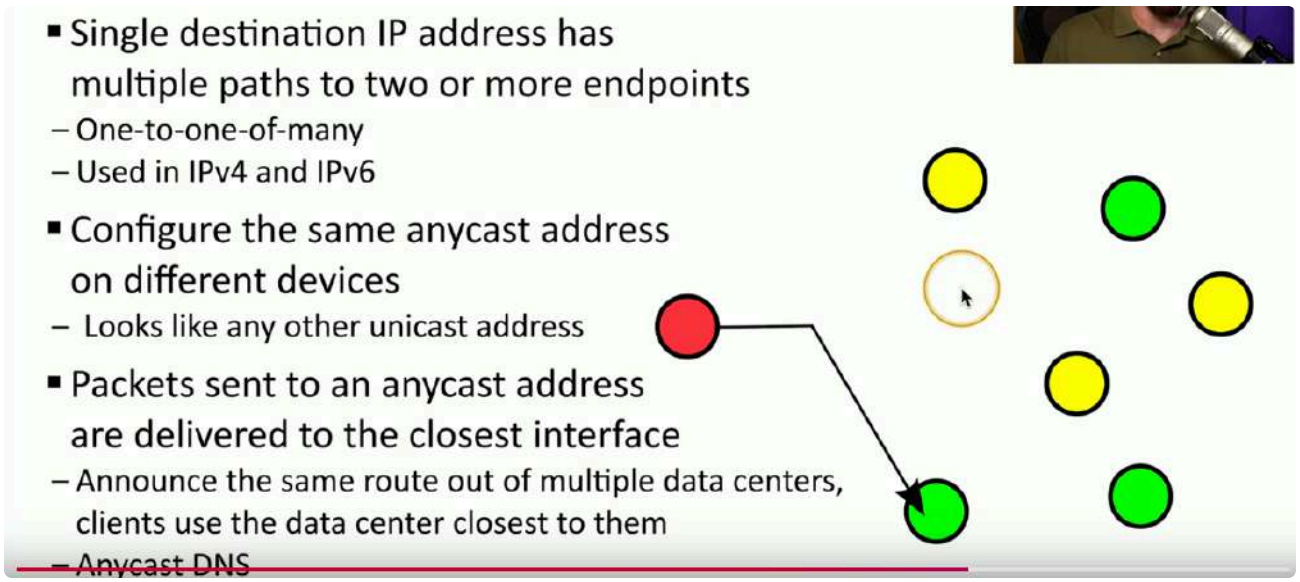
Unicast:



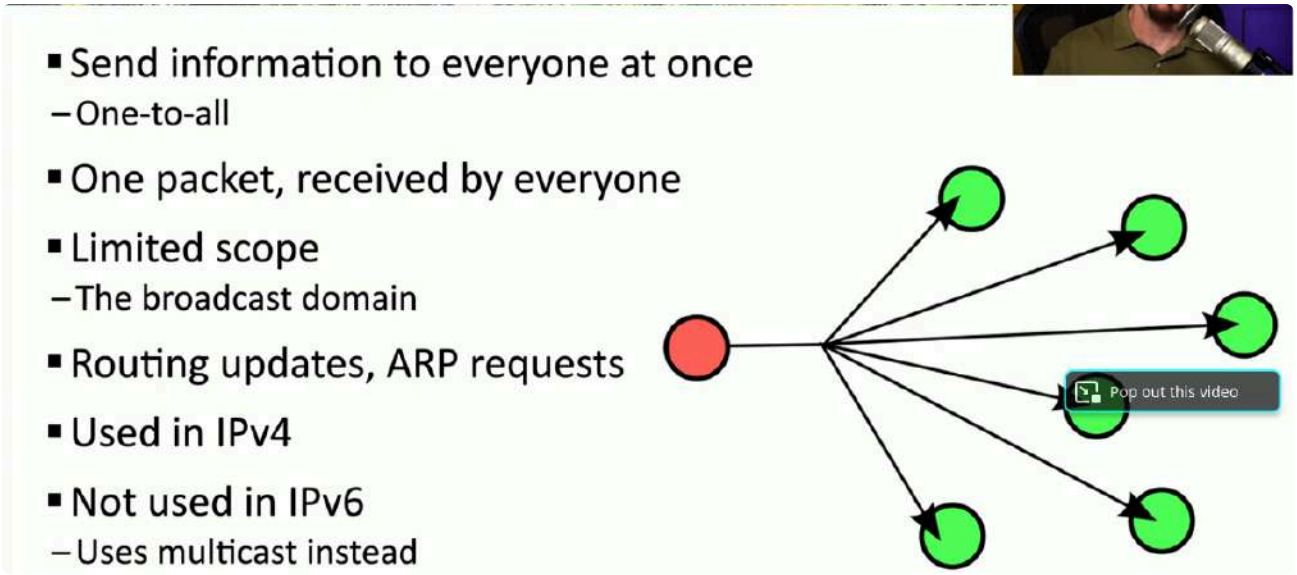
Multicast:



Anycast:



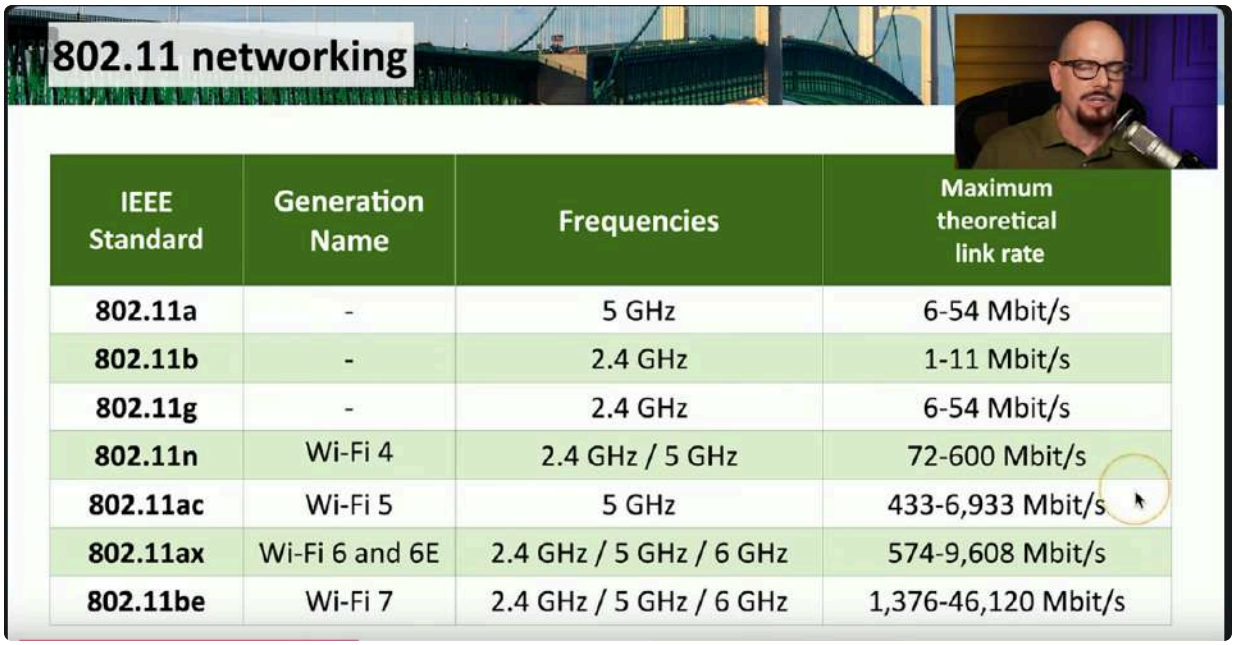
Broadcast:



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

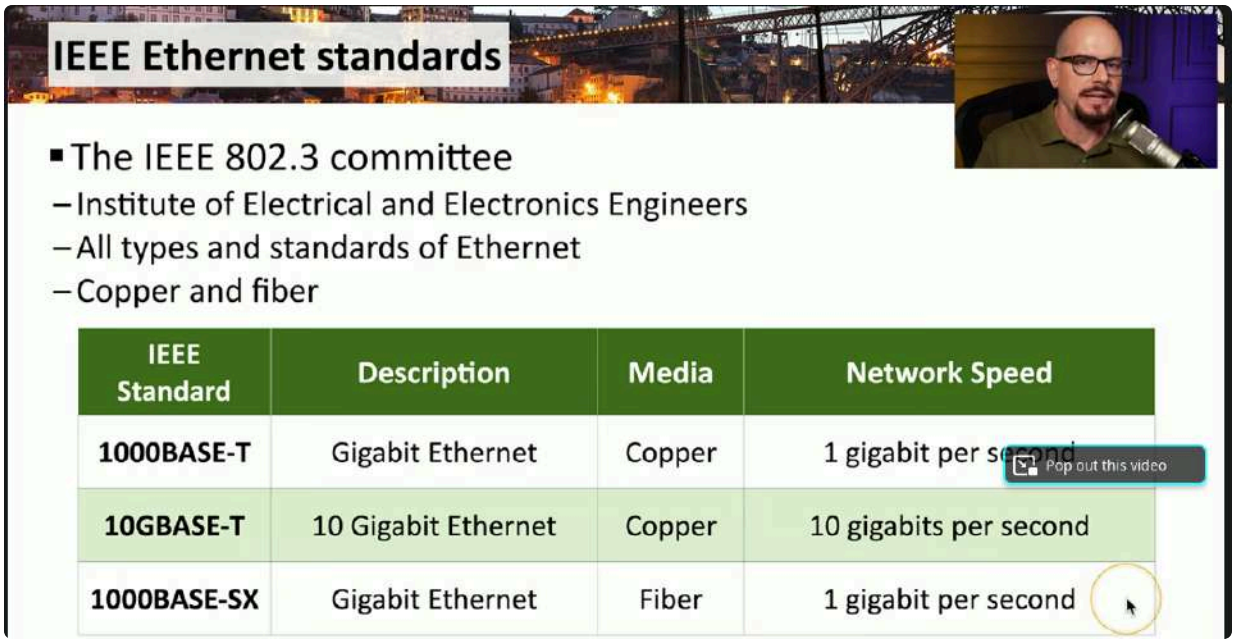
- LTE-A (LTE Advanced)
  - Standard supports download rates of 300 Mbit/s

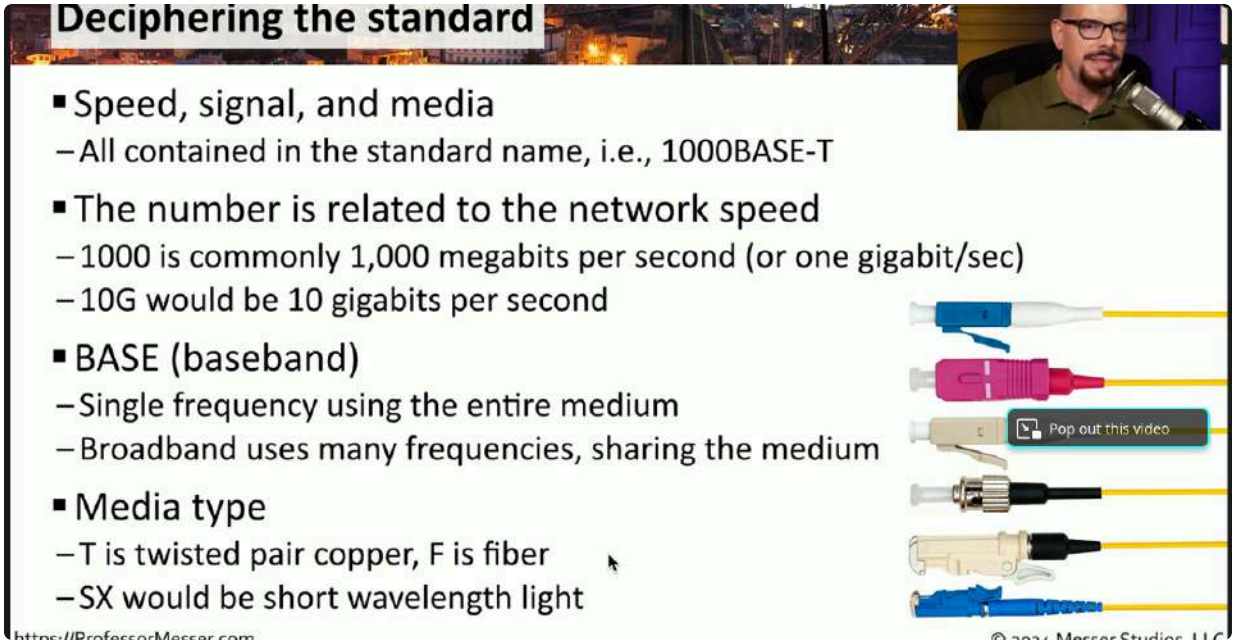
  5G
- Fifth generation cellular networking ->Launched Worldwide in 2020
- Performance improvements -> At higher frequencies, eventually 10 gigabits/s
  - Slower speeds from 100-900 Mbit/s
- Significant IoT (Internet of Things) impact
  - Bandwidth less of constraint, larger data transfers, additional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



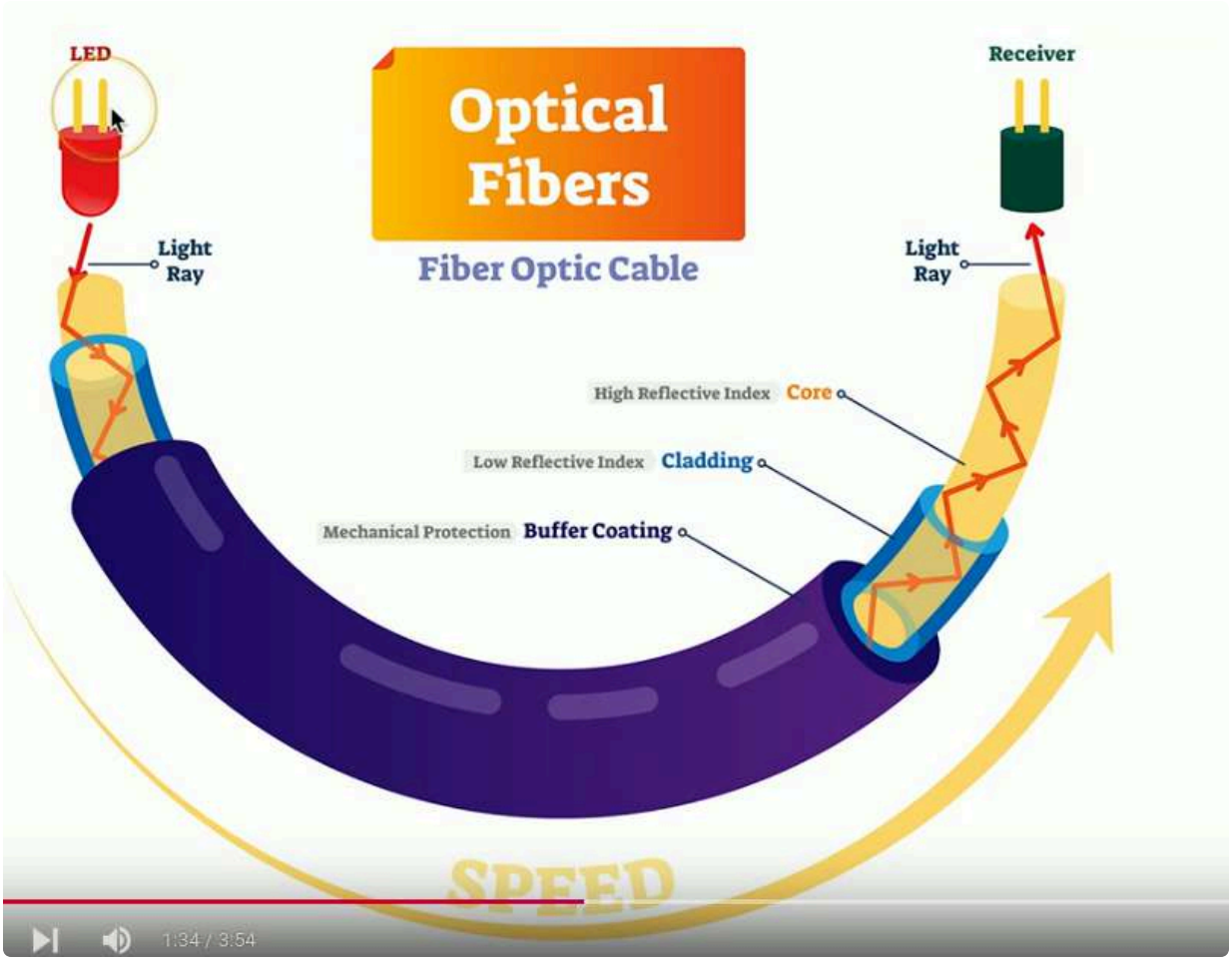


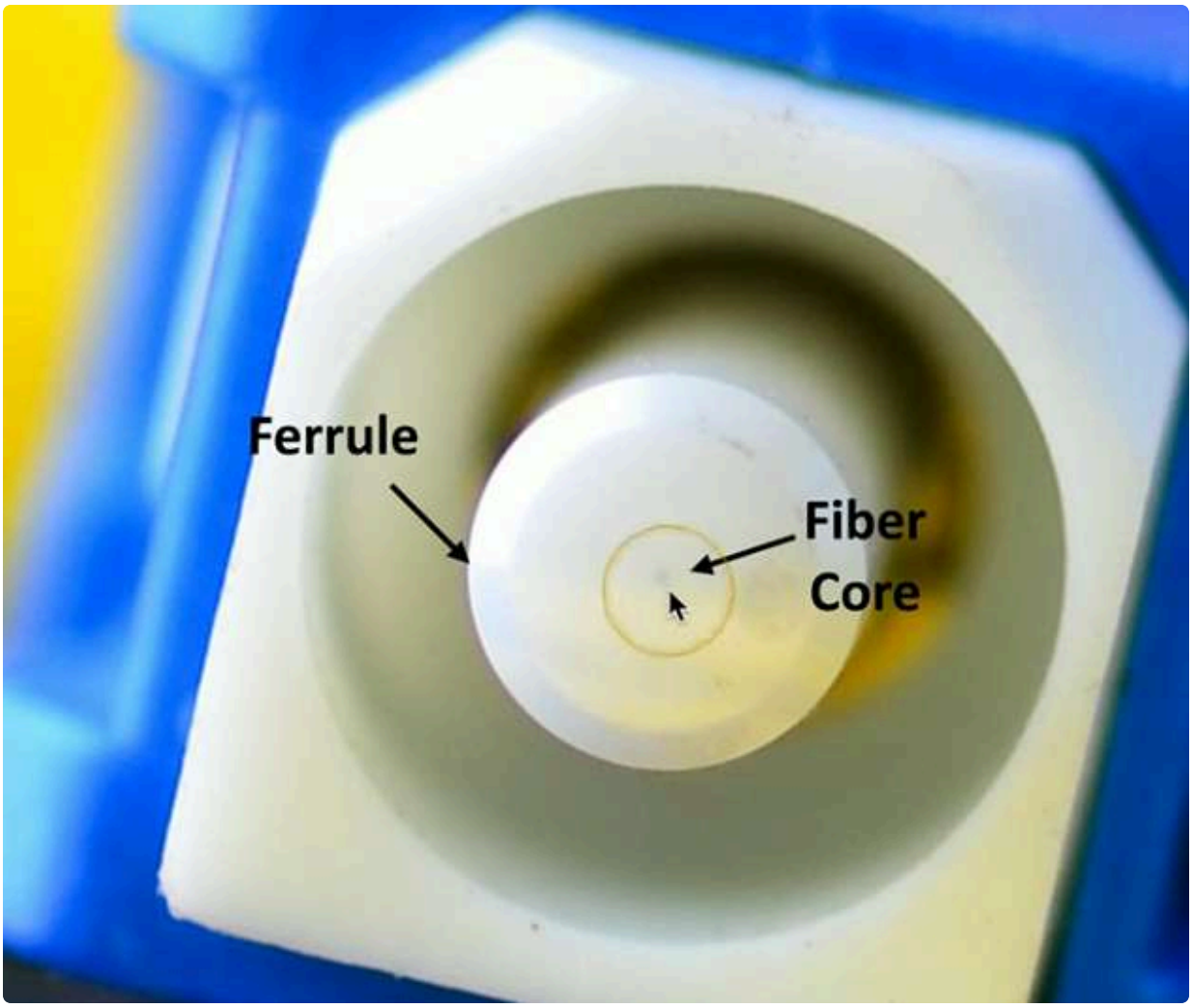
1.5 Optical Fiber

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

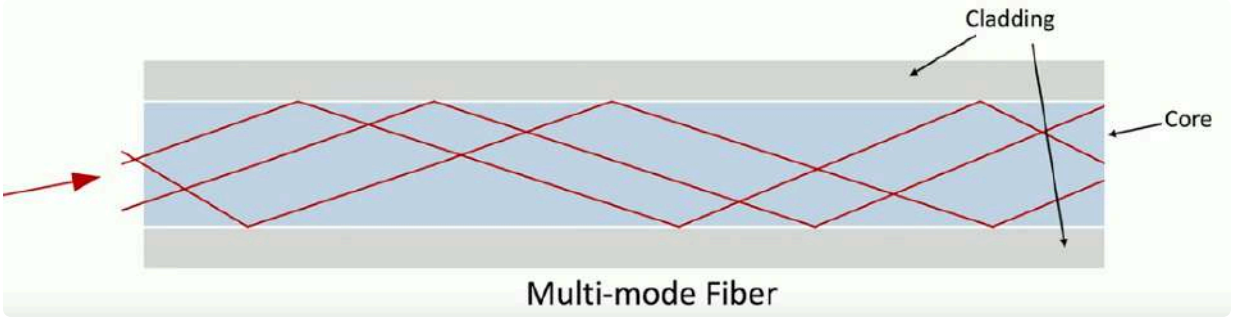


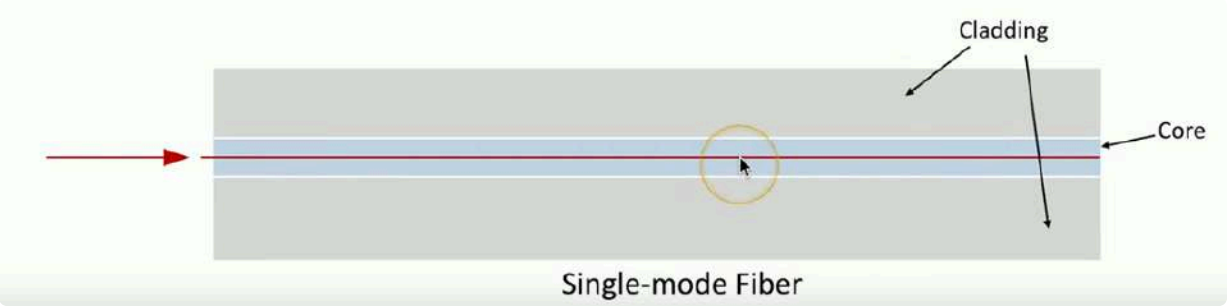
Multimode Fiber

- 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

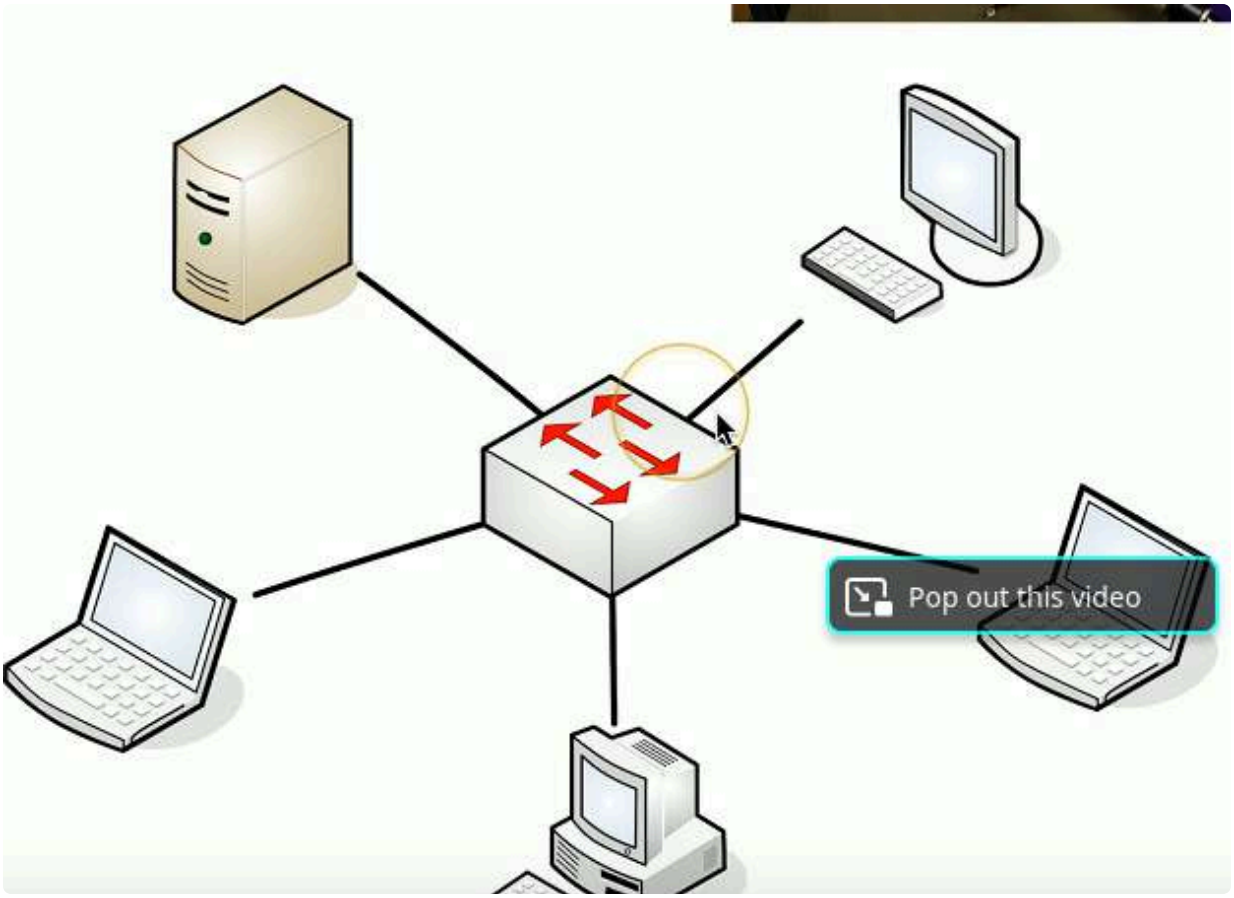
- Registered Jack type 11
  - 6 Position , 2 Conductor (6P2C)

- 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

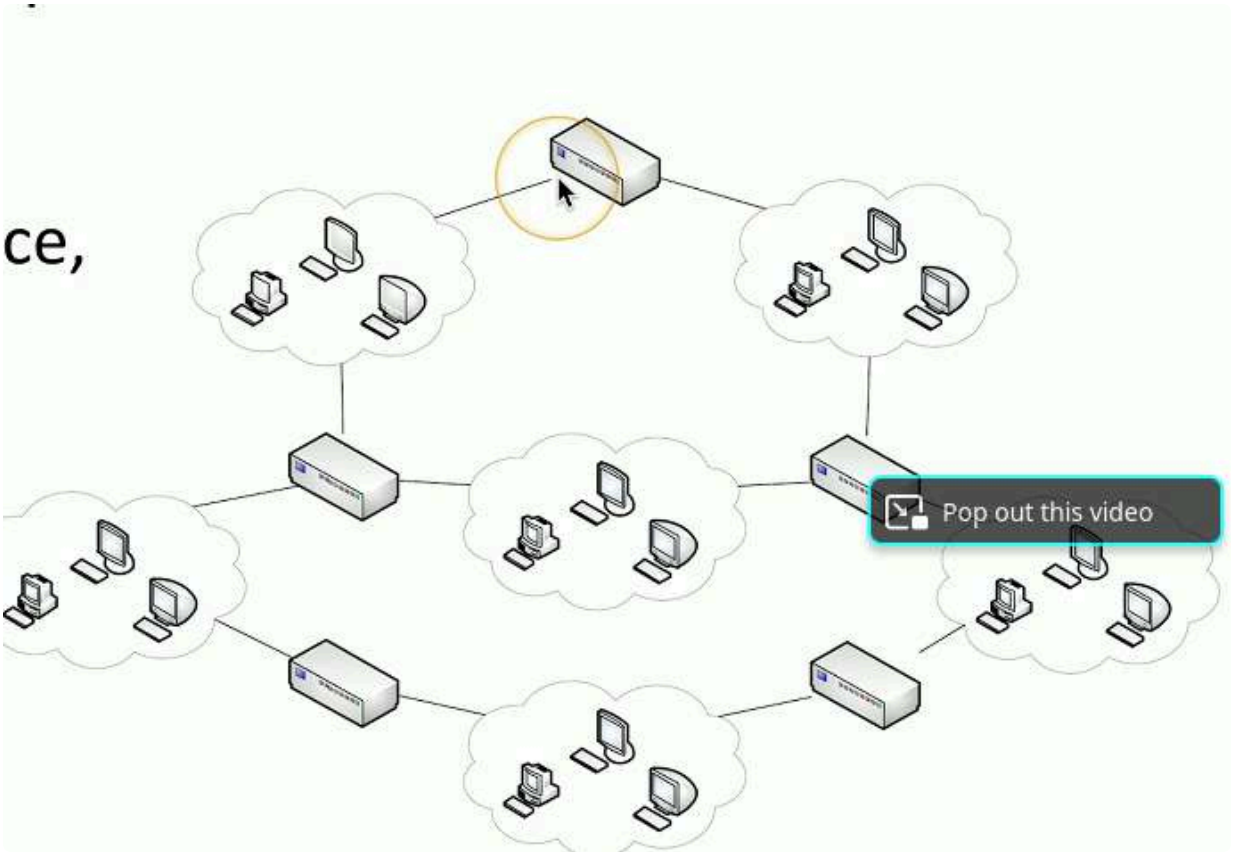
- Useful in planning a new network
  - Analogy -> Physical layout of a building or campus
- Assists in understanding signal flow and troubleshooting problems
  Star/Hub and spoke
- Used in most large and small networks
- All devices are connected to a central device

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



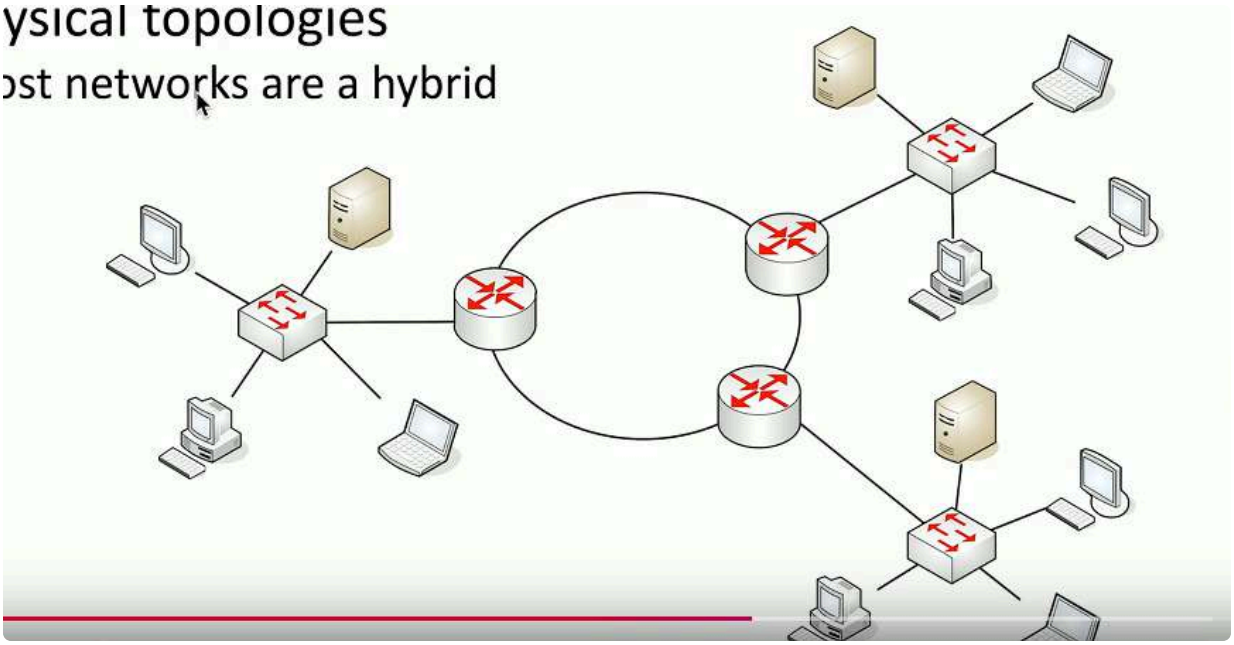
Mesh Network

- 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

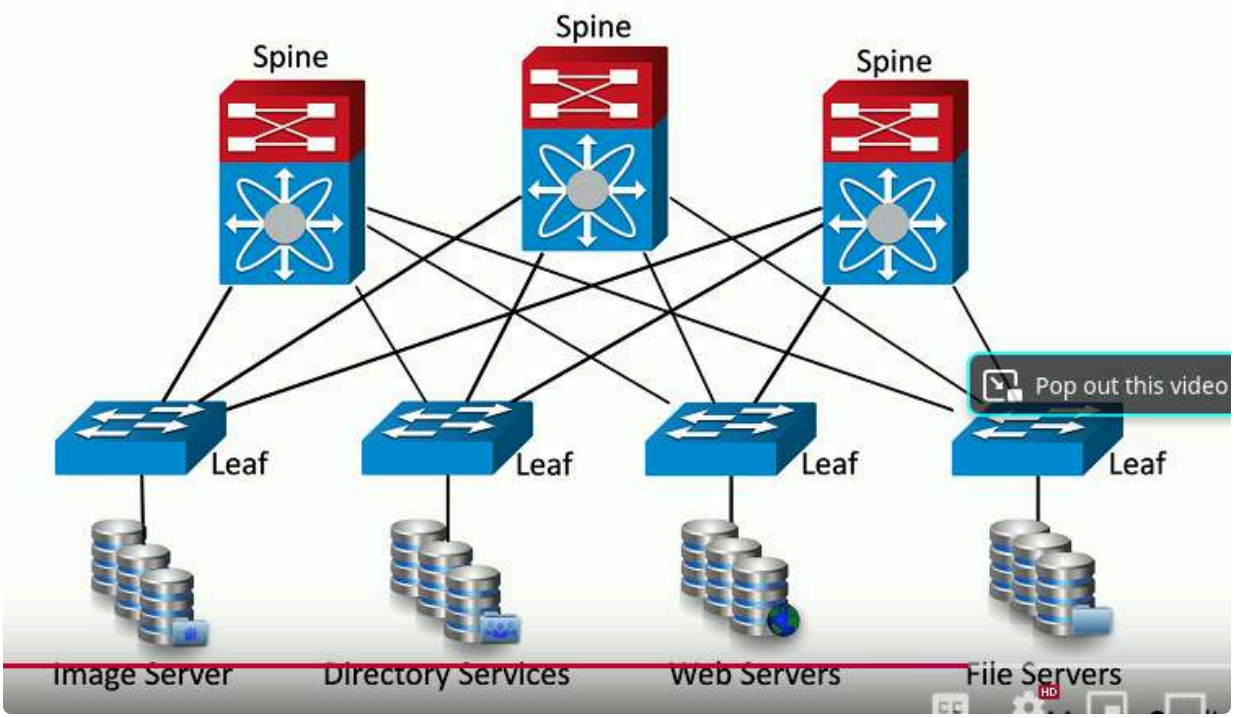
- A combination of one or more physical topologies
- Most networks are a hybrid



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



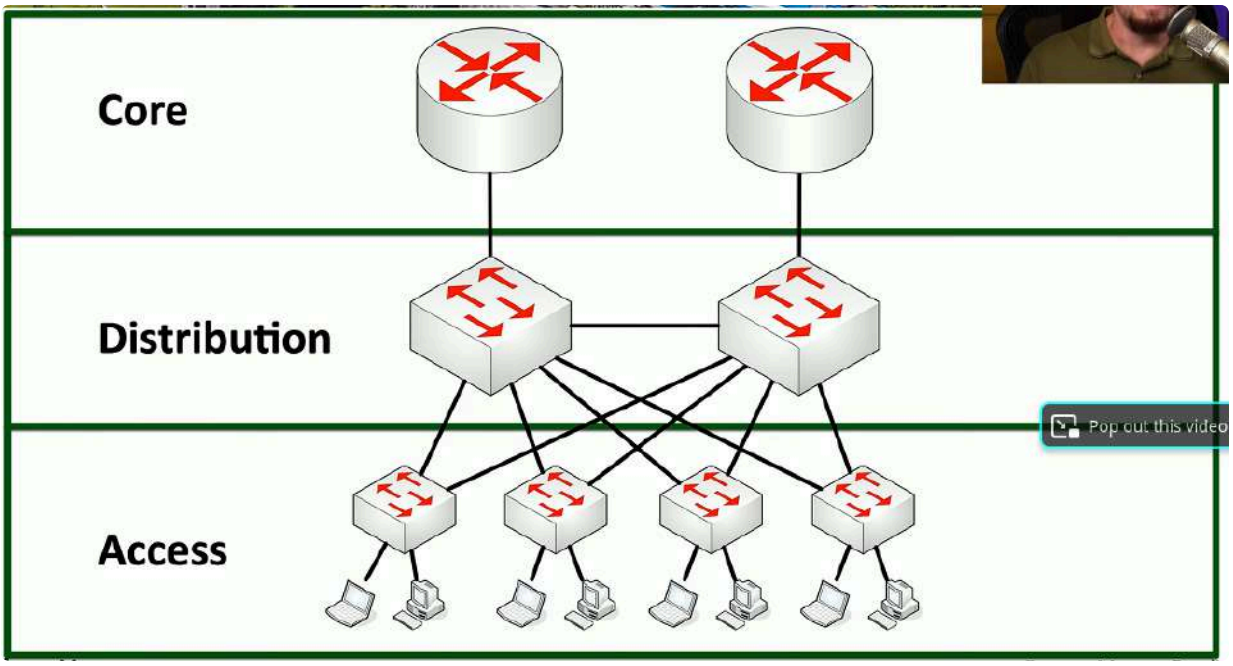
Point-to-point

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

1.6 Network Architectures

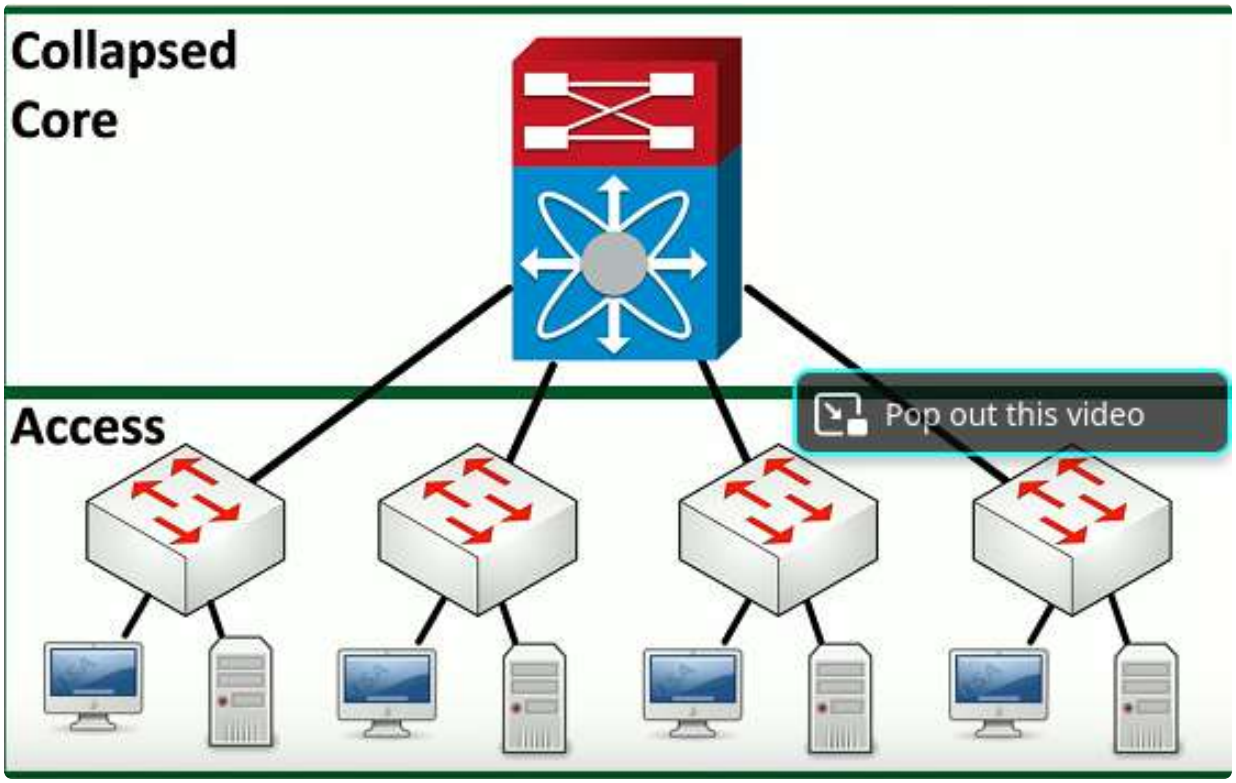
Three tier architecture

- 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



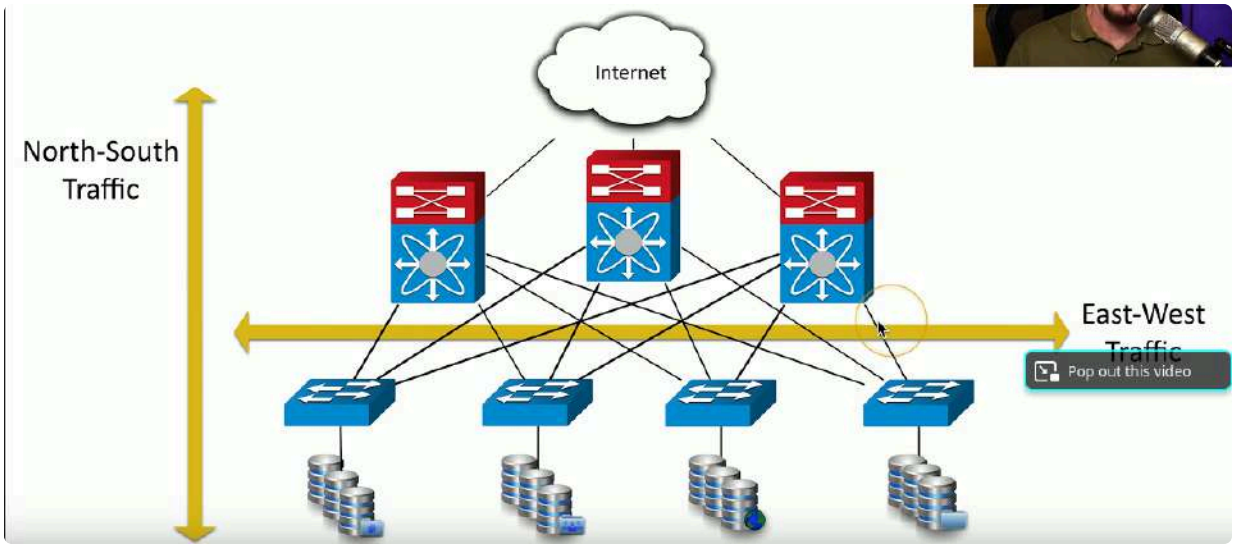
Collapsed core

- 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



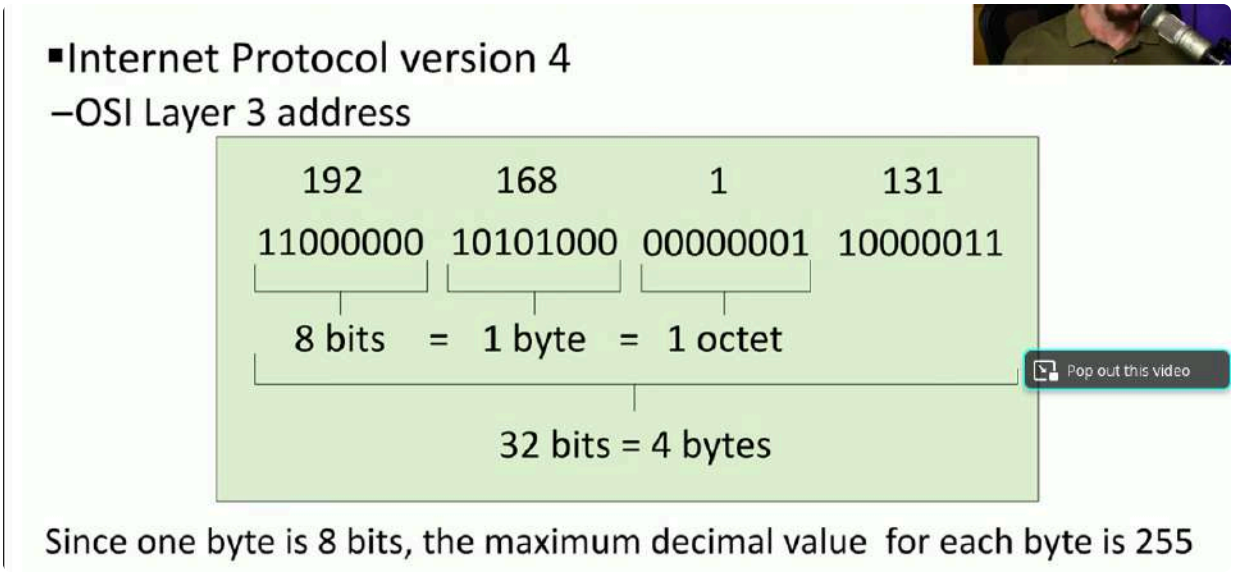
1.7 Binary Math

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

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

1.7 IPv4 Addressing

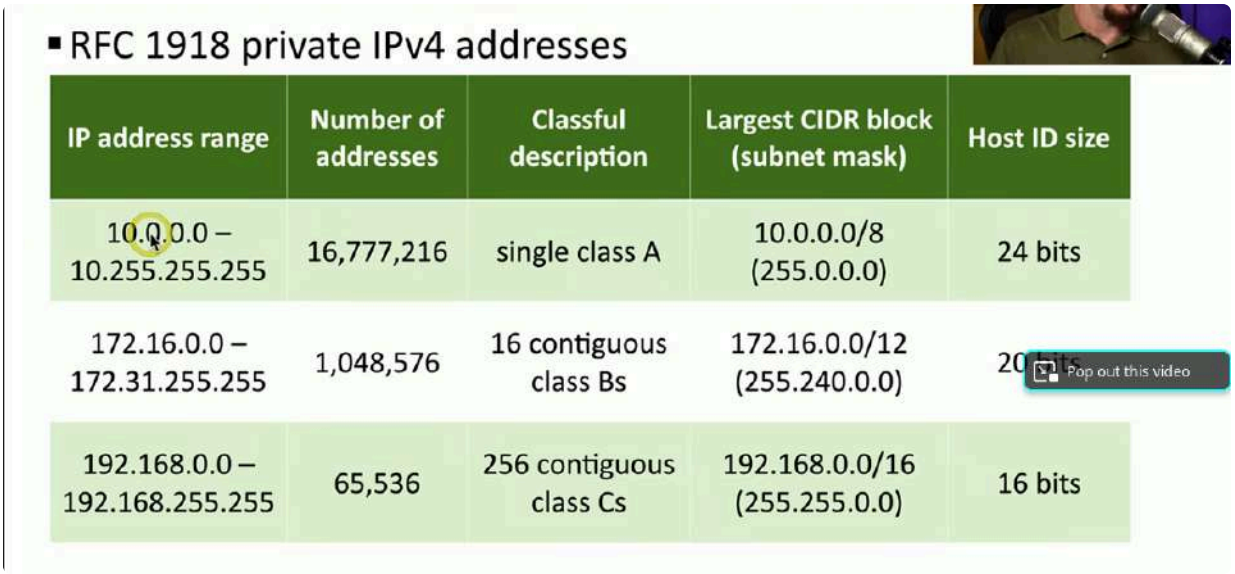
- IP Address, e.g, 192.168.1.165
  - Every device needs a unique IP address
- Subnet mask, e.g, 255.255.255.0
  - Used by local device to determine what subnet it's on
  - Not usually transmitted across the network
- Default gateway, e.g, 192.168.1.1
  - The router that allows you to communicate outside 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



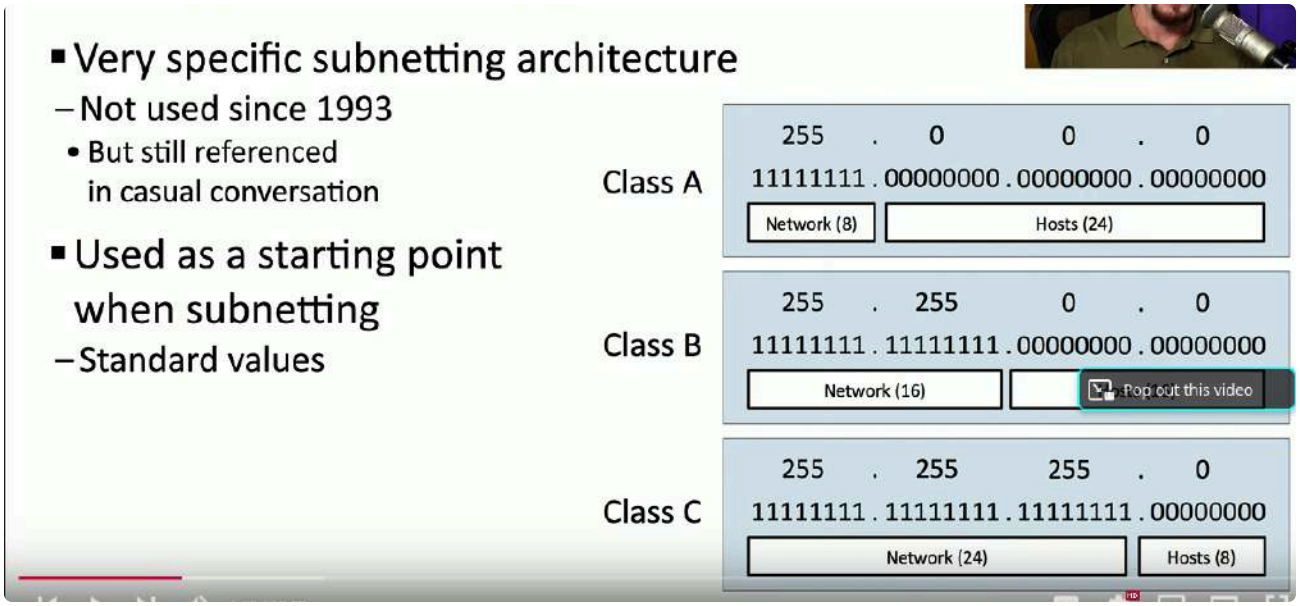
DHCP

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

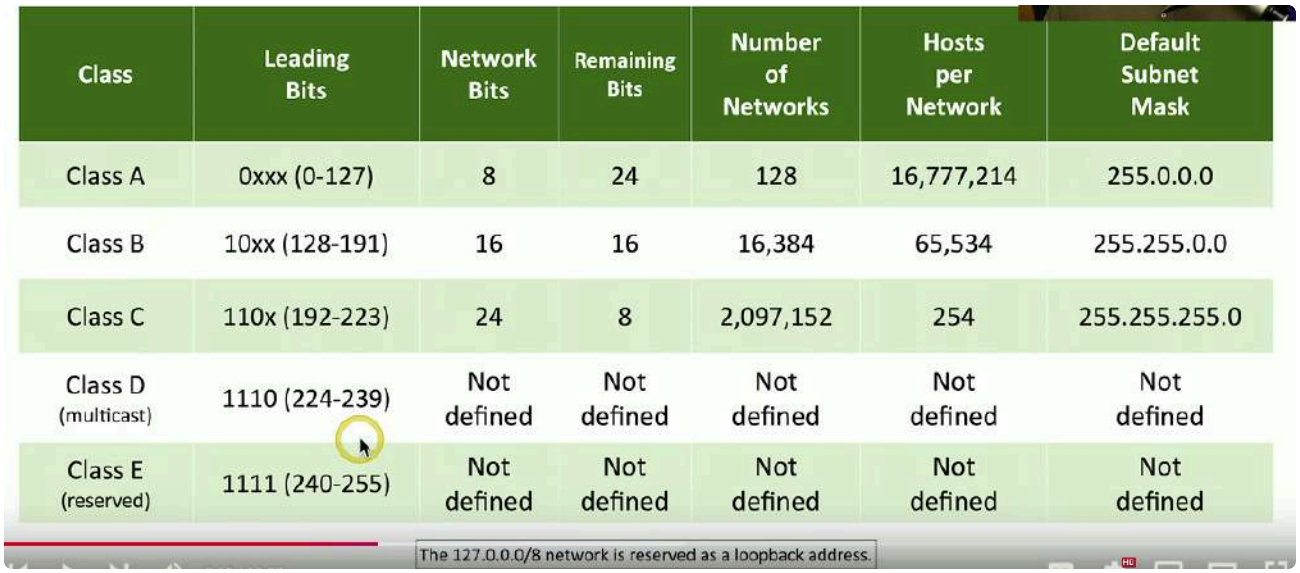
- DHCP (Dynamic Host Configuration Protocol) automatically provides addresses and IP configurations for almost all devices
  Automatic Private IP Addressing (APIPA)
- A link-local address
  - Can only communicate to other local devices
  - No forwarding by routers
- IETF has reserved 169.254.0.1 through 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

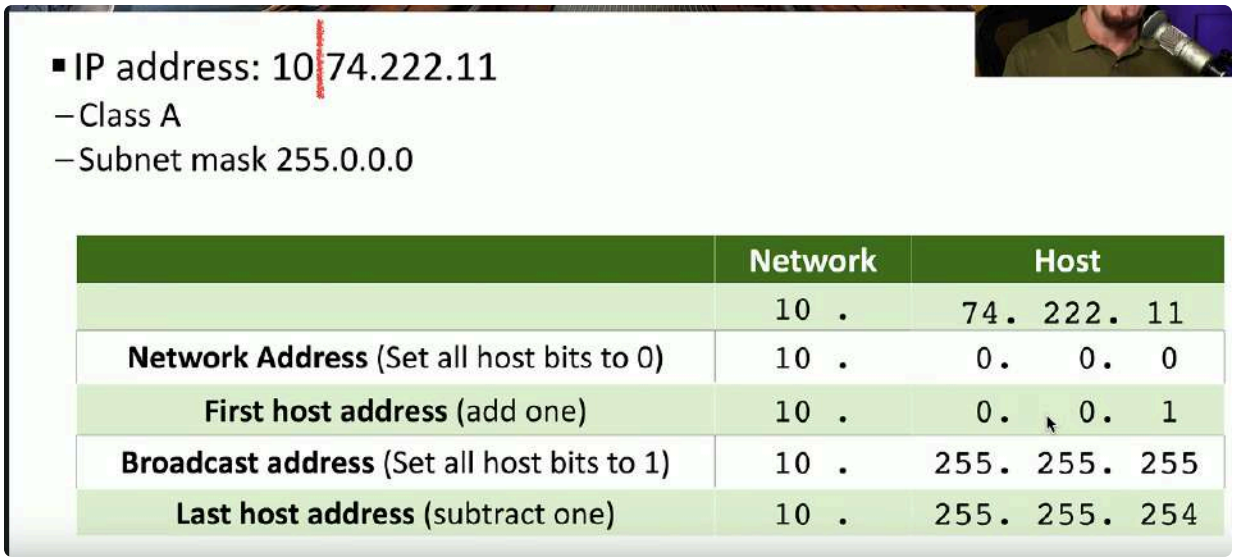


Class	Leading Bits	Network Bits	Remaining Bits	Number of Networks	Hosts per Network	Default Subnet Mask
Class A	0xxx (0-127)	8	24	128	16,777,214	255.0.0.0
Class B	10xx (128-191)	16	16	16,384	65,534	255.255.0.0
Class C	110x (192-223)	24	8	2,097,152	254	255.255.255.0
Class D (multicast)	1110 (224-239)	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

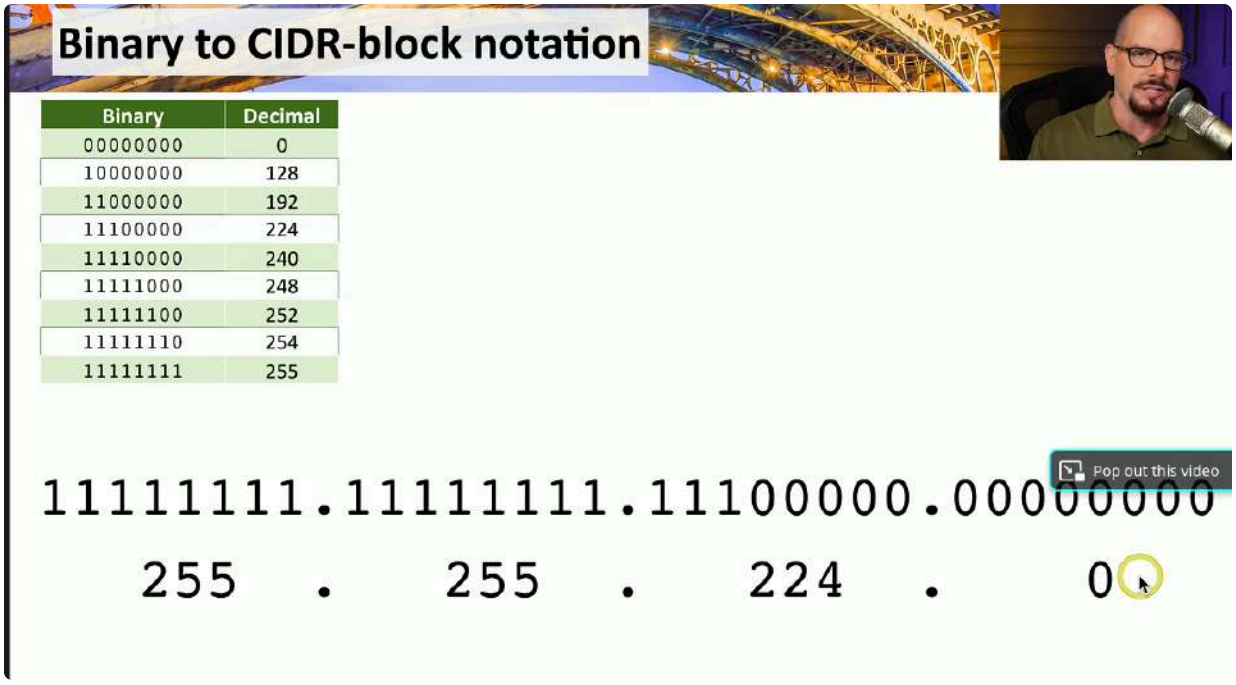
- CIDR (Classless Inter-Domain ROuting)
  - Created around 1993, Removed restrictions created by classful subnet masks
  - "Cider" block notation

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

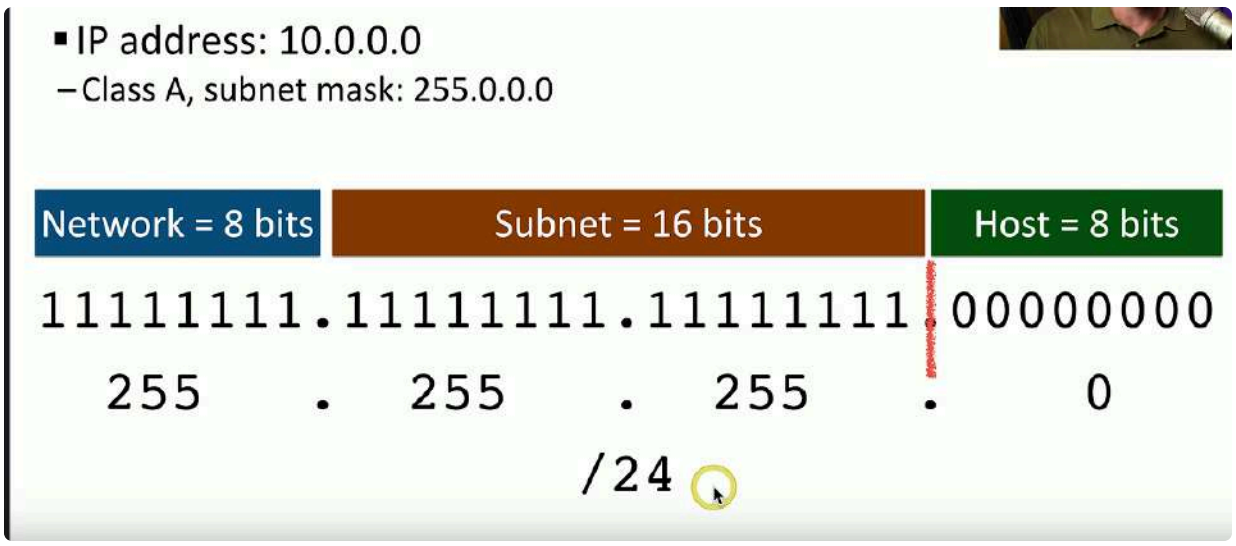
VLSM (Variable Length Subnet Masks)

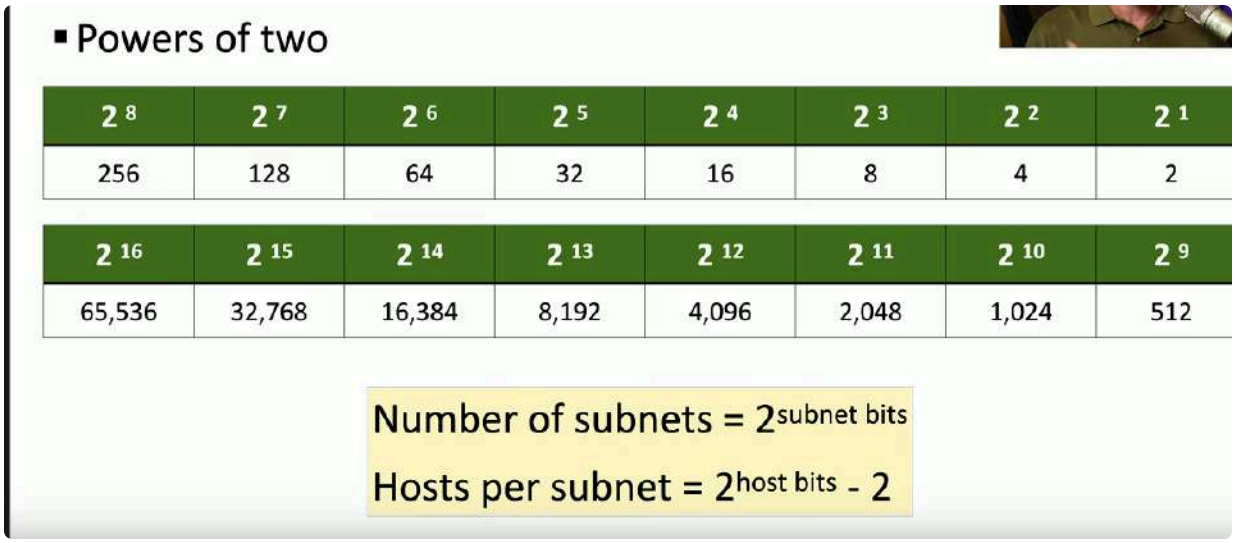
- Class-based networks are inefficient
- VLSM allows network admins to define their own masks
  - Customize subnet mask to specific network requirements
- Use different subnets masks in the same classful network

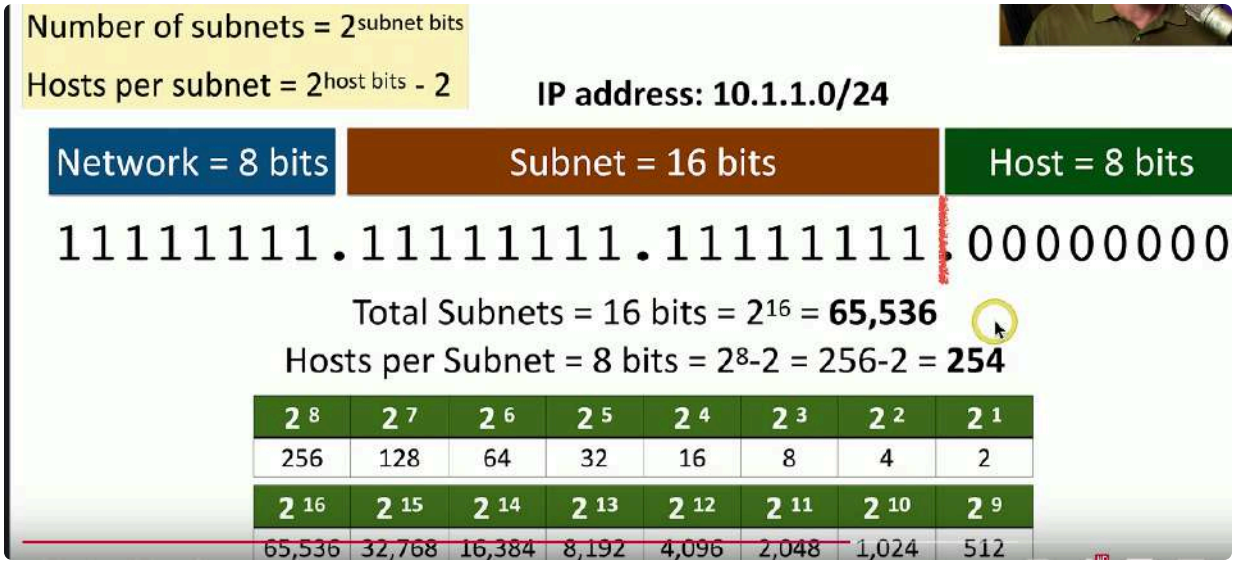
  - 10.0.0.0/8 is the class A network

  - 10.0.1.0/24 and 10.0.8.0/26 would be VLSM

Defining Subnets

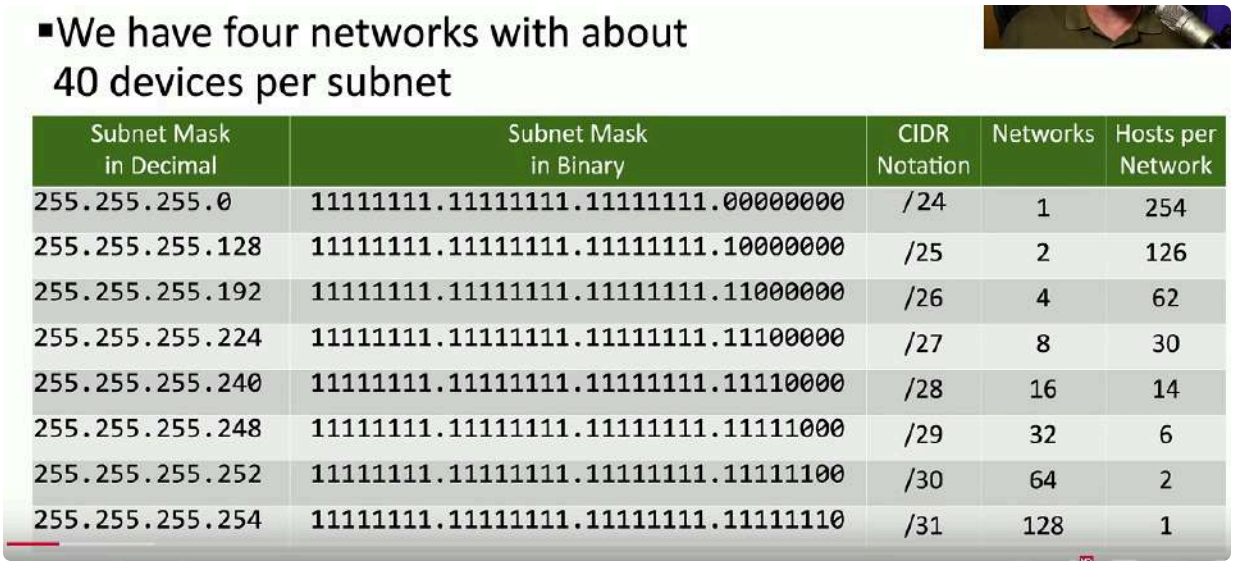






1.7 Magic Number Subnetting

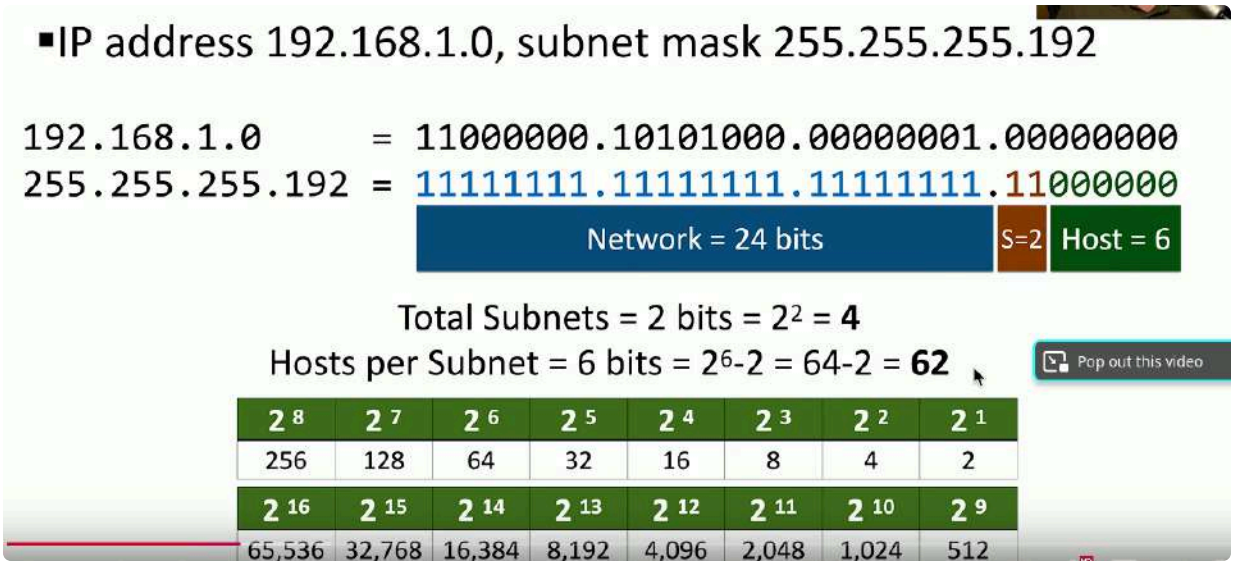
- Say we have IP address assignment
  - Network: 192.168.1.0/24
- We need an IP addressing scheme with more than one network address that can supports 40 devices per subnet



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

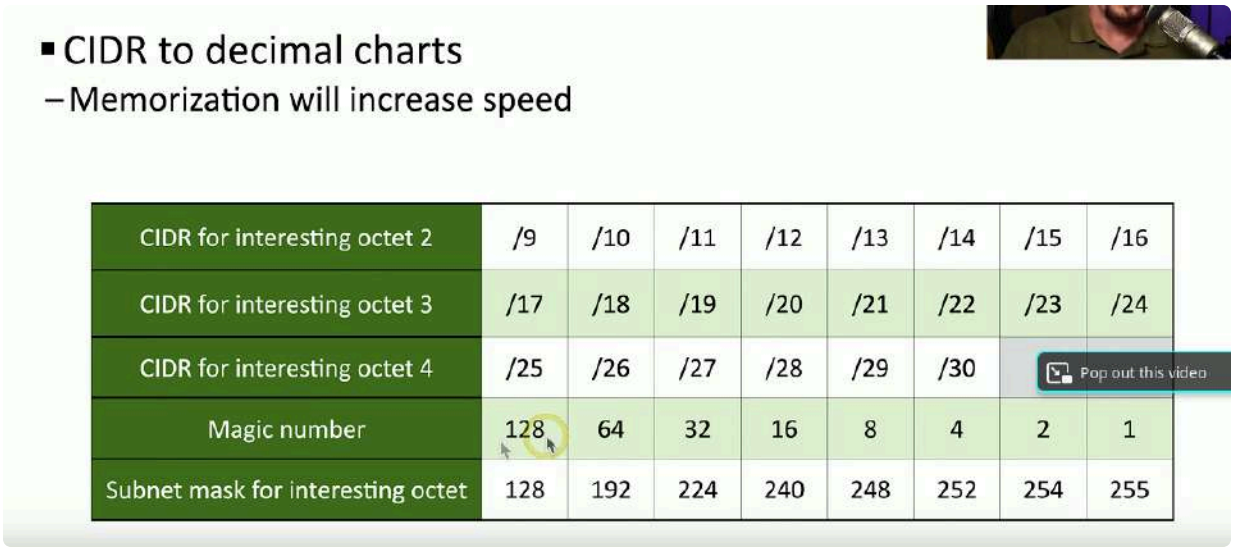
- We can see why we chose this subnet mask from the diagram above which shows that when choosing /26 Subnet mask we get 4 networks and 62 hosts per network which is closest to our 40 devices per subnet and number of networks.
  - Also note how as networks increase hosts per network decrease (inverse)



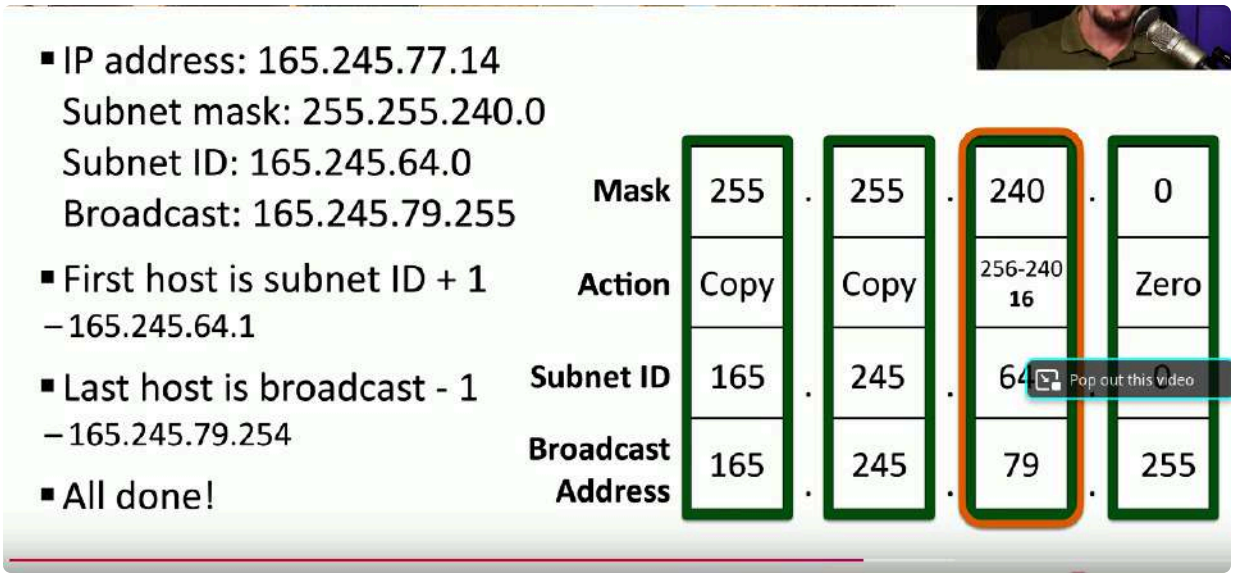
Wanted Addresses :

- 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:

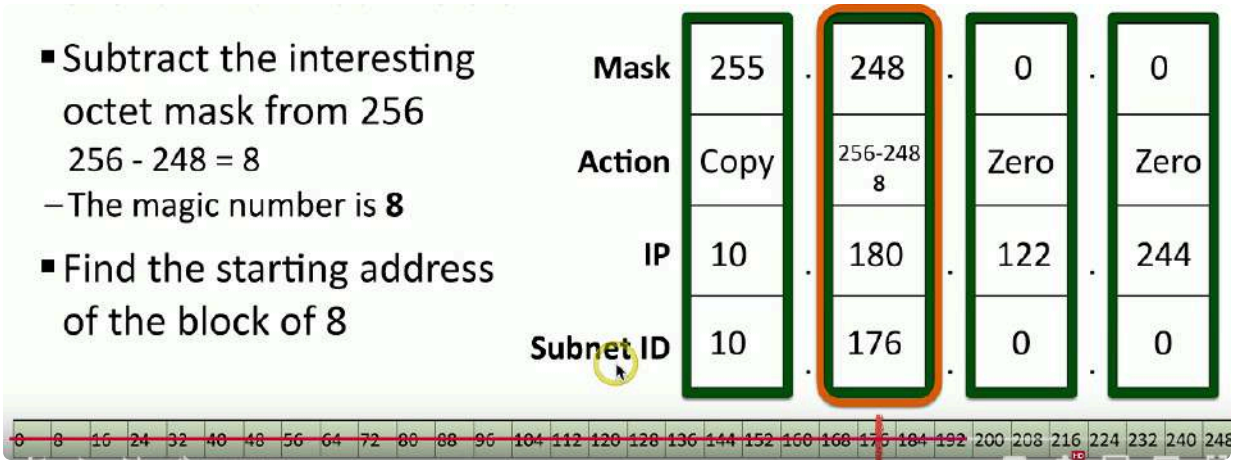


CIDR for interesting octet 2	/9	/10	/11	/12	/13	/14	/15	/16
CIDR for interesting octet 3	/17	/18	/19	/20	/21	/22	/23	/24
CIDR for interesting octet 4	/25	/26	/27	/28	/29	/30		
Magic number	128	64	32	16	8	4	2	1
Subnet mask for interesting octet	128	192	224	240	248	252	254	255

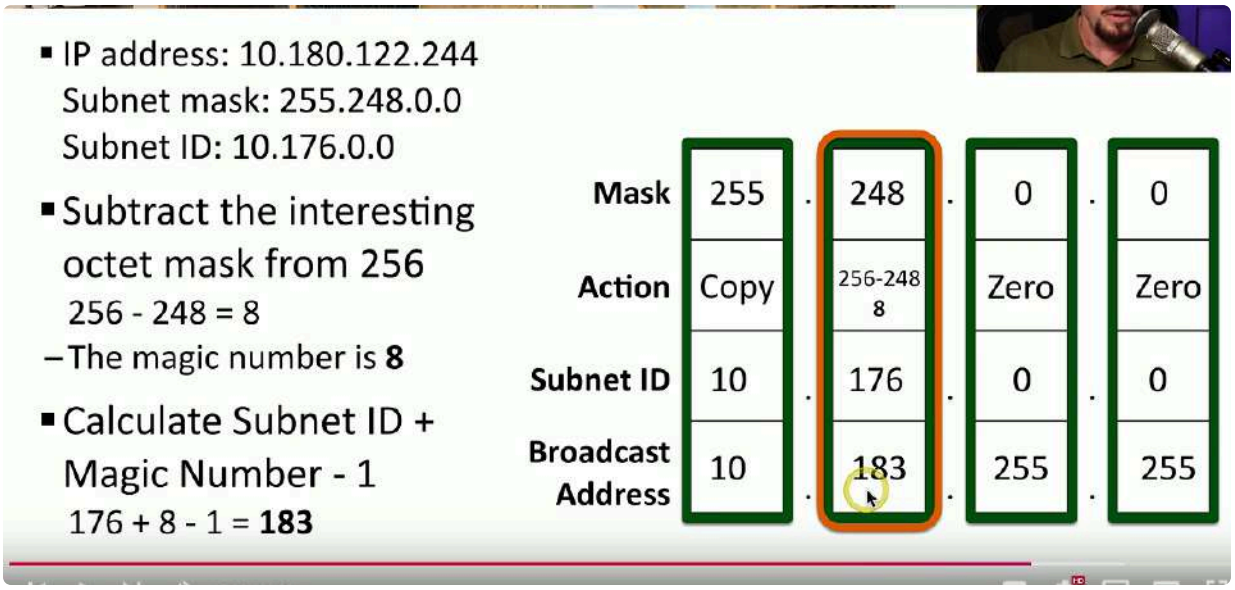


For broadcast - subtract our mask non 255 number from 256 and then take our magic number and add it to the corresponding subnet ID - 1 -> So 16+64-1 = 79

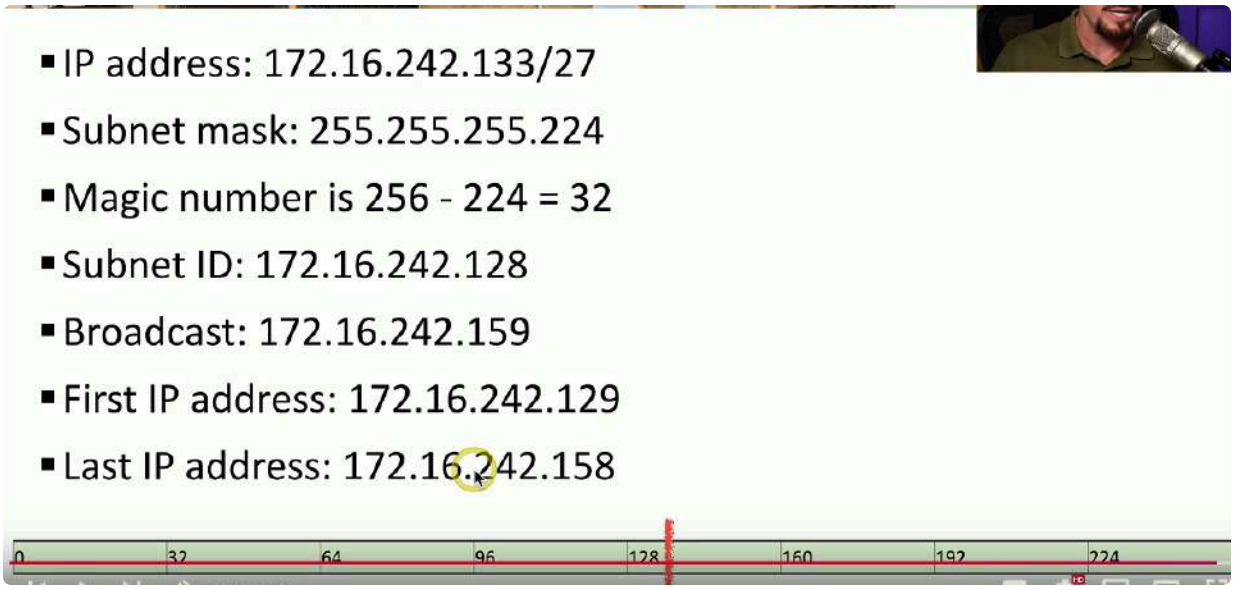
- For 255 in Mask we Copy the IP val to Subnet ID and for any zeroes we place zeros in same corresponding location
- However for calculating broadcast we replace 0 vals with 255



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

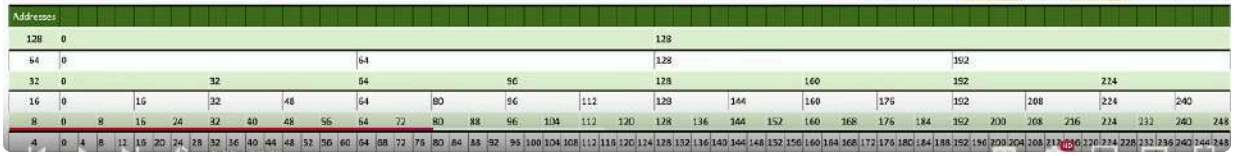
Pop out this video

Network Address Subnet Boundaries

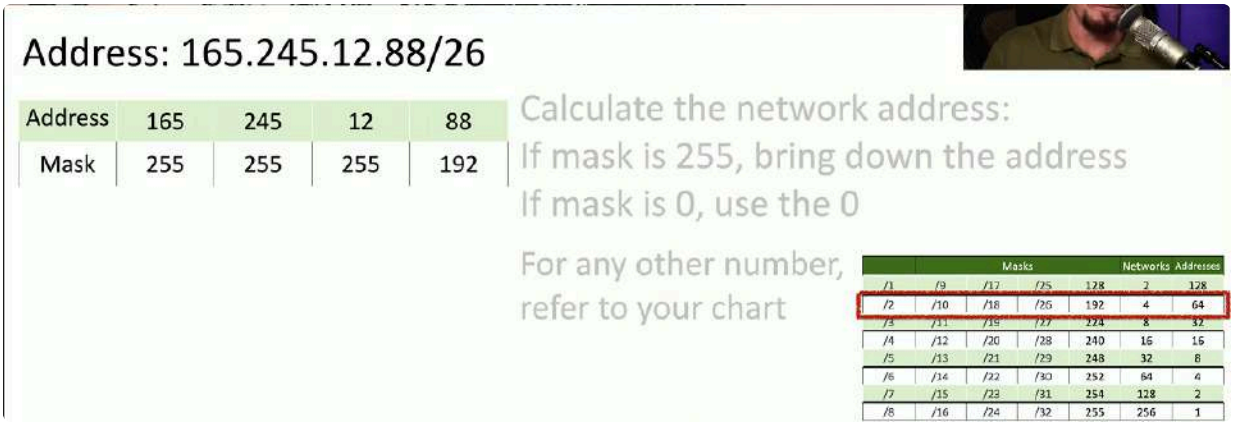
Addresses																
128	0	128														
64	0	64	128	192												
32	0	32	64	96	128	160	192	224								
16	0	16	32	48	64	80	96	112	128	144	160	176	192	208	224	240
8	0	8	16	24	32	40	48	56	64	72	80	88	96	104	112	120
4	0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60

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

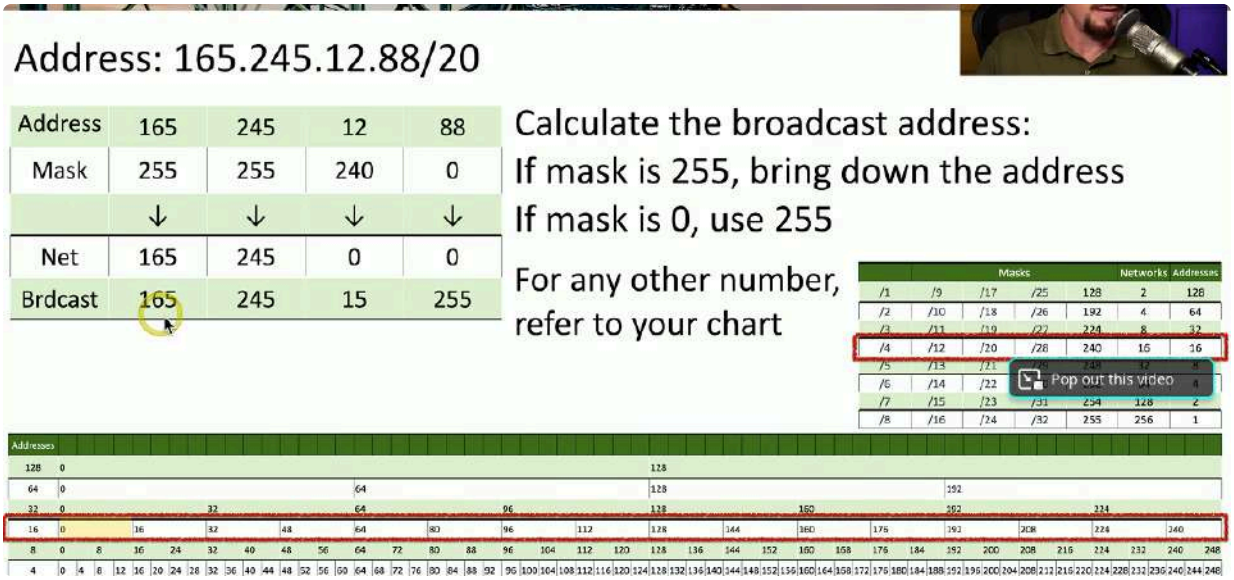


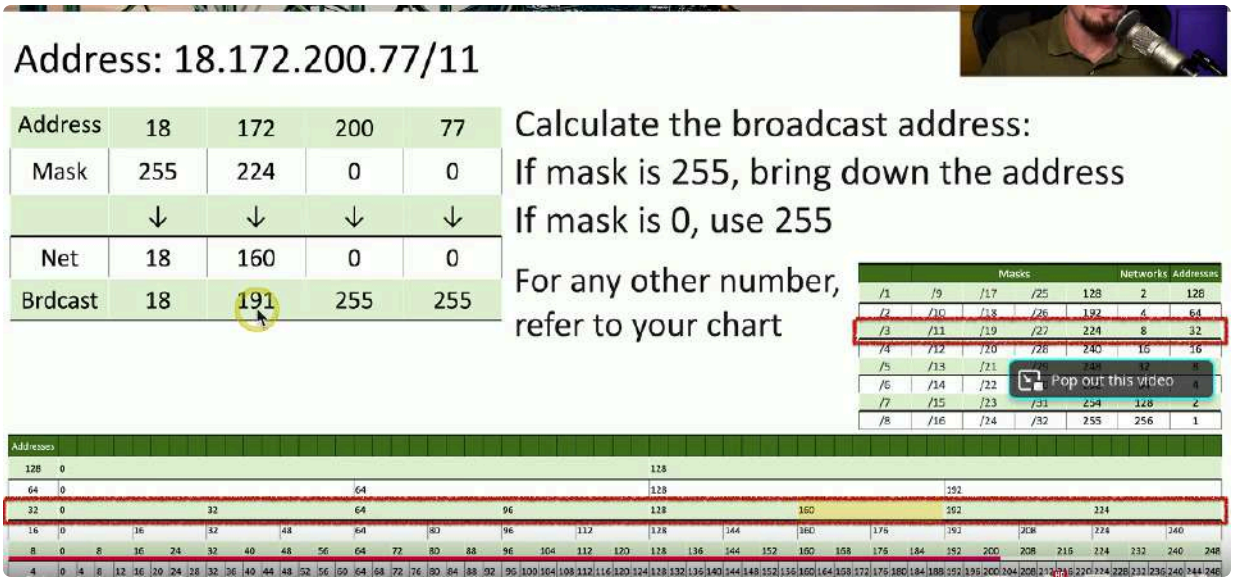
- First IP is Net address +1 -> Last IP is Broadcast address -1



- /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





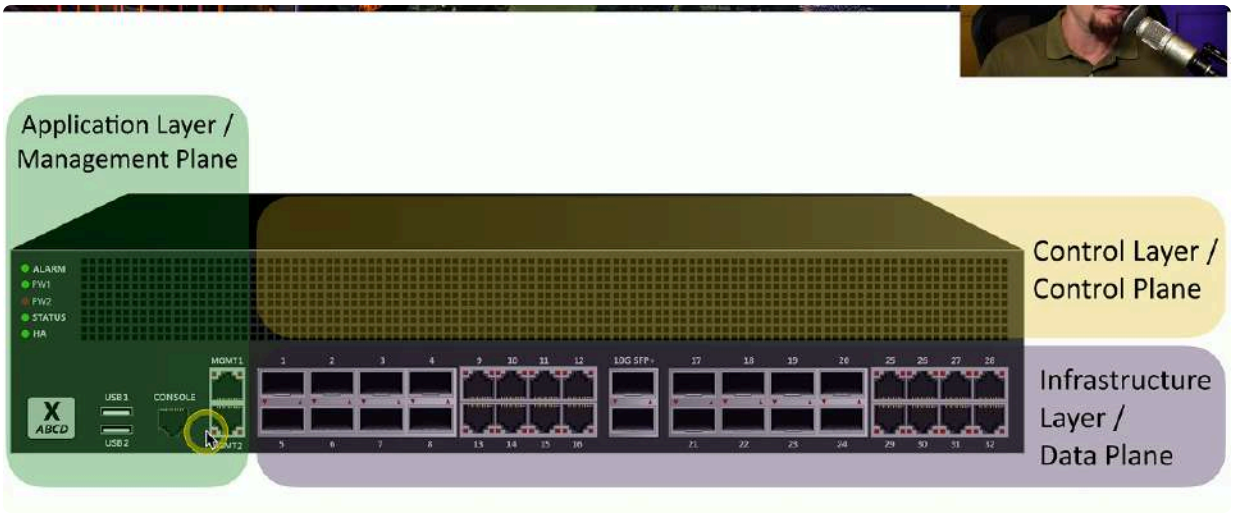
Note how for CDIR /11 we are interested in octet 2 (172), this tells us to use 224 as its subnet mask value, and all others become 0'sa

- 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

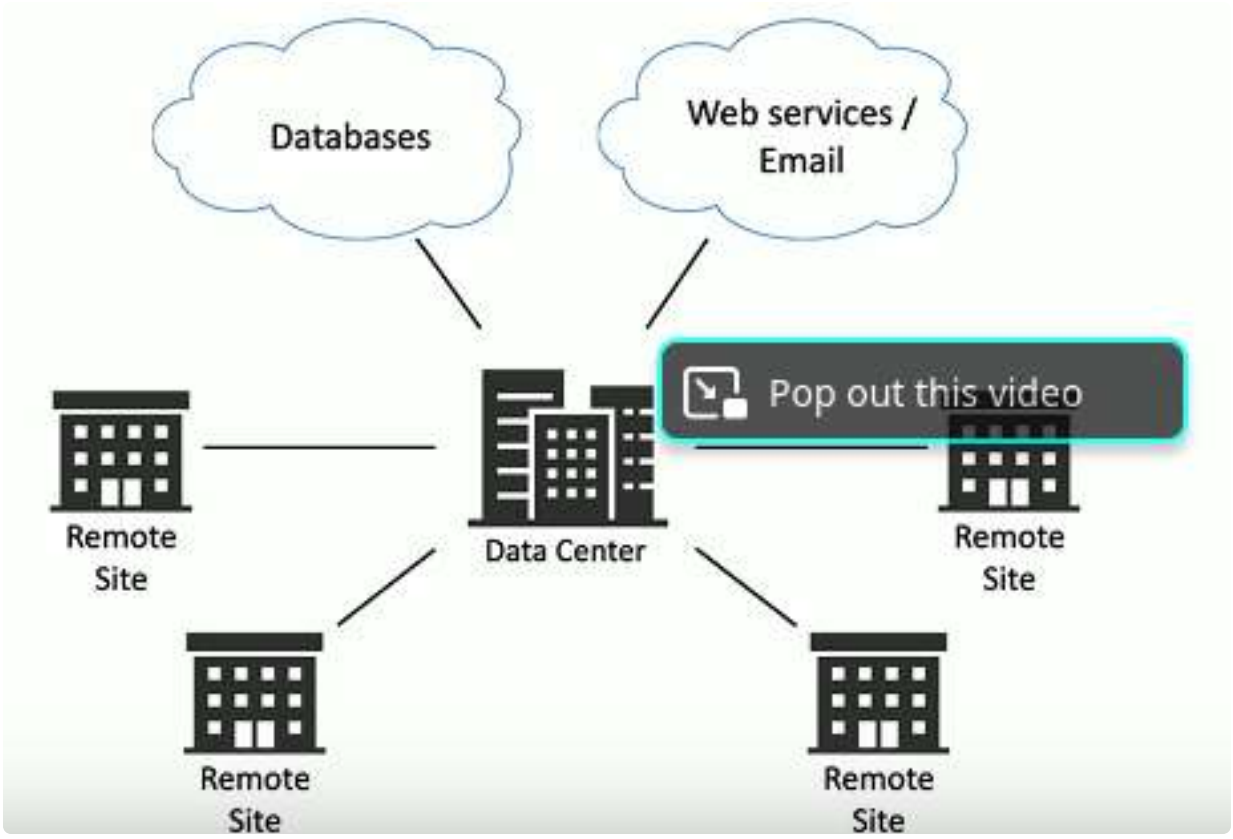
Firewall Example of Physical Architecture



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)

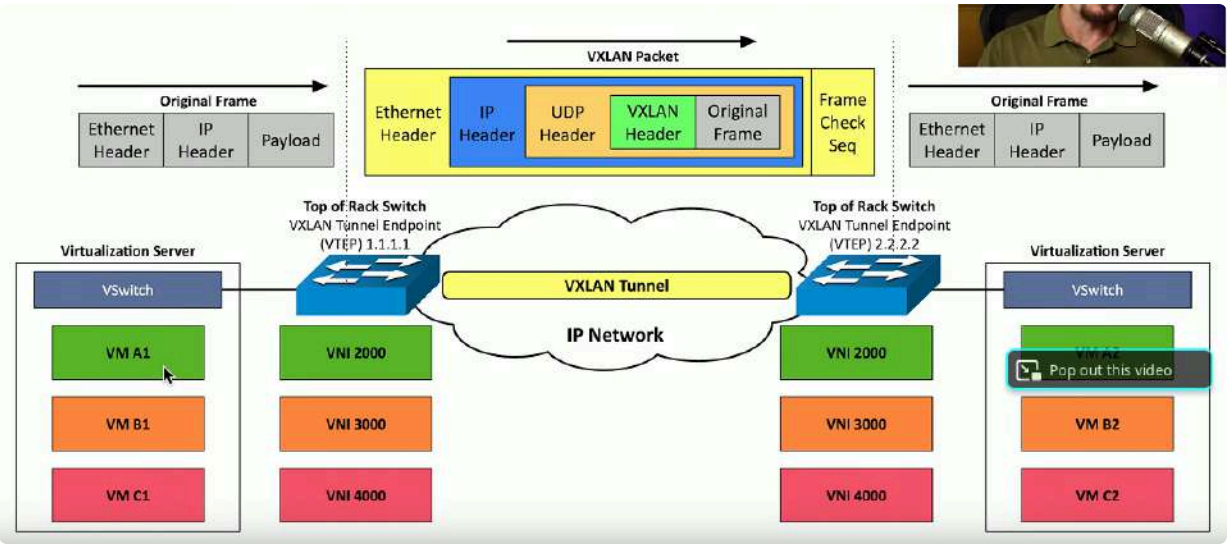
- Connect multiple data centers together
  - Seamlessly span across these geographic distances
- Connect and segment different customer networks
  - Across multiple data centers
  - All customers share the same core network
- Distribute applications everywhere
  - Increase uptime and availability
  -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

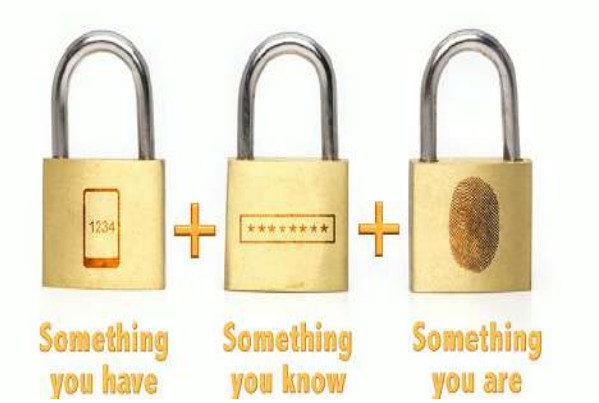
  VXLAN Encapsulation



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...



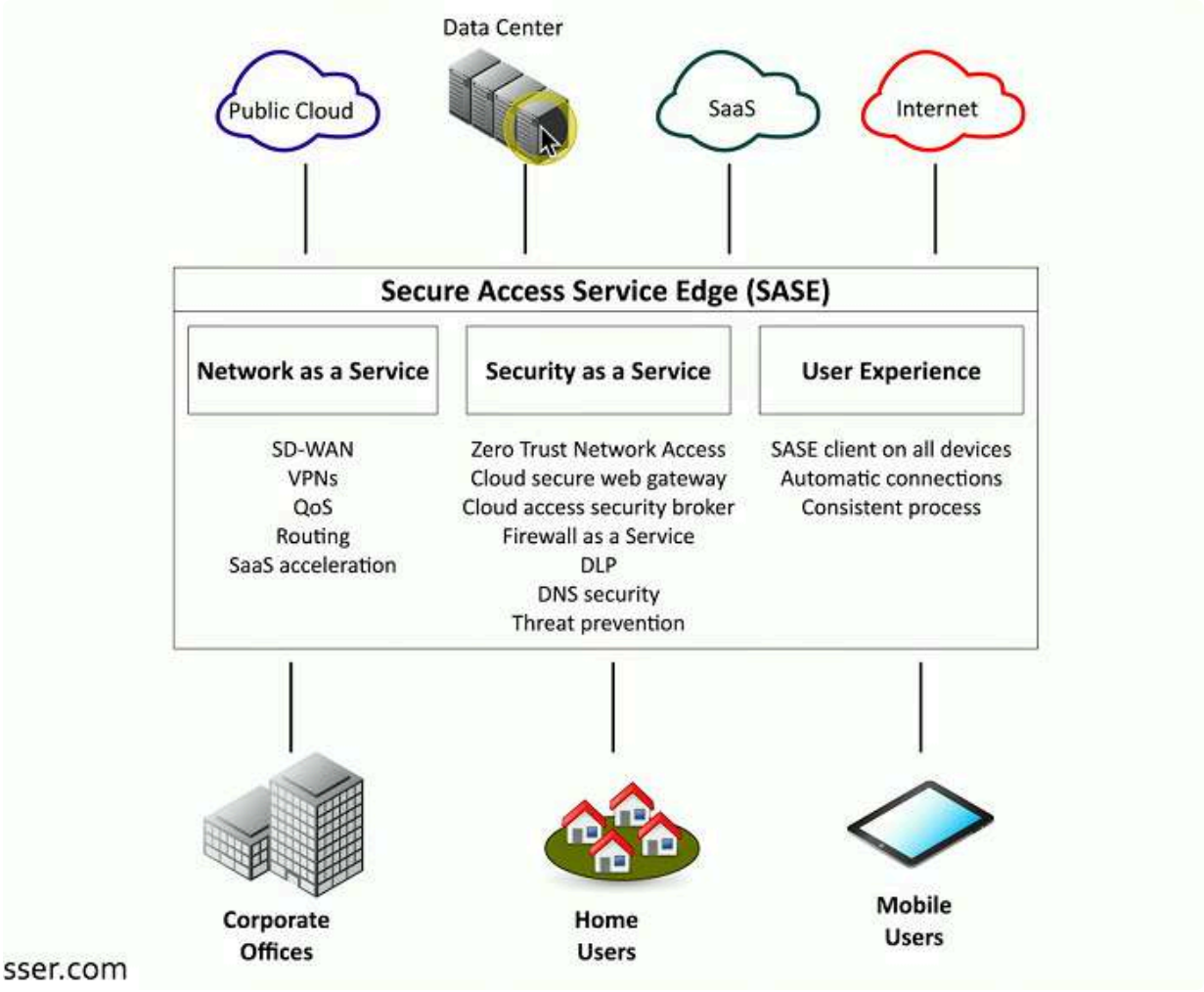
  Policy Based Authentication
- Adaptive identity
  - Consider the source and the requested resources
  - Multiple risk indicators -> relationship to org, physical location, type of connection , IP address, etc.
  - Make the authentication stronger, if needed
- Policy driven access control
  - Combine 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



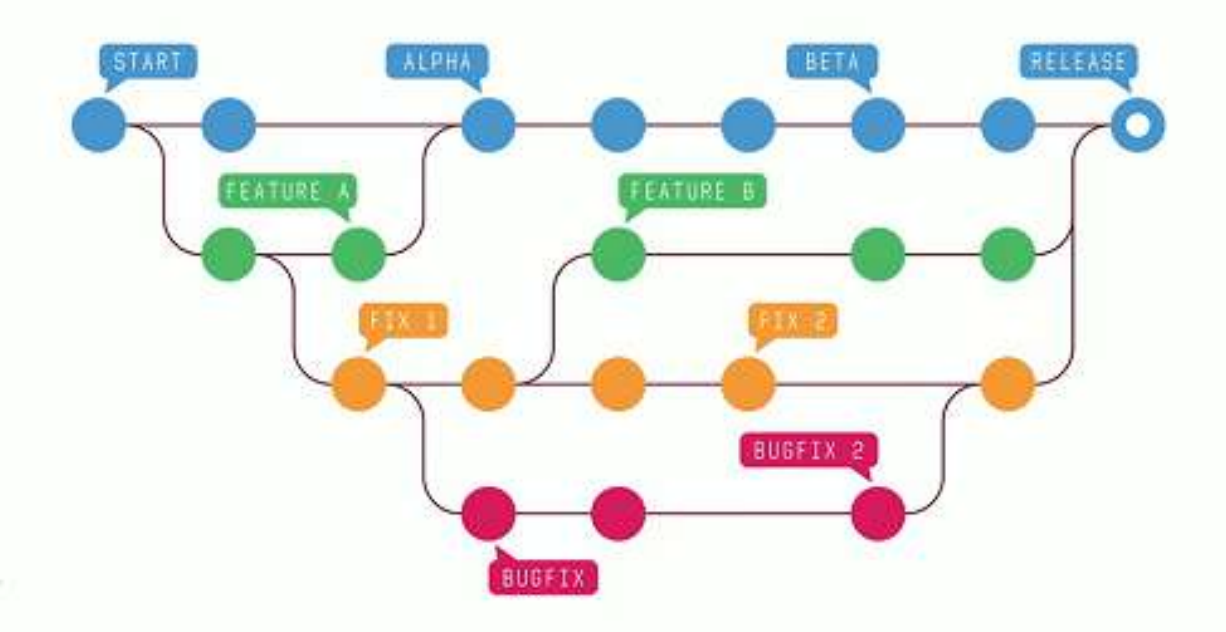
1.8 Infrastructure as Code

- 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

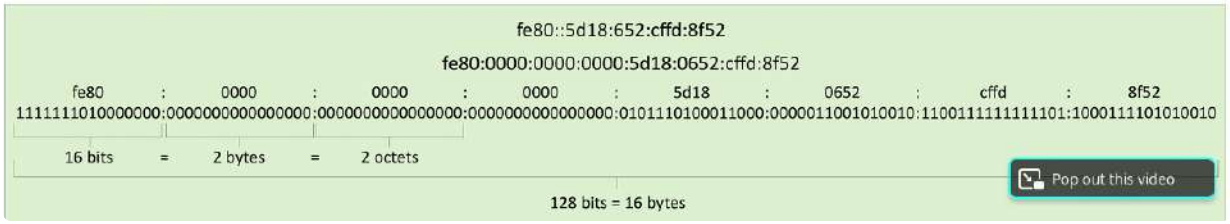
1.8 IPv6 Addressing

IPv4 Address Exhaustion

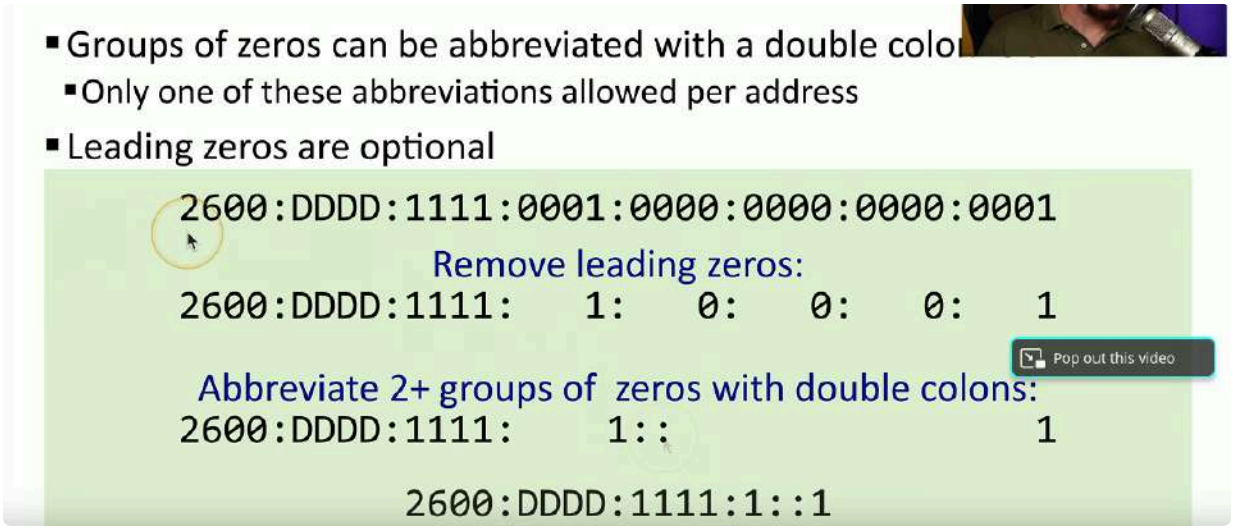
- There are an estimated 20B devices connected to internet and growing
  - IPv4 Supports around 4.29B addresses
- The address space for IPv4 is exhausted -> None available to assign
- IPv4 and NAT is a workaround -> Can be challenging with certain protocols
- IPv6 provides a larger address spaces

  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

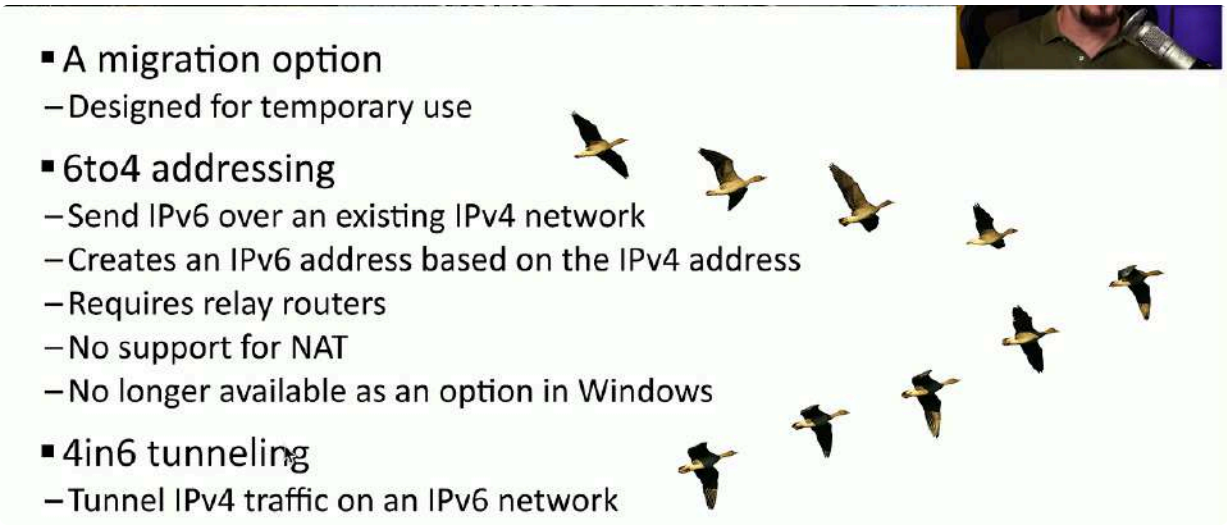
- 2601:4C3:4002:BE00:0:0:0:66

  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.

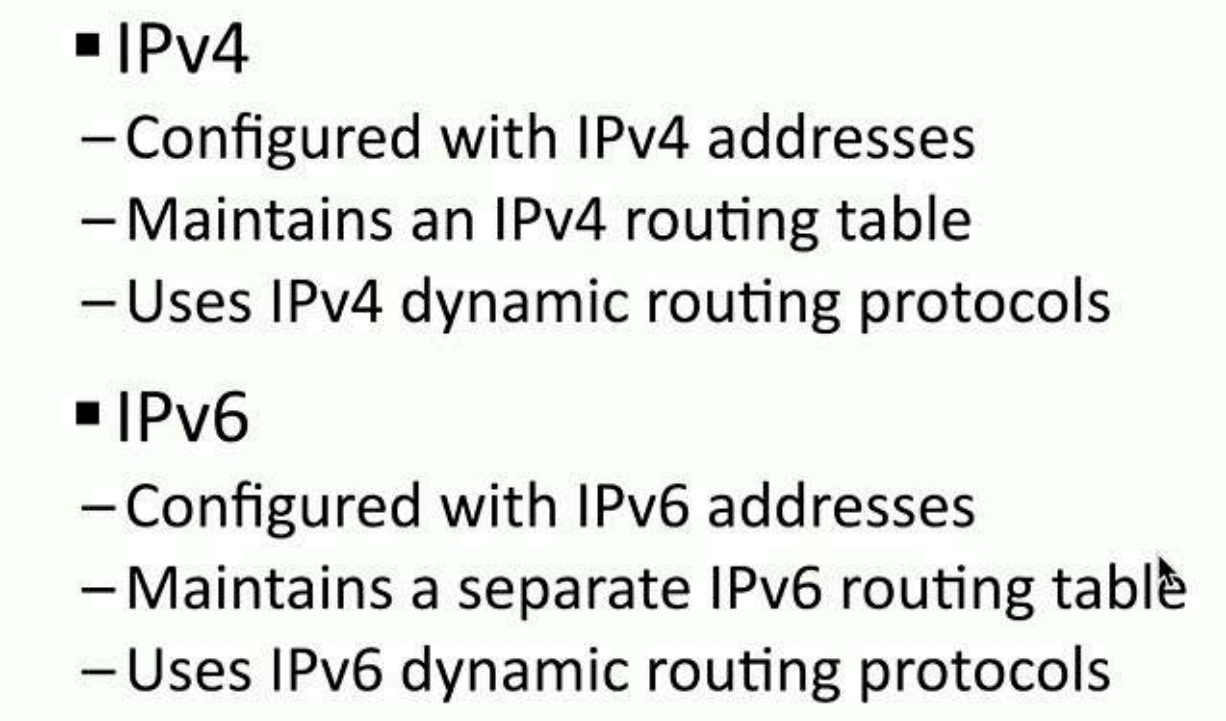
    - How can IPv4 device talk to an IPv6 Server?
    - Can IPv6 device communicate with legacy IPv4 Server?
- Requires alternate form of communication
    - Tunnel: Encapsulate one protocol within another
    - Dual-stack: Have the option to use both v4 and v6
    - Translate: Convert between IPv4 and IPv6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

Tunneling IPv6



Dual-Stack Routing

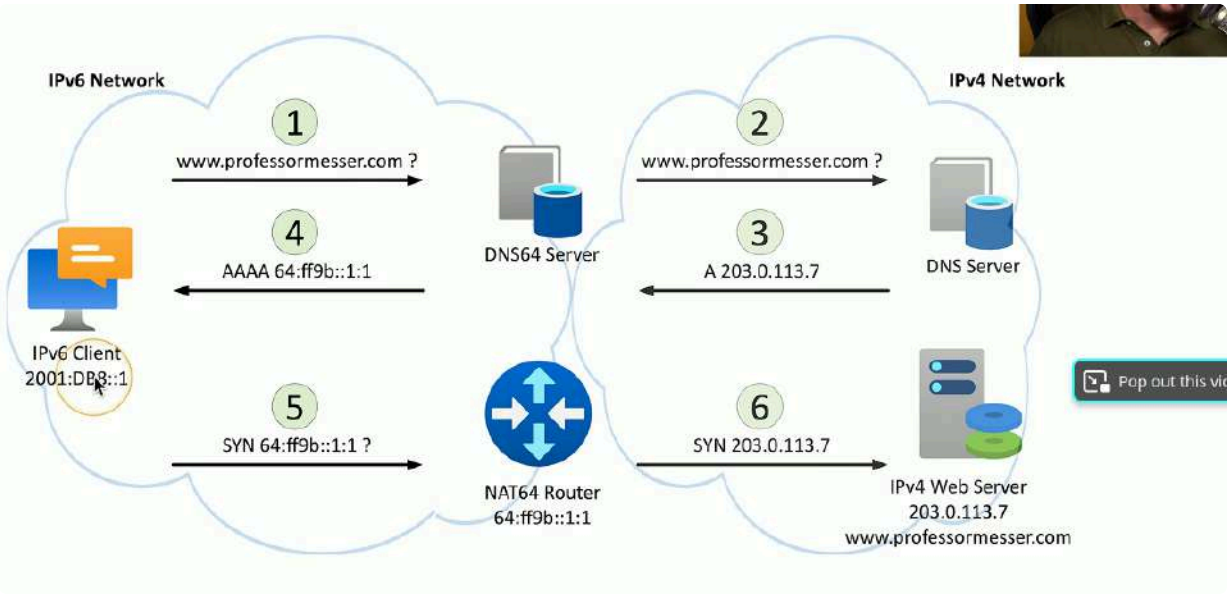
- Dual-stack v4 and v6 -> Run both at same time -> Interfaces assigned multiple address types



Translating between IPv4 and IPv6

- Network address translation using NAT64

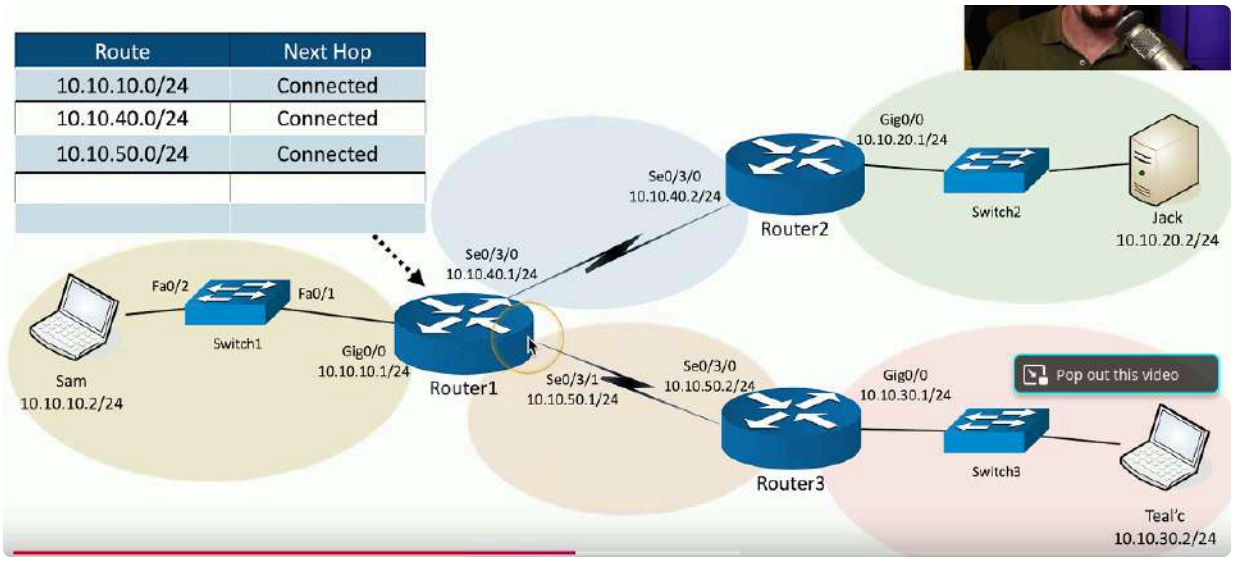
    - Translate between v4 and v6 -> Seamless to the end User
- Requires something in the middle to translate
    - IPv6 not backwards compatible w/ IPv4
    - Use a NAT64 capable router
- Works with DNS64 server
  - Translate the DNS requests



2.1 Static Routing

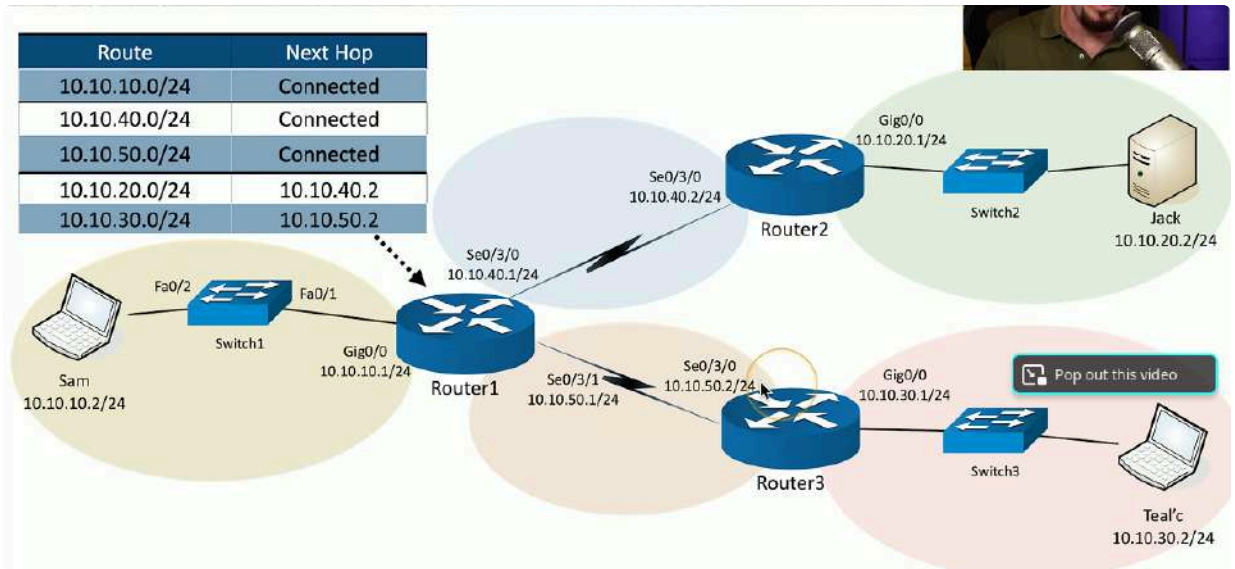
Routing Tables

- 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

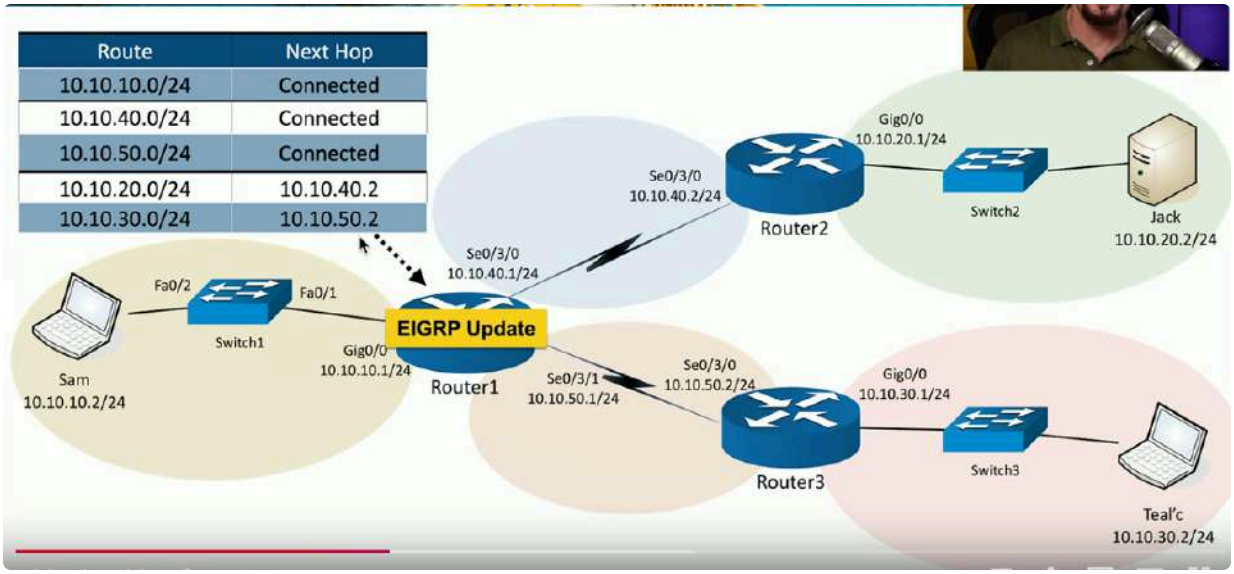
- Administratively define the routes ->You're in control
- Advantages:
  - Easy to config and manage in smaller networks
  - No overhead from routing protocols (CPU,memory,bandwidth)
  - Easy to configure on stub networks (only one way out)
  - More secure- no routing protocols to analyze
- Disadvantages:
  - Difficult to administer on larger networks
  - Not automatic method to prevent routing loops
  - If network change occurs, you have to manually update routes
  - No automatic routing if outage occurs



Note we have added new routes to our static table. Here if router 1 sees Route 10.10.20.0/24 it will know to send to router 10.10.40.2 which at this point will then check its own table and know where to hop next to for 10.10.20.0/24

2.1 Dynamic Routing

- Routers send routes to other routers
  - Routing tables are updated in almost real-time
- Advantages:
  - No manual route calculations or management
  - New routes populated automatically -> Very scalable
- Disadvantages
  - Some router overhead required (CPU,memory,bandwidth)
  - Requires some initial configuration to work properly



Router 2 or Router 3 and so forth send EIGRP update to router 1 so that it may update its routing table, this is done constantly.

Dynamic Routing Protocols

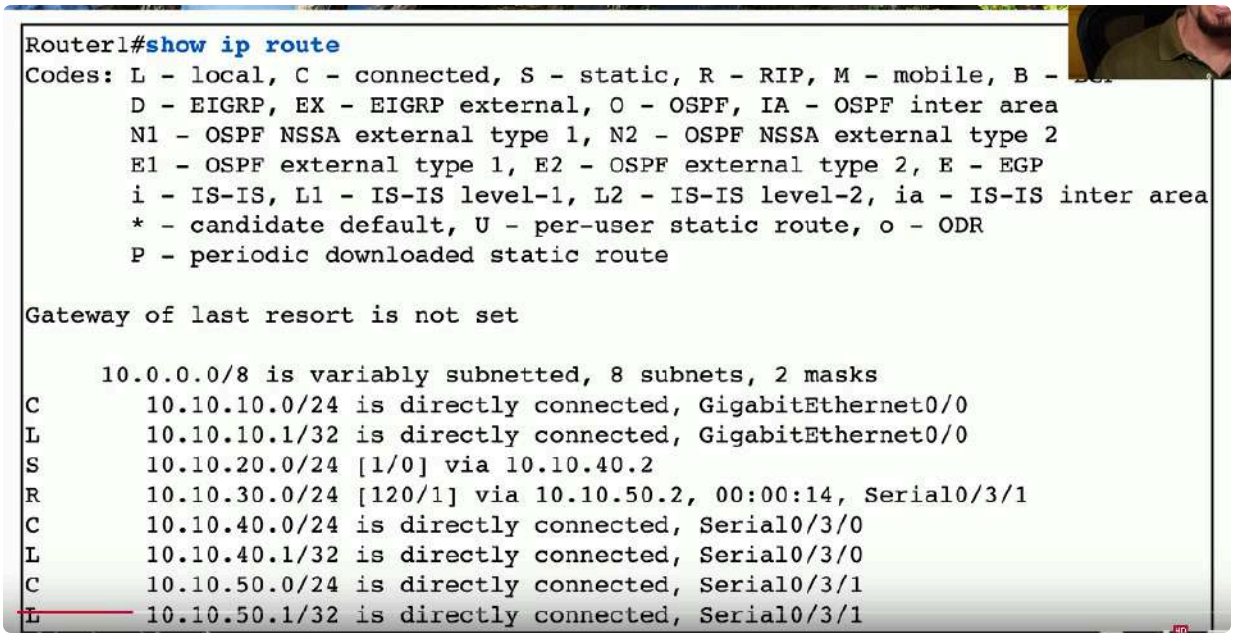
- Listen for subnet information from other routers -> Sent from router to router
- Provide subnet information to other router
  - Tell other routers what you know
- Determine the best path based on this information
  - Every routing protocol has its own way of doing this
- When network changes occur update the available routes
  Standard or Proprietary protocol?
- OSPF and BGP are standards
- Some functions of EIGRP are Cisco proprietary
  EIGRP (Enhanced Interior Gateway Routing Protocol)
- Partly proprietary to Cisco

    - Commonly used on internal Cisco-routed networks ->Relatively easy to enable and use
- Cleanly manage topology changes
    - Speed of convergence is always a concern
    - Loop free operation
- Minimize bandwidth use -> Efficient discovery of neighbor routers
  OSPF
- Open Shortest Path First
    - Common interior gateway protocol
    - Used within a single autonomous system (AS)
- Well established standard -> Available on routers from many manufacturers
- Link-state protocol
  - Routing based on connectivity between routers -> Each link has "cost"
  - Throughput, reliability, round-trip time
  - Low cost and fastest path wins, identical costs are load balanced
  BGP
- Border Gateway Protocol
    - Exterior gateway protocol -> Connect different autonomous systems (AS)
- The "three-napkins protocol"
    - Sketched out to solve an immediate problem -> Turned into most popular
    - Used around world for Internet Routing

2.1 Routing Technologies

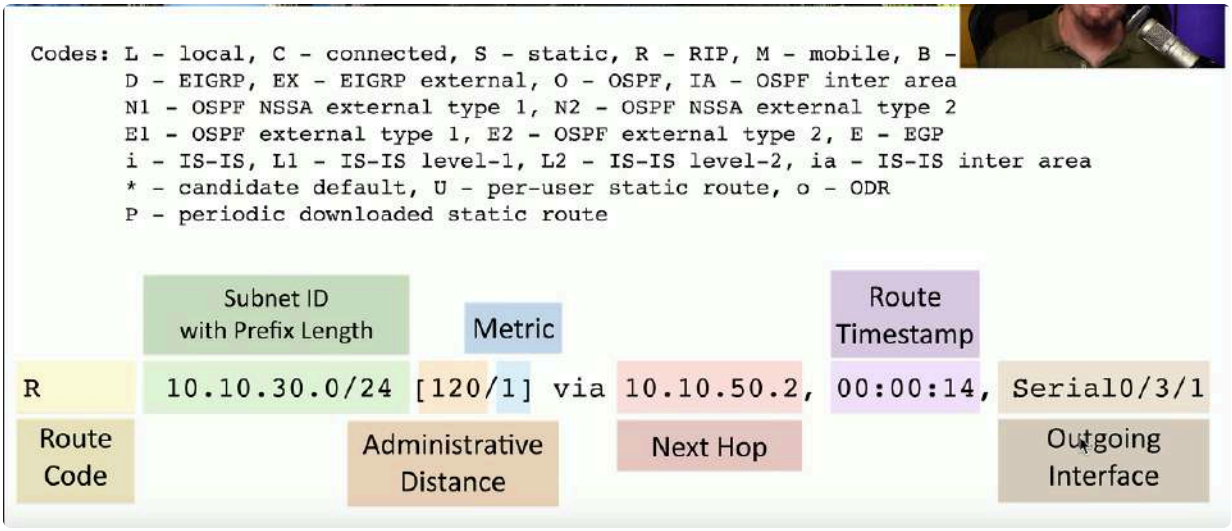
Building A Routing Table

- Routers are digital direction signs
    - How do I get to Google? Go that way.
- Every IP device has a routing table
    - Workstations,servers,routers,etc
- The list of directions is the routing table
    - The most specific route "wins"
- Sometimes there are ties but there are processes to dictate winner
  Routing table with RIPv2



Top Part = Legend || Bottom Part = Routing Table

Route Entries



Prefix Lengths

- Most specific route "wins"
  - Combination of the subnet ID and prefix length
- Routes are more specific as the prefix increases
  - Router forwards traffic to the most specific destination
- Pick the best route to a server with address of 192.168.1.6
- 192.168.0.0/6
- 192.168.1.0/24
- 192.168.1.5/32 <- Correct choice because most specific

Administrative Distances

- Used by router to determine which routing protocol has priority

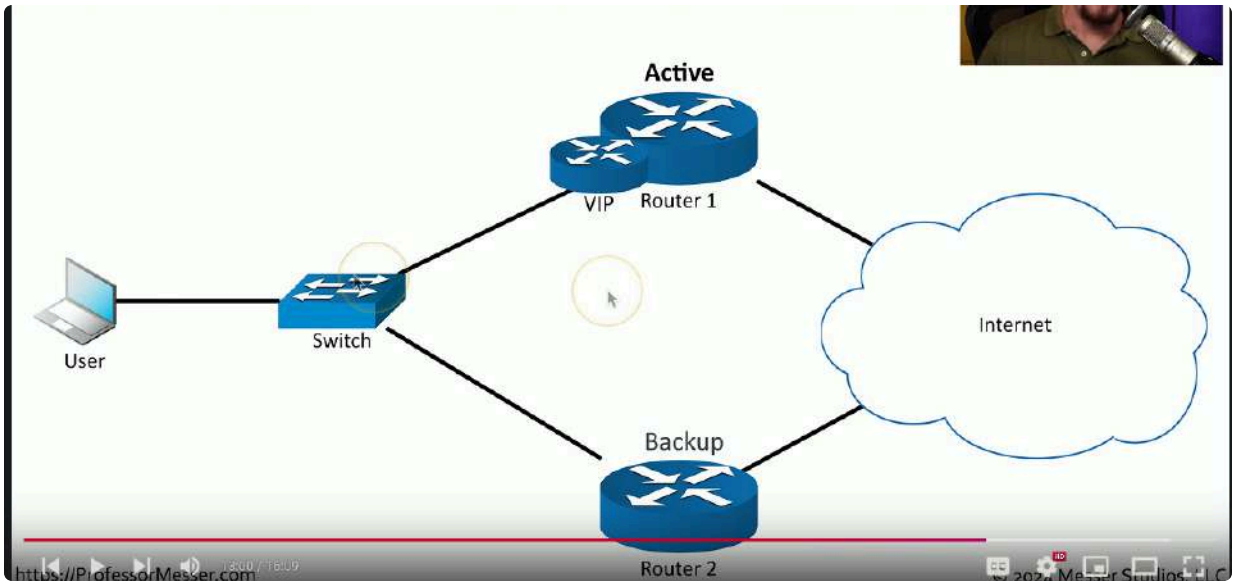
Source	Administrative Distance
Local	0
Static route	1
EIGRP	90
OSPF	110
RIPv1 and RIPv2	120
DHCP default route	254
Unknown	255

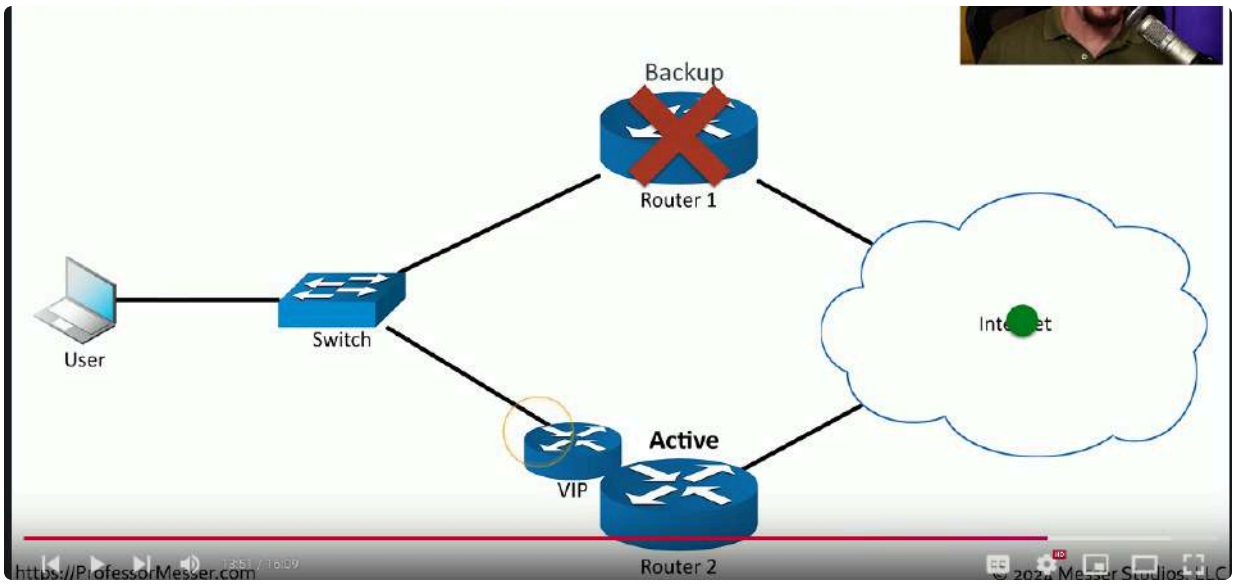
Routing Metrics

- Each routing protocol has its own way of calculating the best route
  - BGP,OSPF,EIGRP
- Metric values are assigned by the routing protocol ->BGP Metric not useful to OSPF or EIGRP
- Use metrics to choose between redundant links -> Choose lowest metric
  - ie. 1 better than 2

First Hop Redundancy Protocol (FHRP)

- Your computer is configured with a single default gateway
  - We need a way to provide uptime if the default gateway fails
- The default router IP address isn't real
  - Devices us a virtual IP(VIP) for the default gateway
  - If router disappears another one takes its place ->Data continues to flow
- Solves a shortcoming with IP addressing
  - One default gateway can really be many different routers



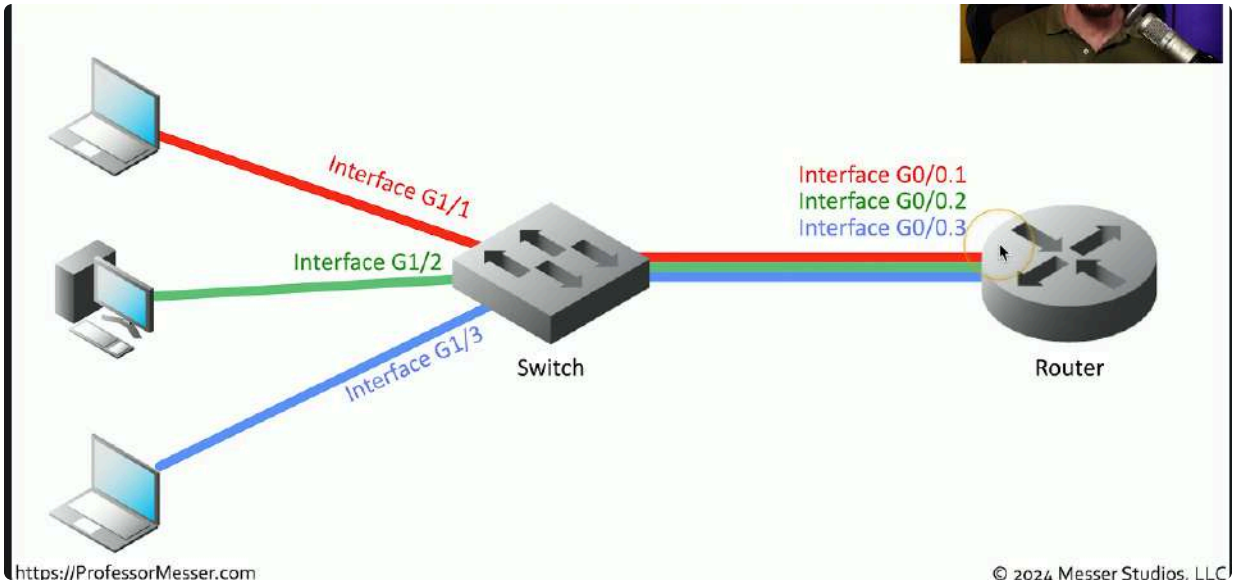


If Active router 1 fails, router 2 takes over VIP and becomes the active one, however user does not know that the router even changed

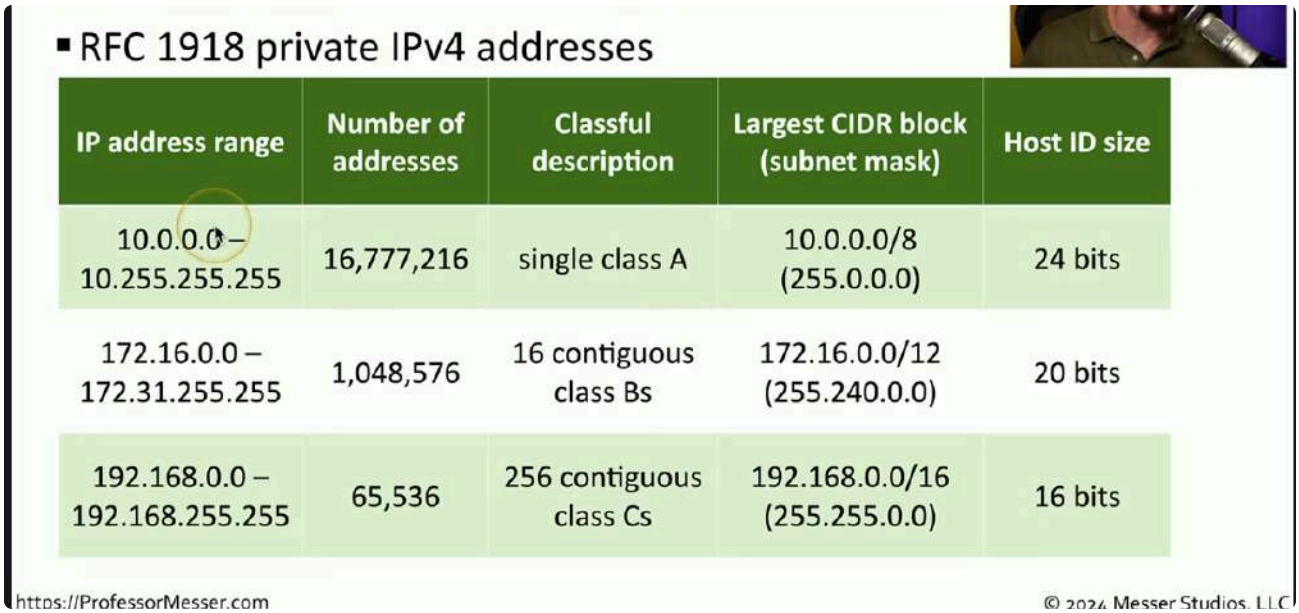
Subinterfaces

- A device has a physical interface ->COnfigure options for each interface
- Some interfaces are not physical
  - VLANS in a trunk
  - These are subinterfaces
- Often referenced with the physical
  - Interface Ethernet1/1
  - Subinterface Ethernet1/1.10
  - Subinterface Ethernet1/1.20

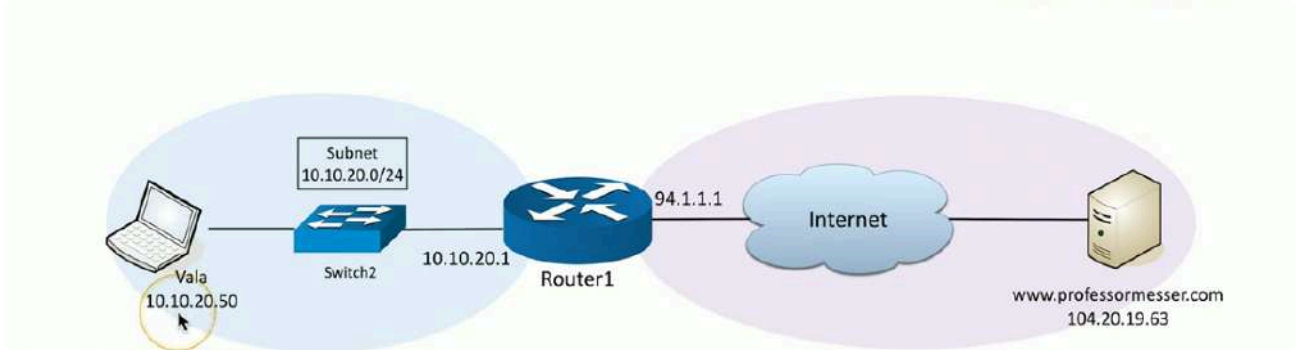
- Subinterface Ethernet 1/1.100



2.1 Network Address Translation



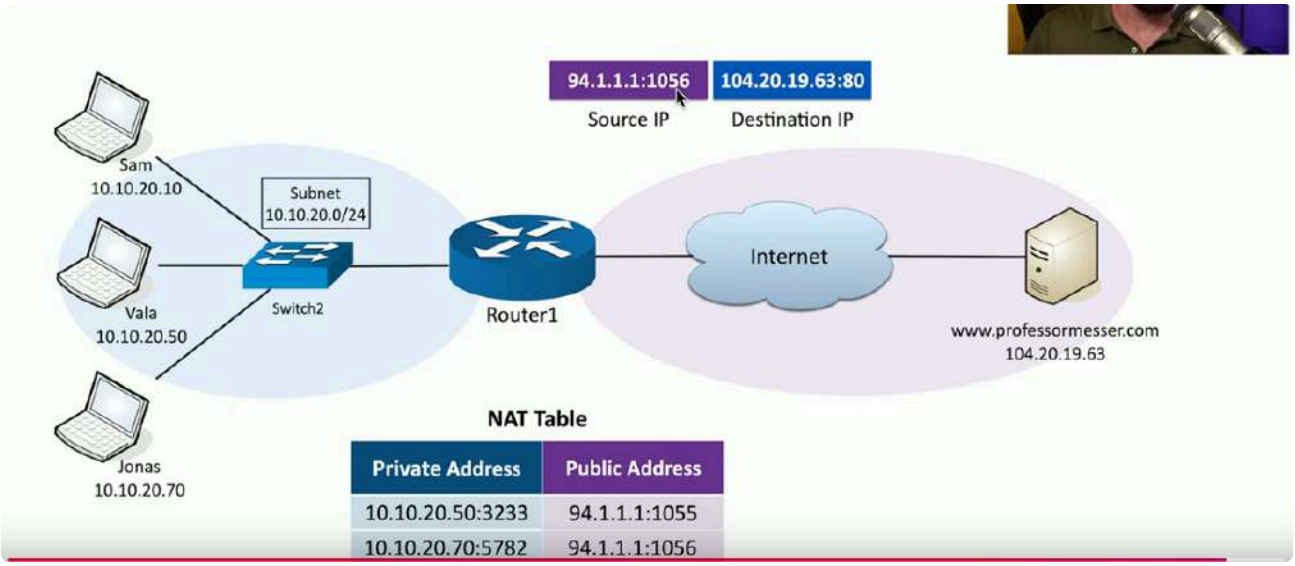
Network Address Translation (NAT)



Private IP goes through switch -> Router Translates Private IP to public before sending over through internet and end destination IP, then the same happens backwards where once sent back Router 1 uses NAT again to translate that public IP back to its private

version.

NAT overload/PAT (Port Address Translation)



By specifying port we can use the same public address given by the Router using NAT

2.2 VLANs And Trunking

LAN's

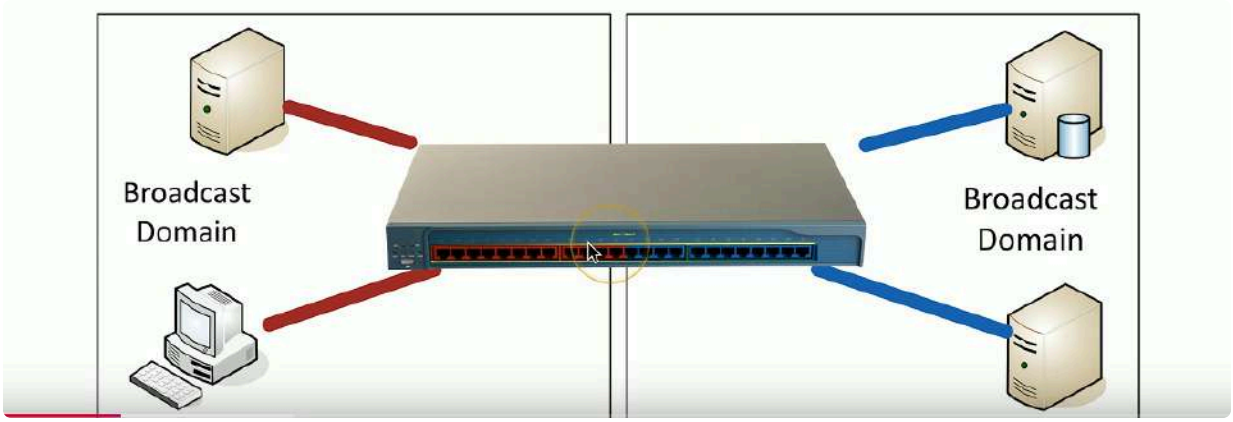
- Local Area Networks
  - A group of devices in the same broadcast domain

All devices connected to the same switch are said to have the same Broadcast Domain

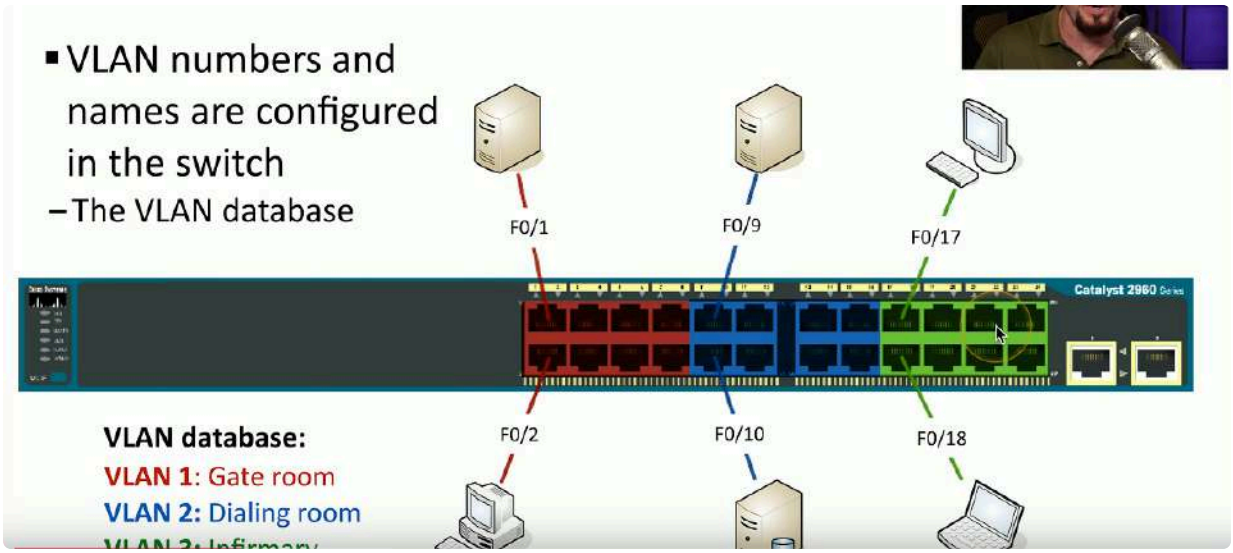
Virtual LAN's

- A group of devices in the same broadcast domain

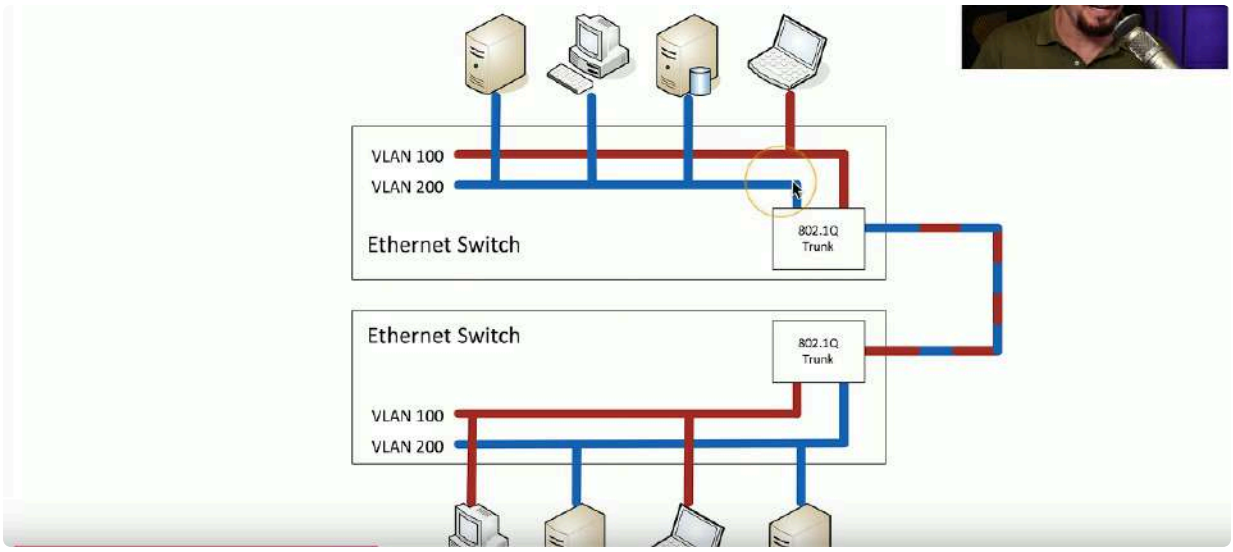
- Separated logically instead of physically



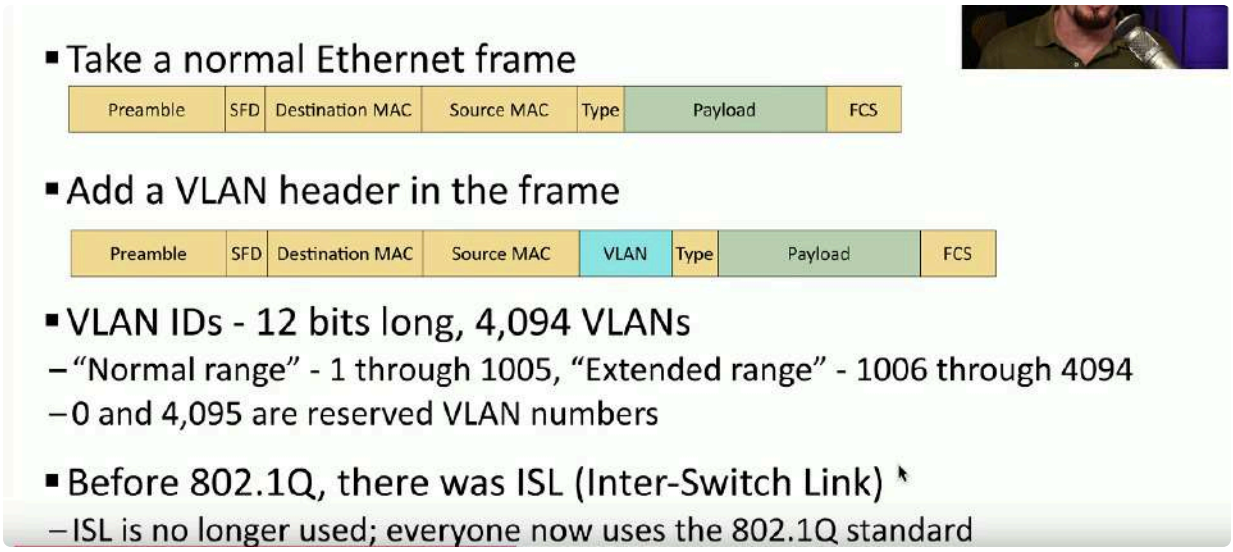
Configuring VLANS



VLAN Trunking



802.1Q Trunking



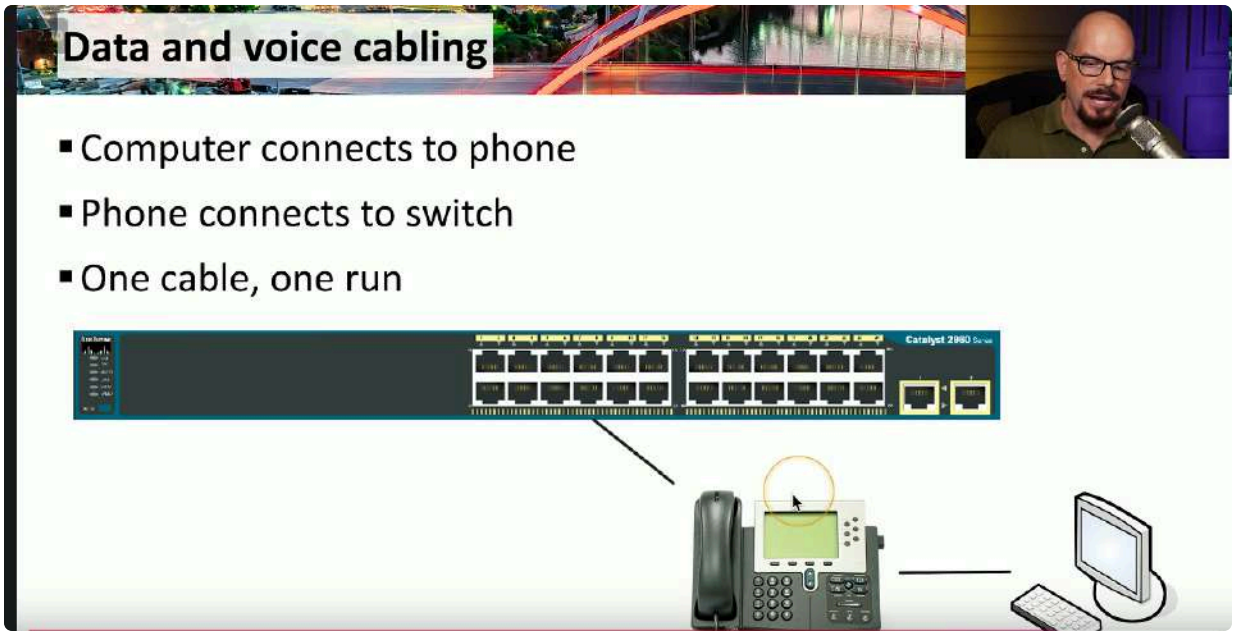
The Native VLAN

- This is different than the "default VLAN"
  - The default VLAN is the VLAN assigned to an interface by default
- Each trunk has a native VLAN -> Native VLAN doesn't add 802.1Q header
- The native VLAN connects switches without a tag
  - Some devices can't talk 802.1Q so we use the native VLAN
- Native VLAN should match between switches->Msg sent if VLAN ID's don't match

Layer 3 Switches

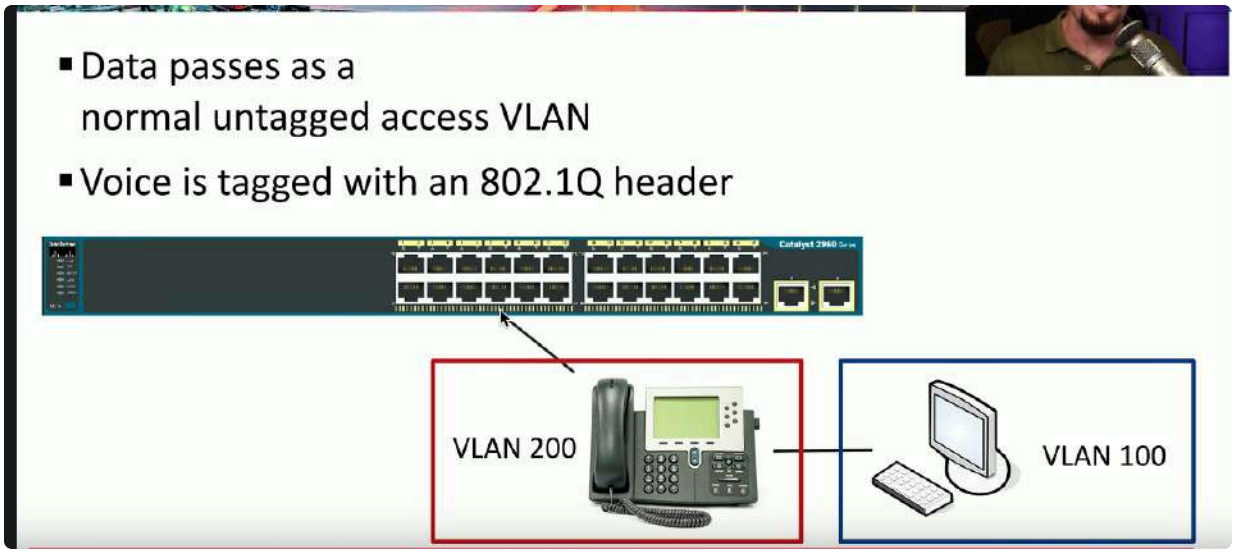
- A switch (Layer 2) and router (Layer 3) in the same physical device
- Switch still operates at OSI layer 2 and routing at OSI layer 3
  - Nothing new or special happening but we are saving space and power
- The internal router connects to the VLAN's over VLAN interfaces
  - Also called switched virtual interfaces (SVI)
- May need to enable routing on your switch
  - Will operate as an L2 device until enabled ->May require a switch restart
- Doesn't replace a standalone router -> Not all designs require extensive routing

- You probably use a layer 3 switch at home



One problem however

- Voice and data don't like each other -> Voice is sensitive to congestion and data loves to congest the network
- Solution: Put the computer on one VLAN and the phone on another
  - Each switch interface has a data VLAN and a voice VLAN
  - Configure each separately

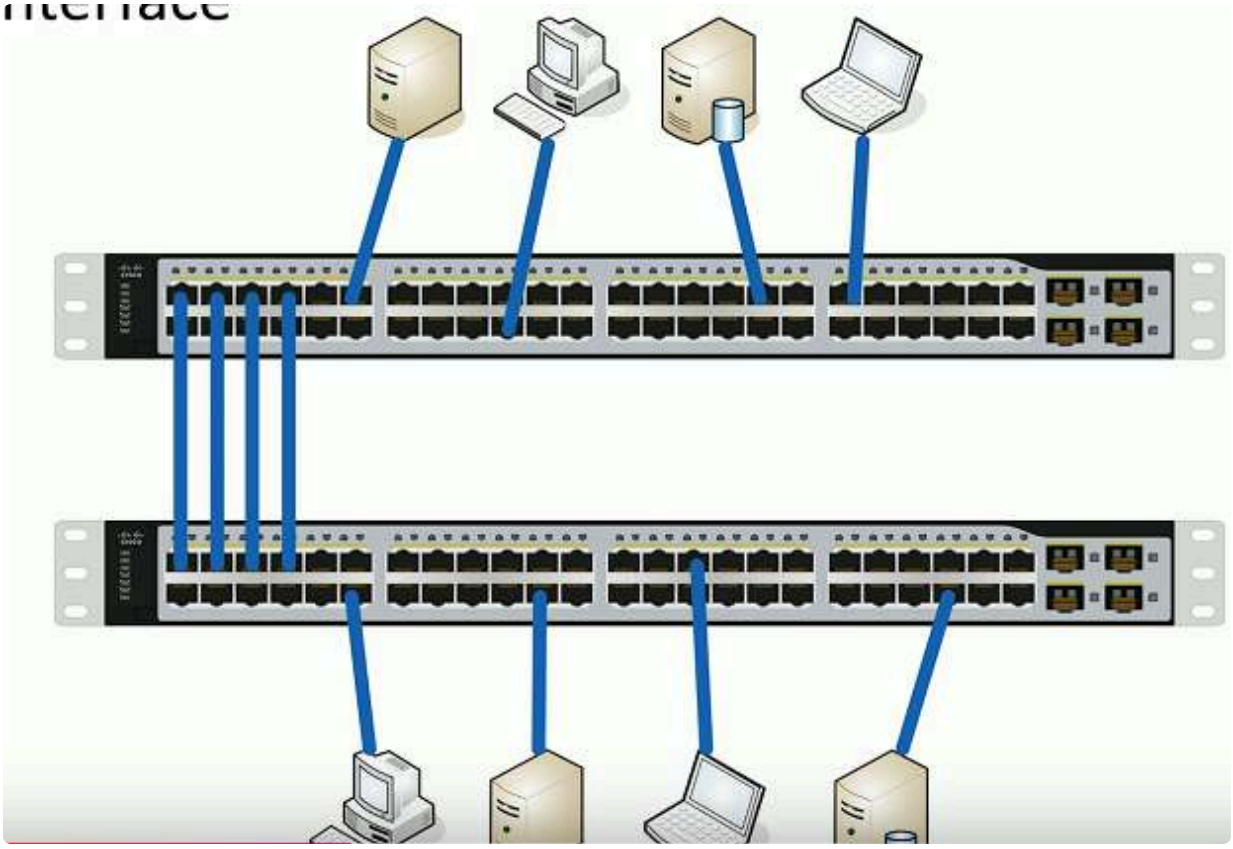


Configure phone to VLAN 200 and computer to VLAN 100 that way switch can distinguish the two

2.2 Interface Configurations

Link Aggregation

- Port Bonding/ Link Aggregation (LAG)
  - Multiple interfaces act like one big interface
  - We can use 4 1GiB Ethernet to now have 4GiB ethernet communication between the two interfaces



LACP

- Link Aggregation Control Protocol ->Adds additional automation and management

Maximum Transmission Unit (MTU)

- Maximum IP packet to transmit -> But not fragment
- Fragmentation slows things down
  - Losing a fragment loses an entire packet -> Requires overhead along path
- Diffult to know the MTU all the way through the path

  - Automated methods often innacurate

  - Especially when ICMP is filtered

Jumbo Frames

- Ethernet frames with more than 1500 bytes of payload
  - Up to 9,216 Bytes of an MTU (9000 is the accepted norm)
- Increases transfer efficiency
  - Per packet size -> Fewer packets to switch/route
- Ethernet devices must support jumbo frames

  - All devices must understand them -> Switches,interface cards etc

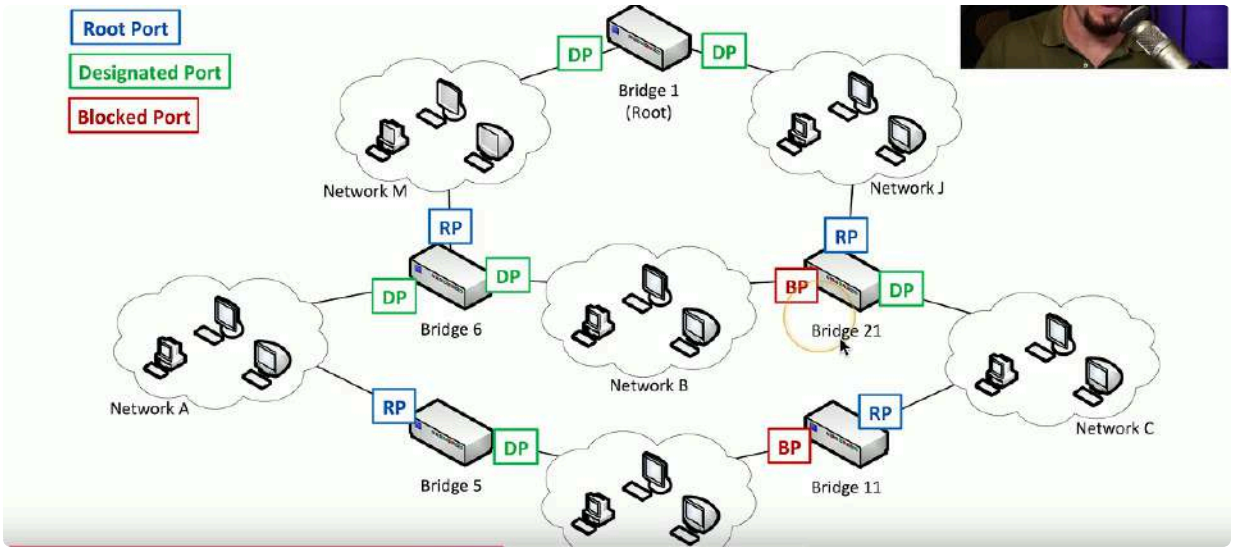
  - Not all devices are compatible with others

2.2 Spanning Tree Protocol

Loop Protection

- Connect two switches to each other

    - Create a loop with two cables ->They'll send traffic back and fort forever
    - There's no "counting" mechanism at the MAC layer
- This is an easy way to bring down a network -> Somewhat difficult to troubleshoot
    - Relatively easy to resolve
- IEEE standard 802.1D to prevent loops in brdiged (switched) networks (1990)
  - Spanning Tree Protocol -> Used practically everywhere
  STP port states
- Blocking -> Not forwarding to prevent a loop
- Listening -> Not forwarding and cleaning the MAC table
- Learning -> Not forwarding and adding to the MAC table
- Forwarding -> Data passes through and is fully operational
- Disabled -> Administrator has turned off the port
  Spanning Tree Protocol Topology



  RSTP (802.1w)
- Rapid Spanning Tree Protocol
    - A much needed update of STP -> This is the latest standard
- Faster convergence -> From 30 to 50 seconds to 6 seconds
- Backwards compatible with 802.1D Spanning Tree Protocol
    - You can mix both in your network
- Still very similar process -> An update not a wholesale change

2.3 Wireless Technologies

IEEE Standards -> Institute of Electrical and Electronics Engineers

- 802.11 Committee
  Wifi Generations:
- 802.11ac ->Wi-Fi 5

- 802.11ax ->Wi-Fi 6 and Wi-Fi 6E (Extended)
- 802.11be ->Wi-Fi 7
  Frequencies -> 2.4GHz, 5GHz, 6GHz ->Sometimes a combination
- Channels
  - Groups of frequencies numbered by the IEEE
  - Using non-overlapping channels would be optimal

- Bandwidth
  - Amount of frequency in use -> 20MHz,40MHz,80MHz,160Mhz...

  Band Selection and Bandwidth

  Band Steering

- Many frequencies to choose from -> Not all are optimal
- Some devices may only use on frequency ->Older devices, specialized systems...
- Other devices may have a choice between 2.4,5 or 6GHz
- Use band steering to direct client to the best frequency
  - 2.4GHz and 5GHz without band steering = strongest frequency

- 2.4GHz and 5GHz with band steering = 5GHz connection
- Without band steering strongest frequency doesn't always guarantee strongest throughput

Regulatory Impacts

- Managing the wireless spectrum is a challenge
  - Individuals, companies, organizations countries all have different regulations/preferences
- Industry standards are also often worldwide standards ->We all have to work together
- IEEE 802.11h standard->Add interoperability features to 802.11

The 802.11h standard

- Complies with ITU Guidelines ->Worldwide approach and part of the 802.11 standard
- DFS (Dynamic Frequency Selection)
  - Avoid frequency conflict
  - Access point can switch to an unused frequency
  - Clients move with the access point
- TPC (Transmit Power Control)
  - Avoid conflict with satellite services
  - Access point determines power output of the client

2.3 Wireless Networking

Independent basis service set (IBSS)

- Two deives communicate directly to each other using 802.11
  - No access point required
- Ad hoc -> Created for a particular purpose without any previous planning
  - Without an AP (Access point)
- Temporary or long-term communication
  - Connect to a device with an ad hoc connection
  - Configure it with the access point settings and credentials

SSID and BSSID

- Every wireless networks needs a name
  - SSID (Service Set Identifier)
- There might be multiple access points supporting an SSID
  - How does your computer tell them apart?
  - The hardware address of an access point is a BSSID (Basic Service Set Identifier)
  - The Mac (Media Access Control) address

Extending The Network

- Most orgs have more than one access point -> Tens or hundreds

- Wireless network names can be used across access points
  - Makes it easier to roam from one part of the network to another
- The network name shared across access points is an ESSID
  - Extended Service Set Identifier
- Your device automatically roams when moving between access points
  - Don't have to manually reconnect

  Captive Portal
- Authentication to a network
  - Common on wireless networks
- Access table recognizes a lack of authentication
  - Redirect your web access to a captive portal page
- Username/password ->And additional authentication factors
- Once proper auth is provided web session continues->Until captive portal removes your access

  Wireless Security Modes
- Open system -> No authentication password is required
- WPA/2/3-Personal /WPA/2/3-PSK
  - WPA2 or WPA3 with a pre-shared key
  - Everyone uses the same 256-bit key
- WPA/2/3-Enterprise / WPA/2/3-802.1X
  - Authenticates users individually with an authentication server
  - Ex: RADIUS, LDAP, etc..

  Omnidirectional antennas
- One of the most common->Included on most access points
- Signal evenly distributed on all sides -> Omni = all
- Good choice for most environments -> Need coverage in all directions
- No ability to focus the signal -> Different antenna would be required

  Directional antennas
- Focus the signal -> Increased distances
- Send and receive in a single direction
  - Focused transmision and listening
- Antenna performance is measured in dB
  - Double power every 3dB of gain
- Yagi Antenna (Type of Directional Antenna)
  - Very directional and high grain

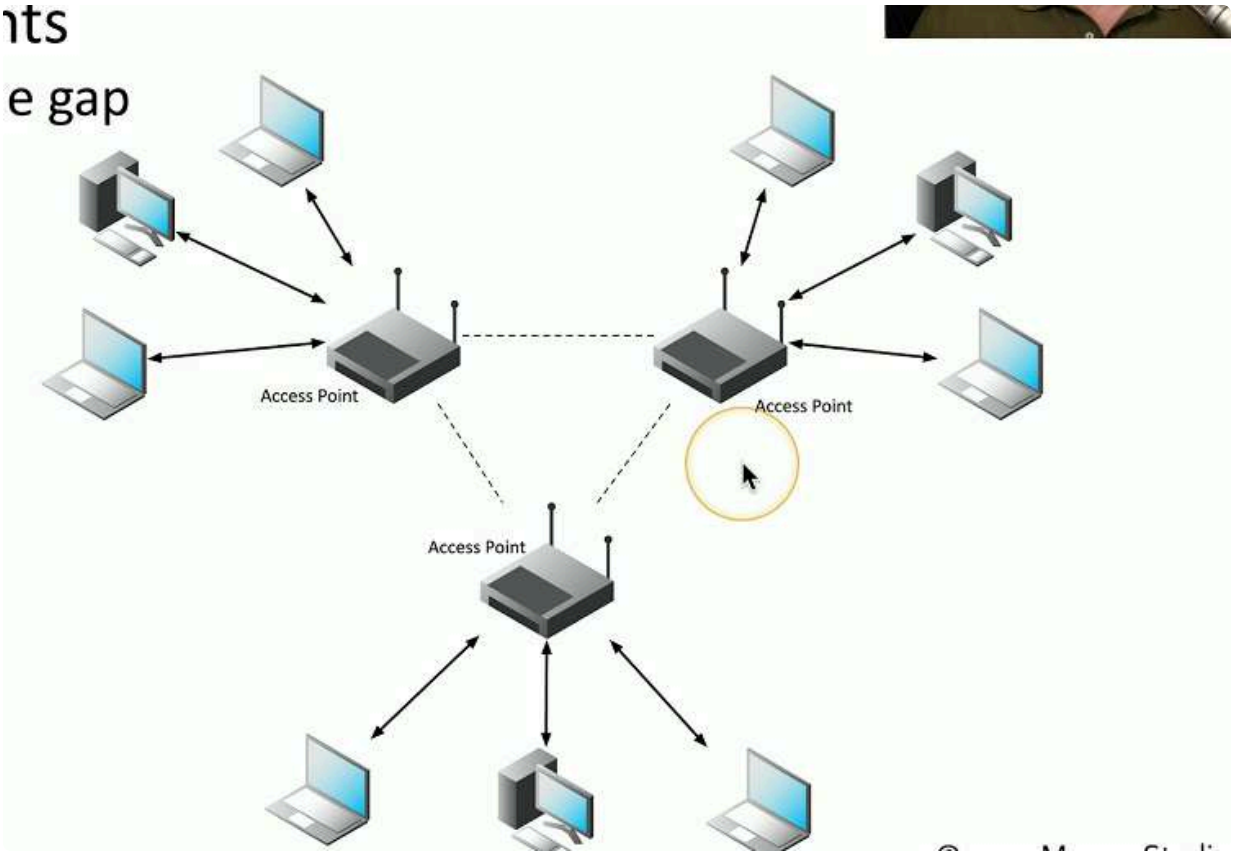
- Parabolic Antenna (Type of Directional Antenna)
  - Focus signal to a single point
  - 
  Managing Wireless Configurations
- Autonomous access points
  - Access point handles more wireless tasks
  - The switch is not wireless-aware
- Lightweight access points
  - Just enough to be 802.11 wireless
  - Less intelligence is in the switch
  - Also less expensive
- Control and Provision
  - CAPWAP is an RFC standard
  - Control and Provisioning of Wireless Access Points (CAPWAP)
  - Manage multiple access points simultaneously

  Wireless LAN controller
- Centralized management of access points
- Deploy new access points -> Configure and deploy changes to all sites
- Conduct performance and security monitoring -> Report on access point use
- Usually a proprietary system -> Wireless controller paired with access points

2.3 Network Types

Wireless Mesh

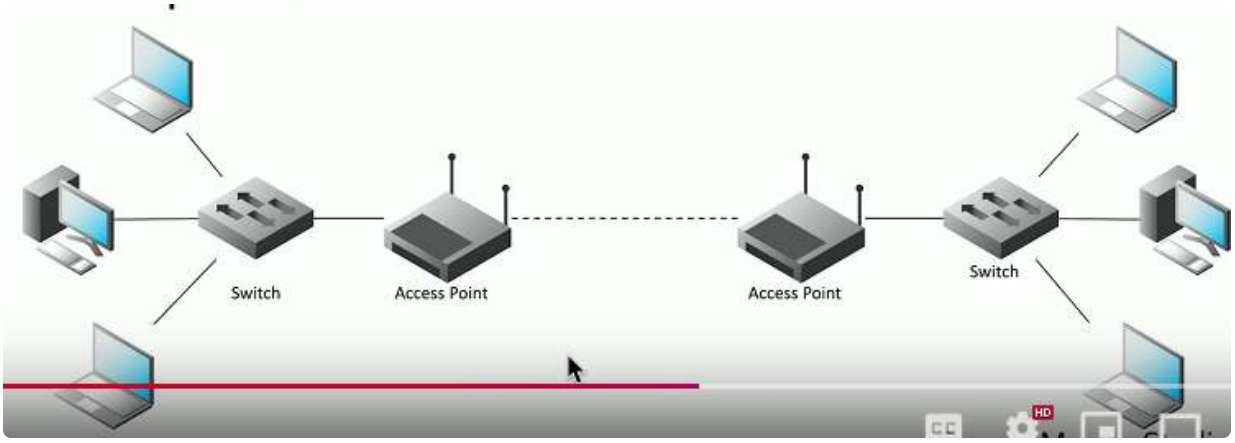
- Multiple access points
  - Access points bridge the gap
  - Clients across an extended distance can communicate with each other



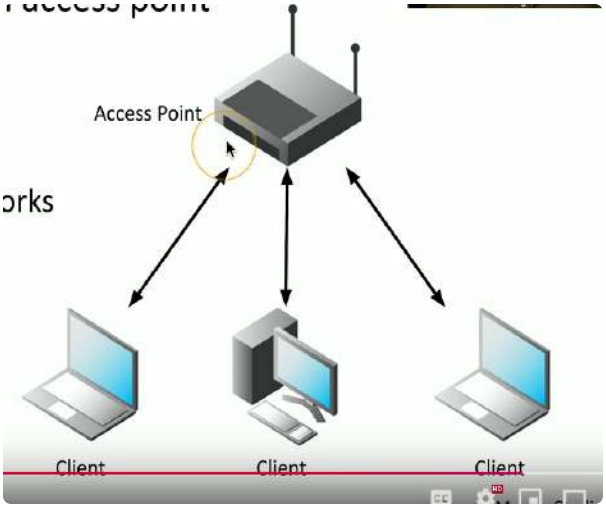
- Ad hoc devices work together to form a mesh "cloud"
  - Self form and self heal

  Ad Hoc Mode
- Created for a particular purpose without previous planning
- Without an AP
- Two devices communicate directly using 802.11
- No AP required -> Independent basic service set (IBSS)

  Point to point Mode
- Connect two access points together
  - Extend wired network over a distance
    - Building to building, site to site
- May require specialized wireless equipment
  - Outdoor antennas and access points
  - Power adjustments
  - Frequency options



Infrastructure Mode

- Clients communicate to an access point
  - Access point forwards traffic
- Clients can communicate to a wired network
  - Access point bridges the networks
- Clients can communicate to each other->If access point allows
- 

2.3 Wireless Encryption

Securing A wireless Network

- An organization's wireless network can contain confidential information
  - Not everyone is allowed access
- Authenticate users before granting access
  - Username, pass, MFA
- Ensure that all communication is confidential ->Encrypt the wireless data
- Verify the integrity of all communication
  - Received data should be identical to original sent data
  - A message integrity check (MIC)

  WPA (Wi-Fi Protected Access)

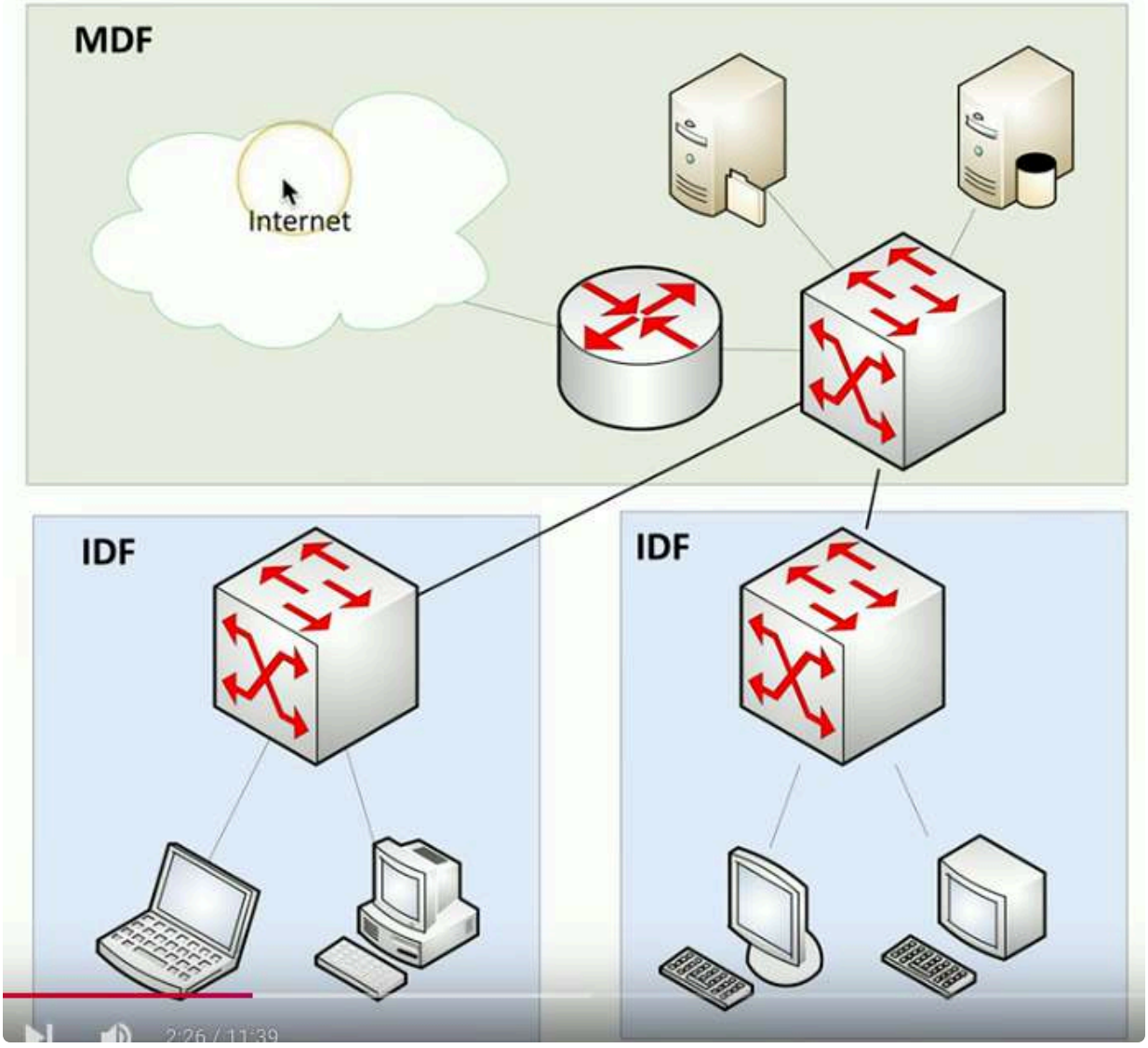
- 2002: WPA was the replacement for a serious cryptographic weakness in WEP
  - Don't use WEP (Wired Equivalent Privacy)
- Needed a short term bridge between WEP and whatever should be the successor -> Had to run on current hardware
  WPA2 and CCMP
- WiFi Protected Access II (WPA2)
  - WPA2 certification began in 2004
- CCMP Block Cipher Mode
  - Counter Mode with Ciper Block Chain Message Authentication Code Protocol
    - Or Counter/CBC-MAC Protocol
- CCMP security services
  - Data confidentiality with AES encryption
  - Message Integrity Check (MIC) with CBC-MAC Protocol
  WPA3 and GCMP
- WiFi Protected Access 3(WPA3)
  - Introduced in 2018
- GCMP Block Cipher Mode
  - Galois/Counter Mode Protocol ->Stronger encryption than WPA2
- GCMP security services
  - Data confidentiality with AES encryption
  - Message Integrity Check (MIC) with Galois Message Authentication Code(GMAC)

2.4 Installing Networks

Distribution Frames

- Passive Cable termination
  - Punch down blocks, Patch Panels
  - 
- Usually mounted on the wall or flat surface -> Uses a bit of real-estate
- All transport media -> Copper,fiber,voice and data

- Often used as room or location name -> Significant part of the network
  Main Distribution Frame (MDF)
- Central point of the network -> Usually in a data center
- Termination point for WAN links -> Connects inside to the outside
- Good test point -> Test in both directions
- Often the data center -> Central point for data
- Example MDF:
- 
  Intermediate Distribution Frame (IDF)
- Extension of the MDF -> Strategic Distribution Point, often in different building
- Connects the users to network
  - Uplinks from the MDF, Workgroup switches, Other local resources
- Common in medium to large organizations ->Users are geographically diverse
- Ex Of MDF and IDF Working Together

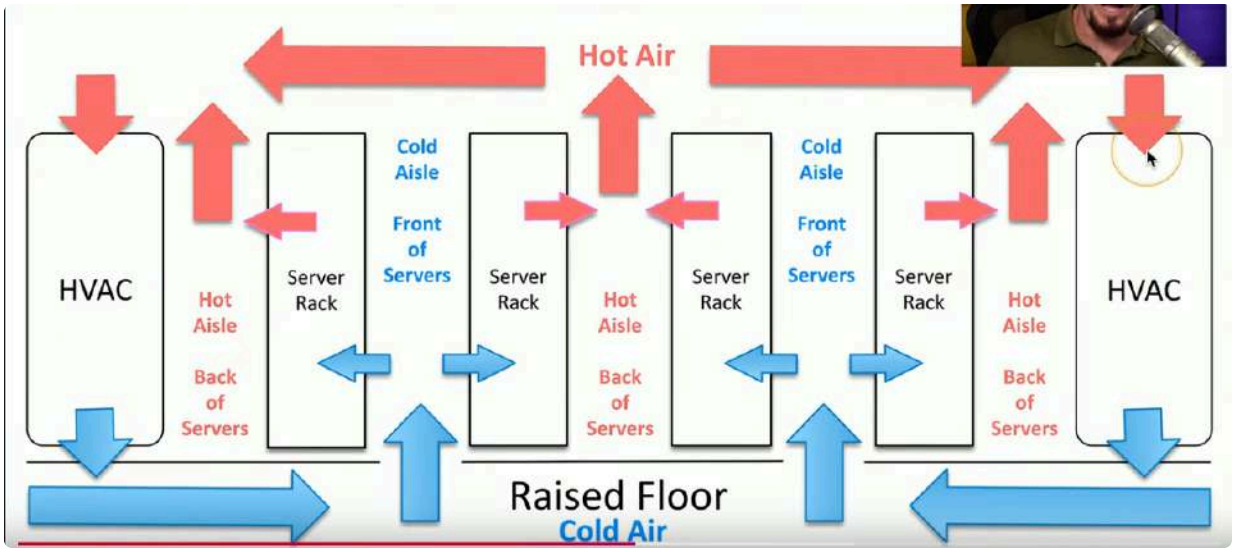


- Equipment Racks
- Rack sizes ->19" rack/device width
- Height measured in rack units -> 1U is 1.75" (Inches)
- Common rack height is 42U (42*1.75") = total height in inches
- Depth can vary -> Often determined by equipment
- Plan and locate ->Devices follow standard sizing

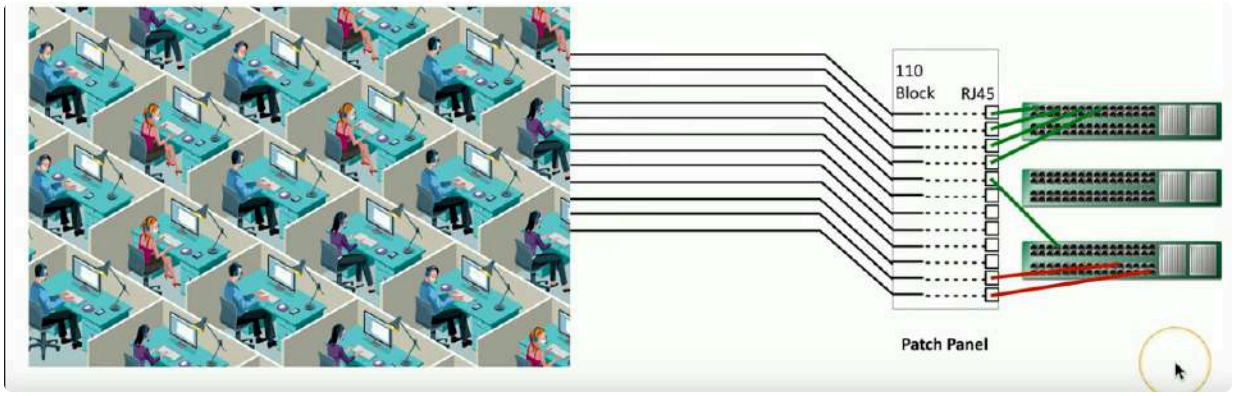
Cooling a Data Center

- Heating, Ventilating and Air Conditioning (HVAC System)
  - Thermodynamics, fluid mechanics and heat transfer
- A complex science-> Not something you can properly design yourself
- Must be integrated into the fire system
- Data Centers Optimize Cooling -> Separate aisles for heating and cooling
- Heat intake and exhaust is important ->Front back or side

- Ex HVAC System



Cable Infrastructure



Copper Patch Panel/Patch Bay

- Punch-down block on one side->RJ45 Connector on the other

- Ex of Copper Patch Panel in an IDF

- Move a connection around ->Different Switch interfaces
- The run to the desk (Office desk for user) doesn't move
- We only need to change the internal connections in our IDF to make changes
  Fiber Distribution Pnale
- Permanent fiber installation -> Patch panel at both ends
- Can't Exceed Fiber bend radius ->Breaks when bent too tightly
- Often includes a service loop ->Extra fiber for future changes

  Locking Cabinets
- Data center hardware is usually managed by different groups

    - Responsibility lies with the owner
- Racks can be installed together -> Side to side
- Enclosed cabinets with locks ->Ventilation on front back top and bottom

2.4 Power

Amp and Volt

- Ampere (amp, A) -> The rate of electron flow past a point in one second
    - The diameter of the hose->Water flow in hose used as analogy for Amp
- Voltage (volt,V) -> Electrical "pressure" pushing the electrong
    - How open the faucet is
    - 120 volts, 240 volts
- Watt (W) -> How much energy is being consumed?
    - Electrical load is measured in watts
    - Watts = Volts * Amps
    - Ex: 120V * 0.5A = 60W
- Current
  - Alternating Current (AC)
  - Direction of current constantly reverses
  - Distributes the electricity efficiently over long distances
  - Frequency of this cycle is important
  - US/Canada =>110-120 Volts of AC (VAC), 60 hertz (Hz)
  - Europe =>220-240 VAC, 50 Hz
  - Direct Current (DC)
  - Current moves in one direction with a constant voltage

  Device Power Supplies
- Devices commonly use DC voltage
    - Most power sources provide AC voltage
- Convert 120V AC or 240V AC to DC Voltages

  UPS (Unninterruptible Power Supply)

- Short term backup power
- Protects from blackouts,brownouts,surges
- Common UPS Types
  - Offline/Standby UPS
  - Line-interactive UPS
  - On-line/Double-conversion UPS
- Features
  - Auto shutdown, battery capacity, outlets, phonel ine suppresion

  PDU's (Power Distribution Units)
- Provide multiple power outlets ->Usually in a rack
- Often include monitoring and control
  - Manage power capacity, enable or disable individual outlets

2.4 Environmental Factors

Humidity

- We use a lot of power for data centers ->Approx 2% of all US power consumption
- Humidity level
  - High humidity promotes condensation
  - Low humidity promotes static discharge
- Industry guidelines for data centers
  - Somewhere around 40%-60% humidity
  - Specific settings vary on location and equipment type

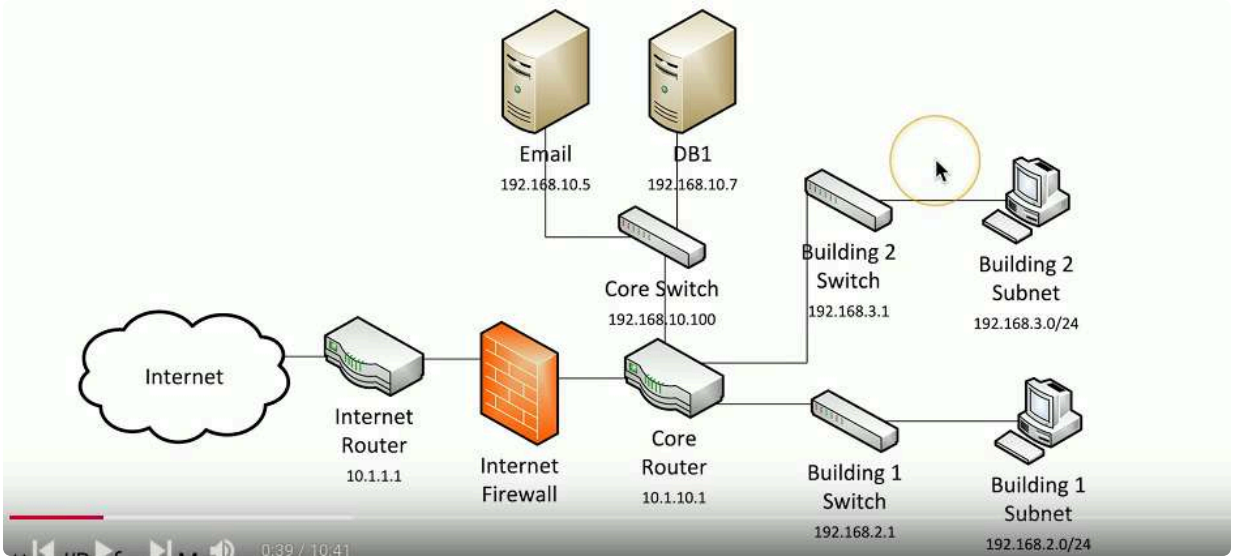
  Temperature
- Electrical equipment has an optimal operating temperature
  - Often part of device specifications
  - Industry best practices are around 64 to 81 Fahrenheit
- Many external influences ->Outdoor temp, System load
- HVAC used to manage temp and humidity->Sensors placed in strategic locations

  Fire Supression
- Data Center Fire Safety
  - Large area, lots of electronics
  - Water isn't the best fire suppression option
- Common to use inert gases and chemical agents
  - Stored in tanks and dispersed during a fire->Many warning signs
- Integrated into HVAC system
  - Monitor for carbon monoxide, Enable/Disable air handlers

3.1 Network Documentation

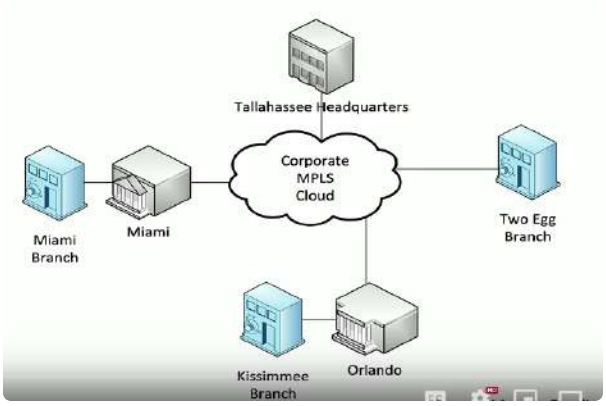
Physical Network Maps

- Follows the physical wire and device ->Can include physical rack locations



Logical Network Maps

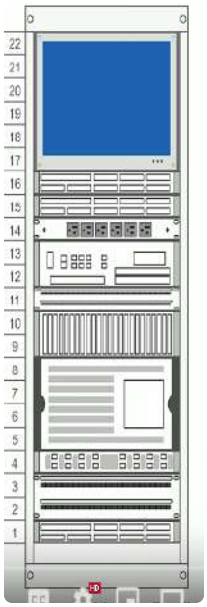
- Specialized software -> Visio, OmniGraffle, Gliffy.com
- High level views -> WAN layout, application flows
- Useful for planning and collaboration



Rack Diagrams

- A network admin might never walk into the data center
  - Physical access often limited
- Provide documentation for installation or changes
  - A picture is worth a thousand words
- Detailed diagram of rack components
  - Often listed by physical location of the rack (row 3, rack W)
  - Each rack unit (U) is documented

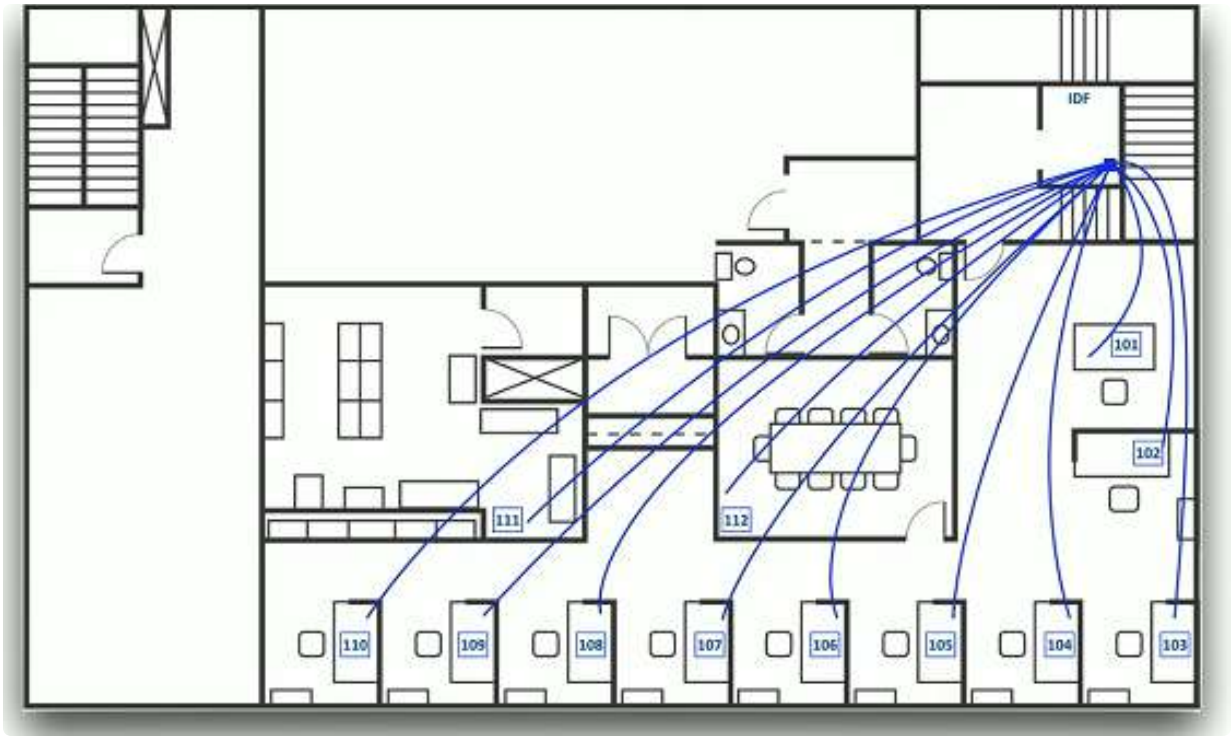
  Ex Rack Diagram



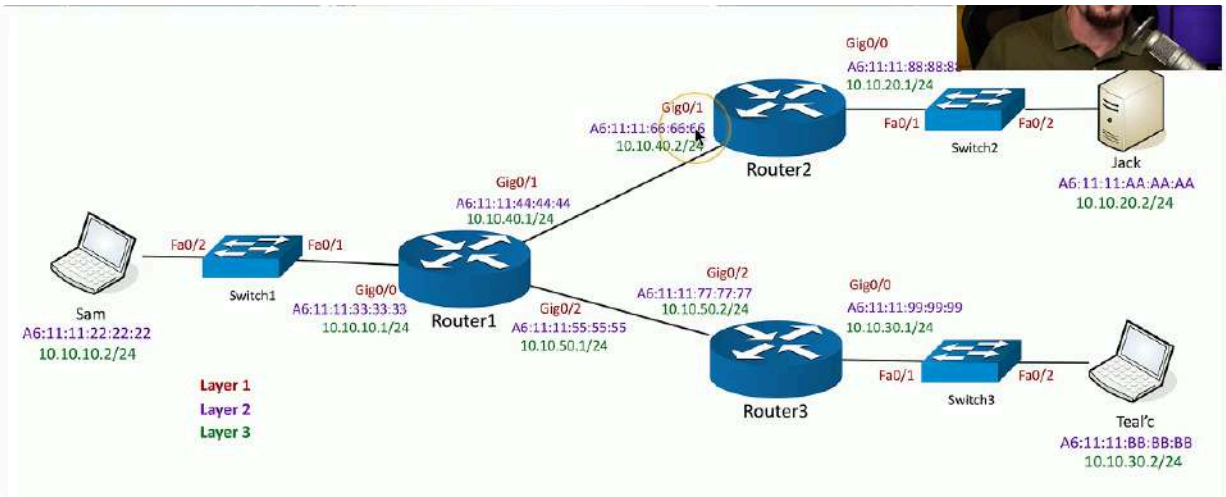
Cable maps and diagrams

- The foundation of the network
  - Physical cable and fiber
- Valuable documentation

  - Planning installation, numbering each network drop, troubleshooting after installation



Network Diagrams



Each Layer Overlay gives different additional info:

- Layer 1->Provides with switches and interfaces
- Layer 2->Overlay MAC addresses
- Layer 3->Overlay IP addresses

Asset Management

- A record of every asset
  - Laptops,desktops,servers,routers,switches...
- Associate support tickets with a device make and model
  - Record of hardware and software
- Financial record, audits, depreciation
- Add an asset tag ->Barcode,RFID, Visible tracking number,Organization Name

Asset Database

- A central asset tracking system

  - Used by different parts of the organization

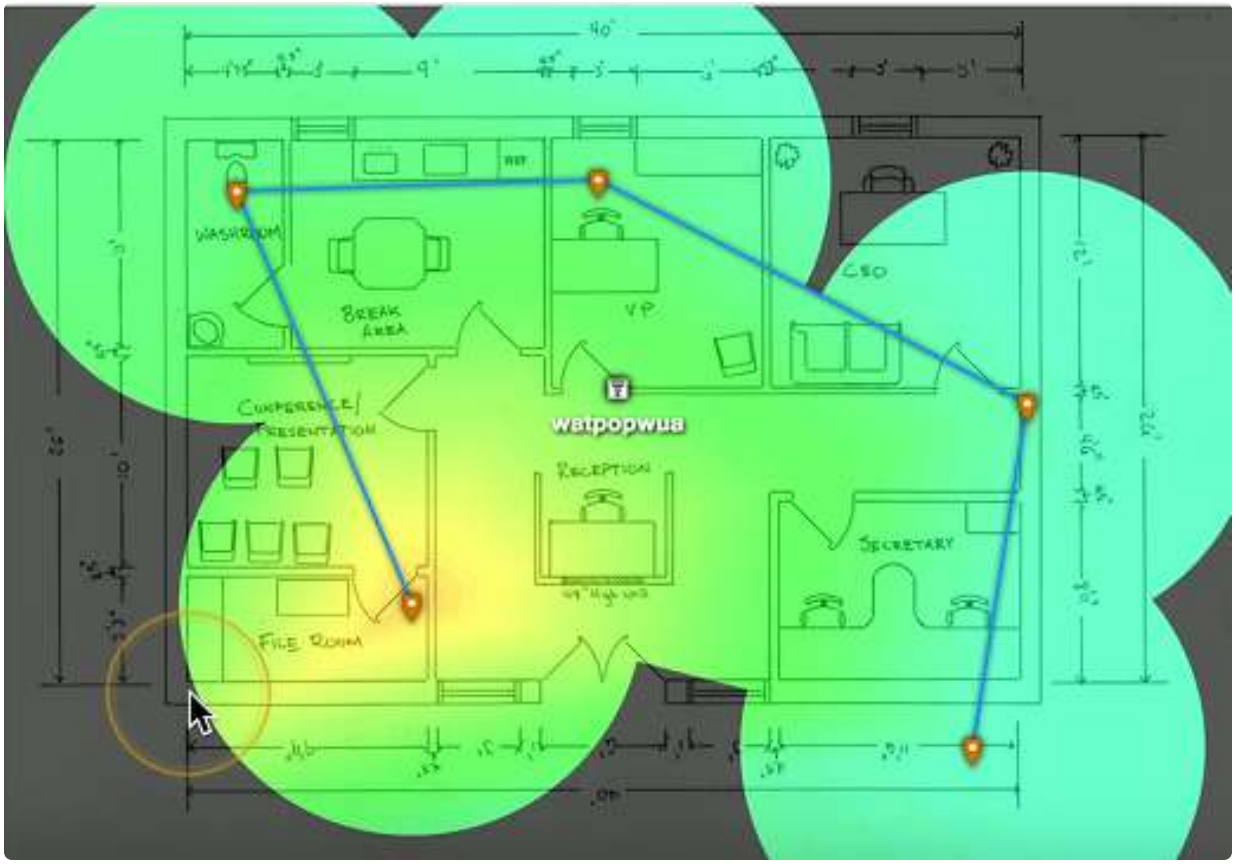
  IPAM (IP Address Management)

- Manage IP addressing ->Plan,track, configure DHCP
- Report on IP address usage ->Time of day, user-to-IP mapping
- Control DHCP reservations -> Identify problems and shortages
- Manage IPv4 and IPv6 -> From one central console

Service Level Agreement (SLA)

- Minimum terms for services provided
- Uptime, response time agreement, etc
- Commonly used between customers and service providers

- Contract with Internet Provider
  Site Surveys
- Determine existing wireless landscape
  - Sample existing wireless spectrum
- Identify existing access points
  - You may not control all of them
- Work around existing frequencies, layout and plan for interference
- Plan for ongoing site surveys -> Things will certainly change
- Use heat maps to identify wireless signal strengths



3.1 Life Cycle Management

End-of-life (EOL)

- Manufacture stops supporting hardware
- May continue to provide security patches and updates
- May provide warranty repair
  End-of-support (EOS)
- Manufactures stops updating a product
- Current version is final version
- No ongoing security patches or udpates
  Firmware management

- Software inside of the hardware
  - The OS of the hardware device
- The potential exists for security vulnerabilities
  - Upgrade firmware to non-vulnerable version
- Plan for unexpected ->Always have rollback plan -> Save those firmware binaries
  Decommissioning
- Managing asset disposal -> Desktops,laptops etc ->Sanitize media or destroy
- May be a legal issue ->Some info must not be destroyed
  - Consider offsite storage
  Change Managaement
- Upgrade software, change firewall configuration, modify switch ports
- One of most commons risks in the enterprise
  - Occurs frequently -> Often overlooked or ignored
- Have clear policies->Frequency,duration,installation process,fallback procedures
  Request Process Tracking
- Best way to manage service requests
  - Document,assign,resolve,report
- Usually responsibility of help desk ->Take calls, triage, determine next best step, assign ticket and monitor

3.1 Configuration Management

- Only constant is change
  - Operating systems, patches, application updates, network modifications etc.
- Identify and document hardware and software settings
  - Manage the security when changes occur
  Production Configuration
- The most current running config -> Everyone uses this config
- Covers all aspects of the configuration
  - Hardware devices and firmware version
  - Device driver version, Application software updates
  Backup Configuration
- There always needs to be a backup
- Create backup before making a change ->Revert if problems occur
  - Copy files, create snapshot of a VM, etc.
  Baseline/Golden configuration
- An application environment should be well defined
  - All app instances must follow this baseline

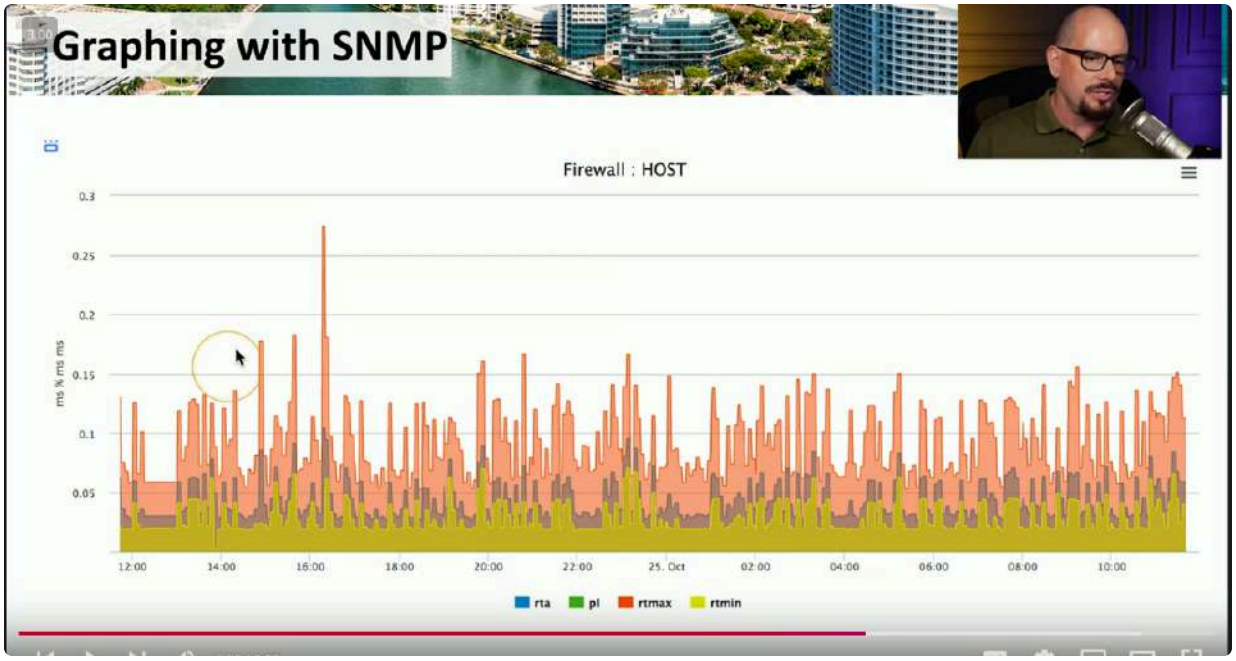
    - Firewall settings, patch levels, OS file versions
    - May require constant updates
- Integrity measurements check for the secure baseline
    - Should be performed often -> Check against well-documented baselines
    - Failure require an immediate correction

3.2 SNMP

Simple Network Management Protocol

- A database of data (MIB) - Management Information Base
- Database contains OID's - Object Identifiers -> We can query the SNMP for info with these
- Poll devices over udp/161
- SNMP v3 -> The new standard -> Message integrity, authentication, encryption
  SNMP OID's
- An object identifier can be referenced by name or number
  - .iso(1).org(3).dod(6).internet(1).....

  – .iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).snmp(11).snmpOutGetResponses(28).0
  – .1.3.6.1.2.1.11.28.0
- Every variable in the MIB has a corresponding OID
    - Some are common across devices
    - Some manufacturers define their own OID's
- The SNMP manager requests information based on OID
- A Consistent reference across devices



SNMP Traps

- Most SNMP operations expect a poll
  - Devices then respond to the SNMP request ->This requires constant polling
- SNMP traps can be configured on the monitored device
- Communicates over udp/162
- Set a threshold for alerts
  - If number of CRC errors increases by 5, send a trap
  - Monitoring station can react immediately

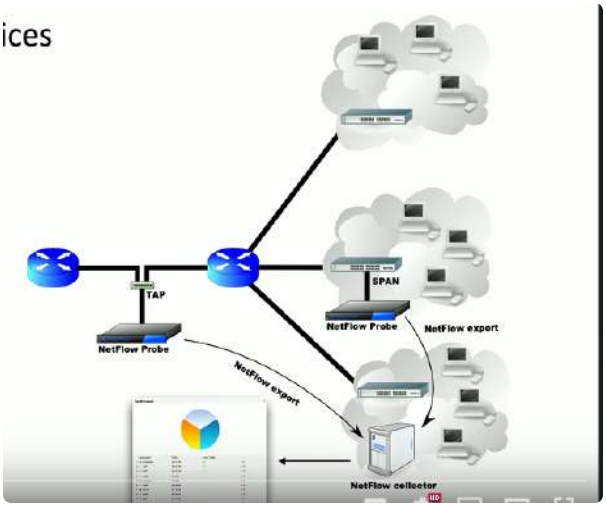
Authentication

- Community String
  - Simple password-style authentication method
  - Read-only,read-write and trap
  - Common community strings are public and private
  - Used with SNMP v1 and SNMP v2c
- Username and password
  - Used in SNMP v3 -> Transmitted as a password hash

3.2 Logs and Monitoring

Flow Data

- Gather traffic statistics from all traffic flows
  - Shared communication between devices

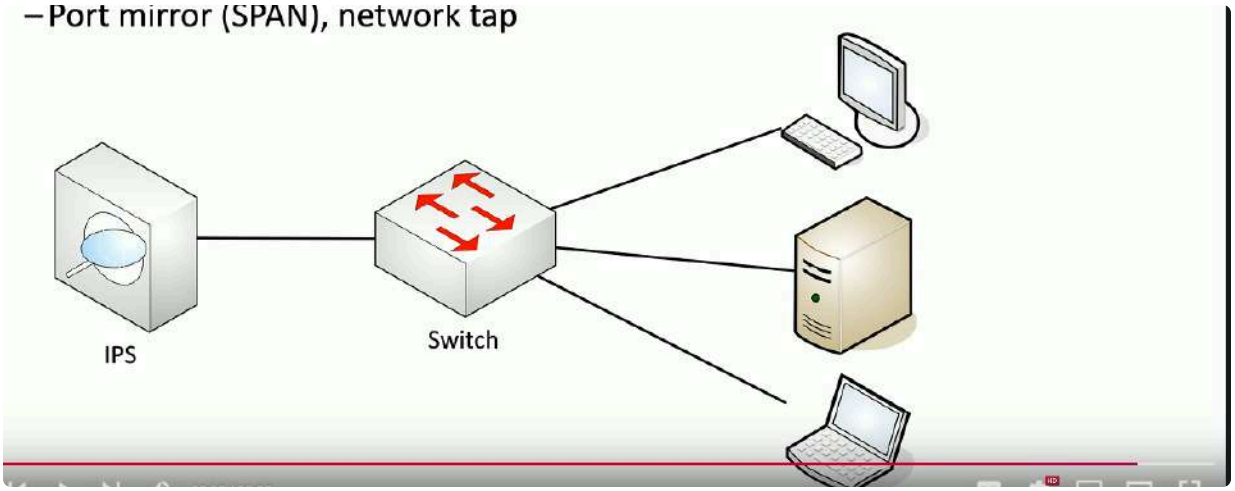


- NetFlow ->Standard collection method ->Many products and options
- Probe and collector
  - Probe watches network communication
  - Summary records are sent to the collector

- Usually a separate reporting app
  - Closely tied to the collector
  Protocol analysers
- Solve complex application issues
  - Get into the details
- Gathers frames on the network (or in the air)
  - Sometimes built into the device
- View traffic patterns
  - Identify unknown traffic ->Verify packet filtering and security controls
- Large scale storage -> Big data analytics
  Network performance Baseline
- Troubleshooting starts with a blank slate ->Baseline can add context
- Some organizations already collect this date
  - Check SIEM or management console
- Alarm and alert when anomalies occur
  Syslog
- Standard for message loging
  - Diverse systems create a consolidated log
- Usually a central logging collector ->Integrated into the SIEM
- Each log entry is labeled
  - Facility code(program that created the log) and severity level
- Common with most devices->Firewalls,switchers,routers,servers,etc..
  Getting The Data
- Sensors and logs
  - Data is sent to SIEM using syslog
  - Operating systems
  - Infrastructure devices
  - NetFlow sensors
- Sensitivity settings
  - Easy to be overwhelmed with data
  - Some info is unnecessary ->Filter for urgent or critical data or alerts
  API Integration
- Control and manage devices
- Hundreds of firewalls, routers, switches and servers
  - Log into each device and make changes manually
- Automate the command line -> Batch processes
  - Very little control or error handling

- API's (Application programming interfaces)
  - Interact with third party devices and services
  - Cloud services, firewalls, operating systems
  - Talk their language

  Port Mirroring
- Copy traffic from one or more interfaces
  - Used for packet captures, IDS , performance monitoring
  - Mirror traffic on the same switch
- Also referred to as a SPAN, network tap



3.2 Network Solutions

- Difficult to see beyond the wall jack, we can use services like
  - LLDP (Link Layer Discovery Protocol)
  - CDP (Cisco Discovery Protocol) , etc..
  - IP Scanners (Nmap)
  - Commercial network scanners
  - SNMP
- Ad Hoc -> Scan network as needed or required for troubleshooting etc
- Scheduled -> Scans occur at regular intervals

  - Report on moves, adds and changes

  Performance Monitoring
- The fundamental network statistic ->Amount of network use over time
- Many different ways to gather this metric
  - SNMP,NetFlow, protocol analysis, software agent
- Identify fundamental issues ->Nothing works properly if bandwidth is highly used

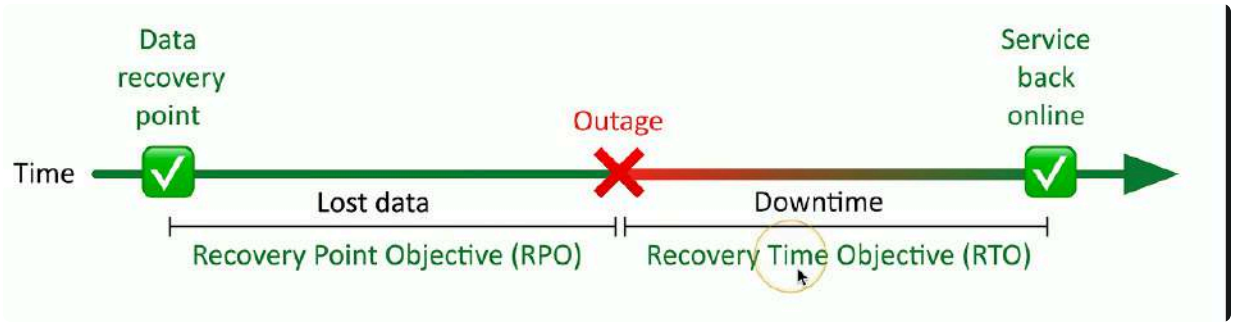
  Availability Monitoring
- Up or Down

    - The most important statistic ->No special rights or permissions required
        - Green good, red bad
- Alarming and alerting ->Notifications through email or SMS should interface fail
- Short term and long term reporting-> View availability over time
- Additional details/monitoring may require SNMP

3.3 Disaster Recovery

Disaster Recovery Plans ->Detailed plans for resuming operations after a disaster
RTO (Recovery Time Objective)

- Time to resume operations ->Want this to be near zero
- Get back to a particular service level in a certain timeframe
  RPO (Recovery Point Objective) -> Also measured as time and want near zero
- How much data loss is acceptable?
- Bring the system back online->How far back in time does data go?
- Define the right RPO
  - Banking transactions,patient info ->Short-less than an hour
  - Web site updates, internal documents -> 1-4 hours



MTTR and MTBF

- Meant time to repair->Time from failure to full functionality
- Meant time between failures->Time between outages
  Cold Site -> No hardware -> No Data ->No people
- Empty building, need to bring data with us and bus in our team
  Hot Site -> Exact replica ->Stocked with hardware constantly updated
- Flip a couple switches and everything moves to new site
  Warm Site -> Just enough to get going -> Big room with rack space
- Hard is ready and waiting but must bring software and data

3.3 Network Redundancy

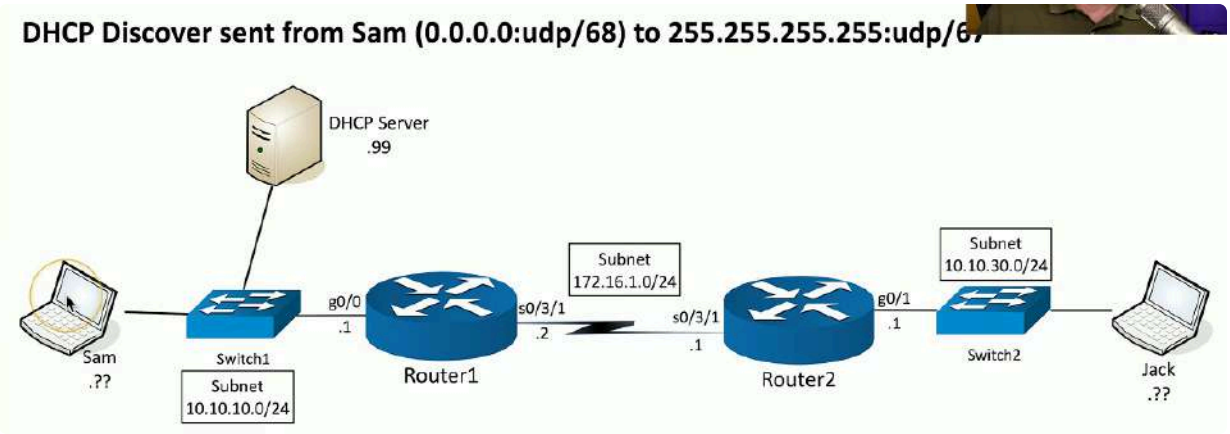
Active-passive

- Two devices are installed and configured-> Only one operates at a time
- If one fails other takes over
  - Constant communication between the pair
- Configuration and real time session information is constantly synchronized
  Active-active
- Bough two devices -> Use both at the same time
- More complex to design and operate
  - Data can flow in many different directions
  - Challenging to manage the flows
  - Monitoring and controlling data requires very good understanding of underlying infrastructure

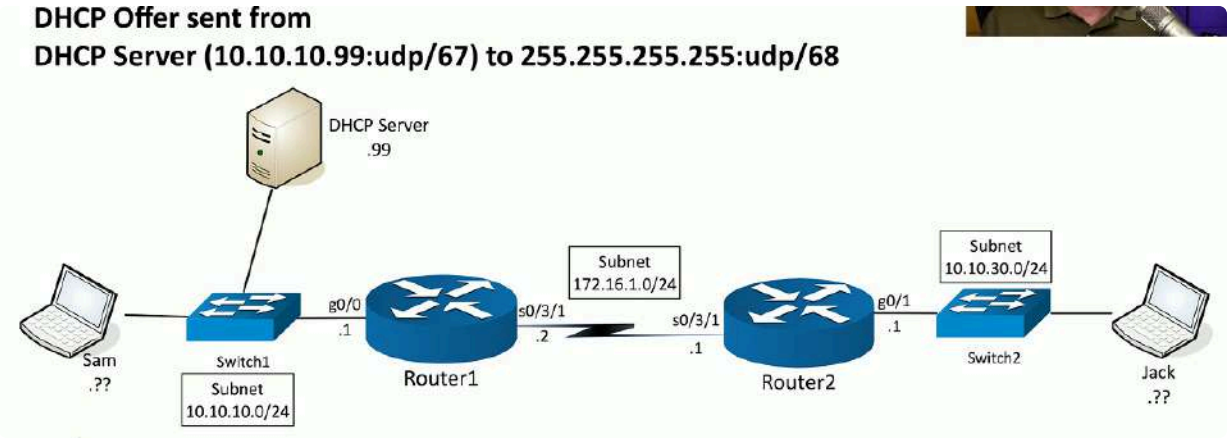
3.4 DHCP

DHCP Process

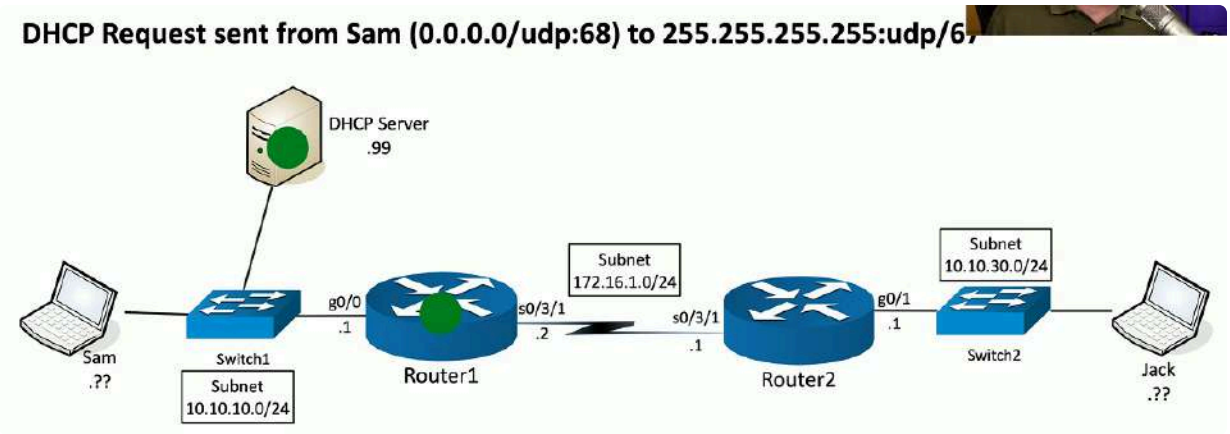
- Dora ->Four step process
  - DIscover ->Find a DHCP Server
  -



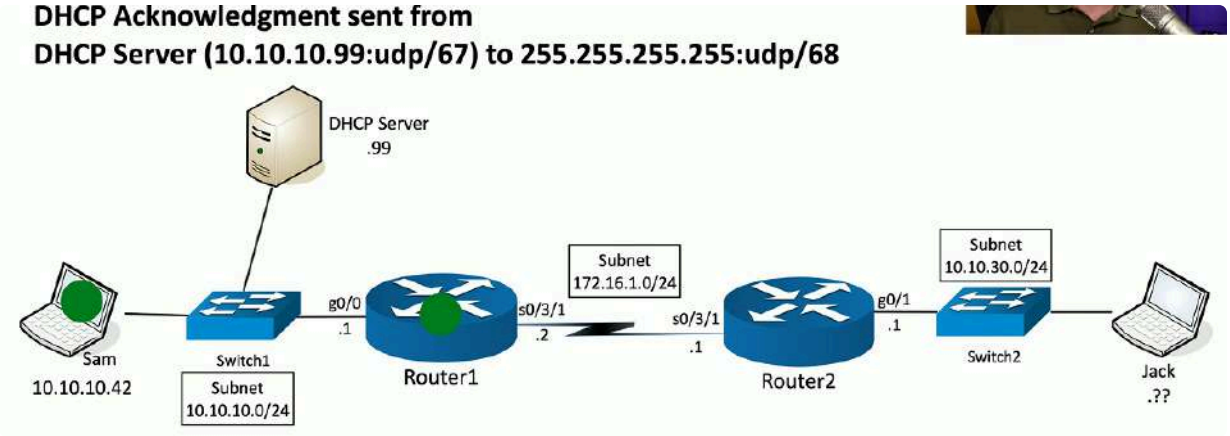
  - Offer -> Get an offer



  - Request -> Lock in the offer

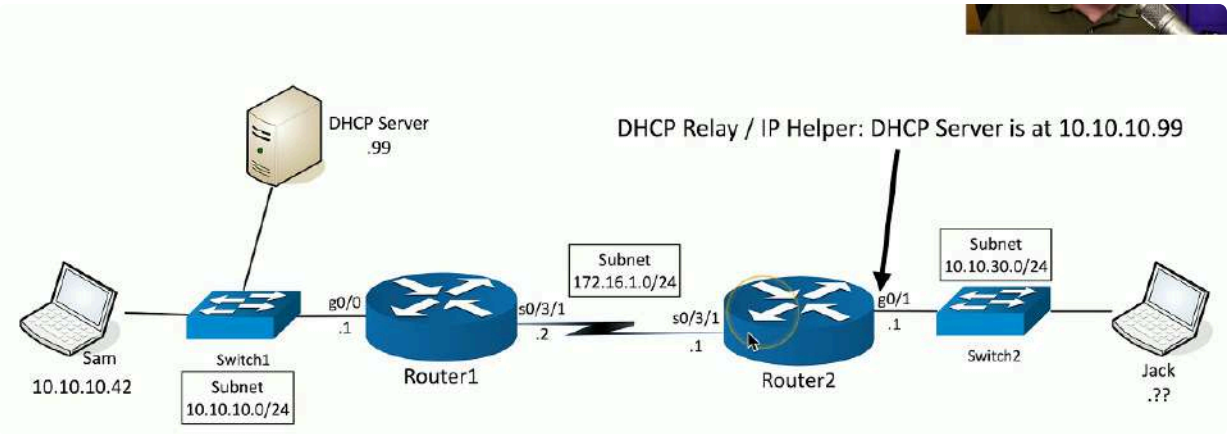


- Acknowledge -> DHCP server confirmation



DHCP Relay

- Configure router with DHCP Relay configuration



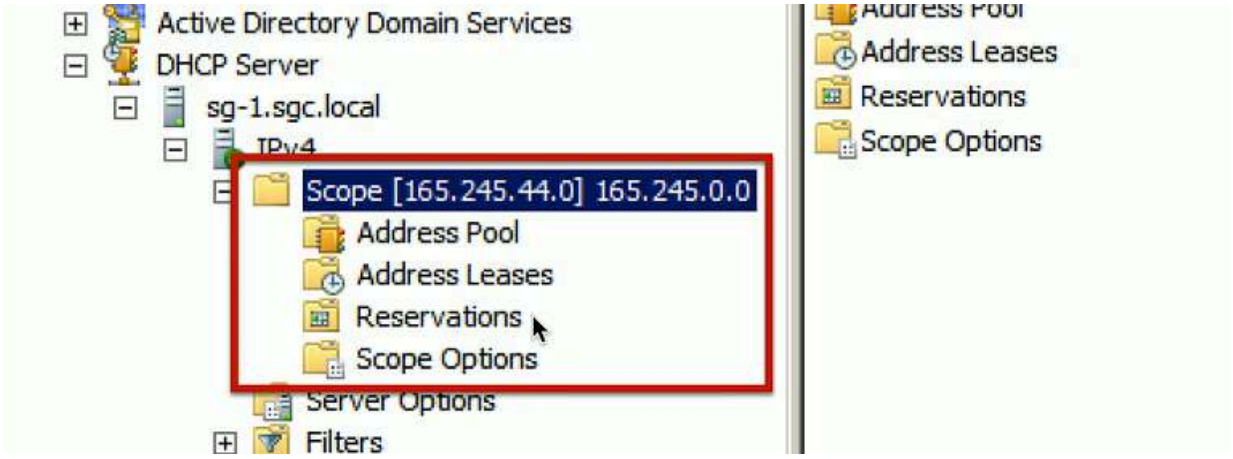
3.4 Configuring DHCP

Scope Properties

- IP address range -> And excluded addresses
- Subnet mask
- Lease durations
- Other scope options ->DNS server,default gateway,VOIP servers

DHCP pools

- Grouping of IP addresses
  - Each subnet has its own scope
- A scope is generally a single contiguous pool of IP addresses
  - DHCP exclusions can be made inside of the scope



DHCP Address Assignment

- Dynamic assignment
  - DHCP server has a big pool of addresses to give out
  - Addresses are reclaimed after a lease period
- Automatic assignment
  - Similar to dynamic allocations
  - DHCP server keeps a list of past assignments
  - You'll always get the same IP address

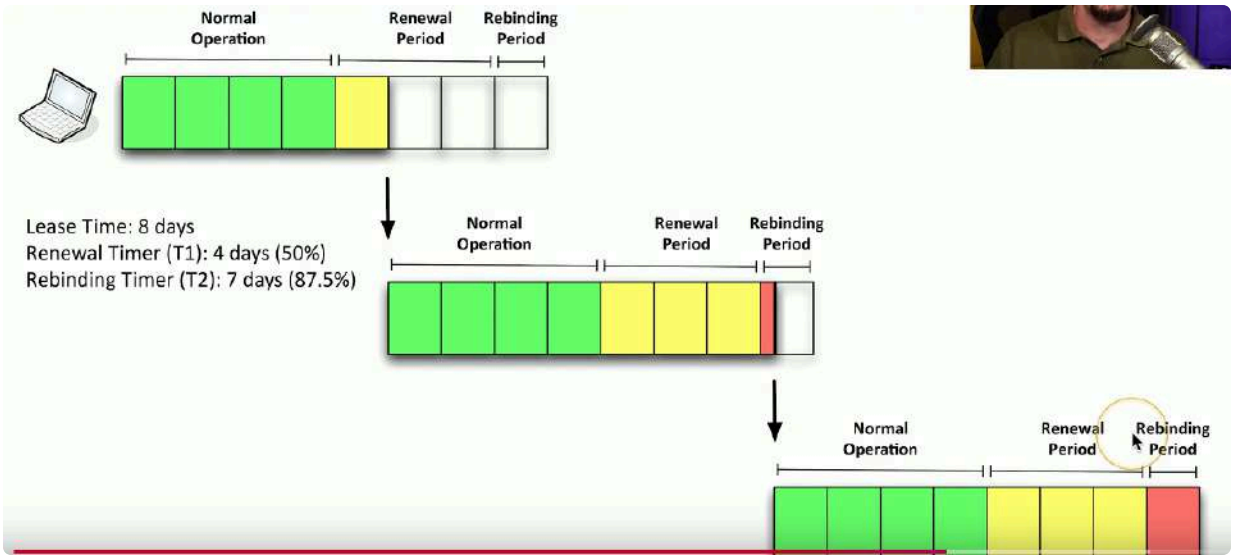
  Address Reservation
- Address reservation ->Administratively configured
- Table of MAC addresses
  - Each MAC address has a matching IP address
- Other names -> Static DHCP assignment, Static DHCP, IP Reservation

DHCP Reneweal

- T1 Timer

    - Check in with the lending DHCP server to renew the IP address
    - 50% of the lease time (by default)
- T2 Timer
  - If original DHCP server is down, try rebinding with any DHCP server
  - 87.5% of the lease time (7/8ths)

  The DHCP Lease Process



DHCP Options

- A special field in the DHCP message -> Many many options to configure
- 256(254 usable) options -> 0 through 255 (0 is pad,255 is end)
- Common options ->Subnet mask, DNS, domain name, etc
- Configured on the DHCP server however not all servers support configuration

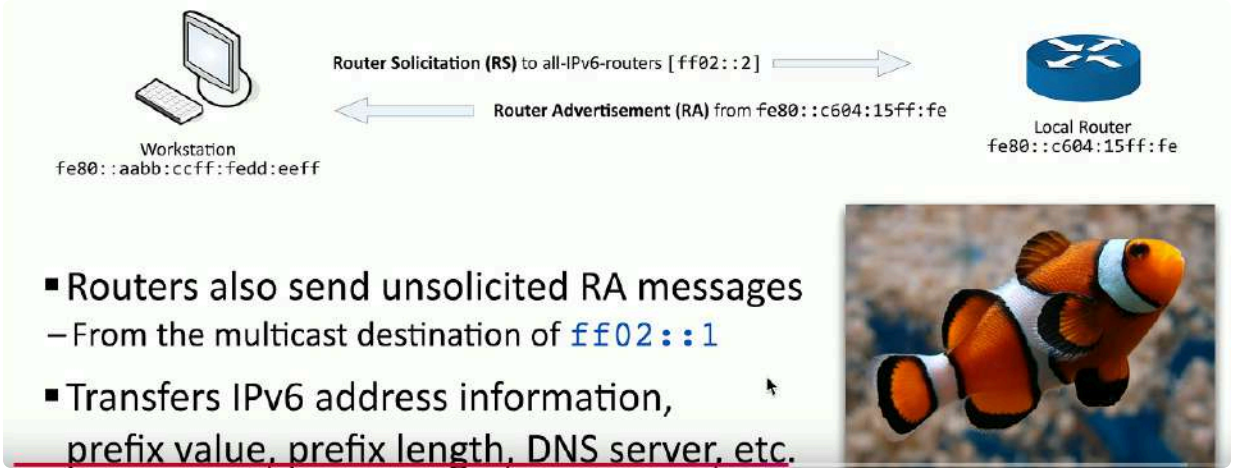
3.4 IPv6 and SLAAC

Automatic IP addresing in IPv6

- DHCP servers
    - Similar process as IPv4
    - Requires redundant DHCP servers
    - Ongoing administration
- Stateless addressing
  - No separate server keeping the state
  - No trackikng of IP or MAC addresses
  - Lease times don't exist

  NDP(Neighbor Discovery Protocol)
- No broadcasts
    - Operates using multicast over ICMPv6
- Neighbor MAC Discovery -> Replaces the IPv4 ARP

- SLAAC (Stateless Address Autoconfiguration)
  - Automatically configure an IP address without a DHCP server
- DAD (Duplicate Address Detection) ->Ensures no duplicate IPs
- Discover Routers
  - Router Solicitation (RS) and Router Advertisement (RA)
  Finding Router
- ICMPv6 adds the Neighbor Discovery Protocol



SLAAC Methodology

- Determine the IP prefix using NDP
  - Router solicitation and router advertisement (RS and RA)
- Use the IP Prefix with a modified EUI-64 address (or randomize)
  - Put them together to make a complete IPv6 address

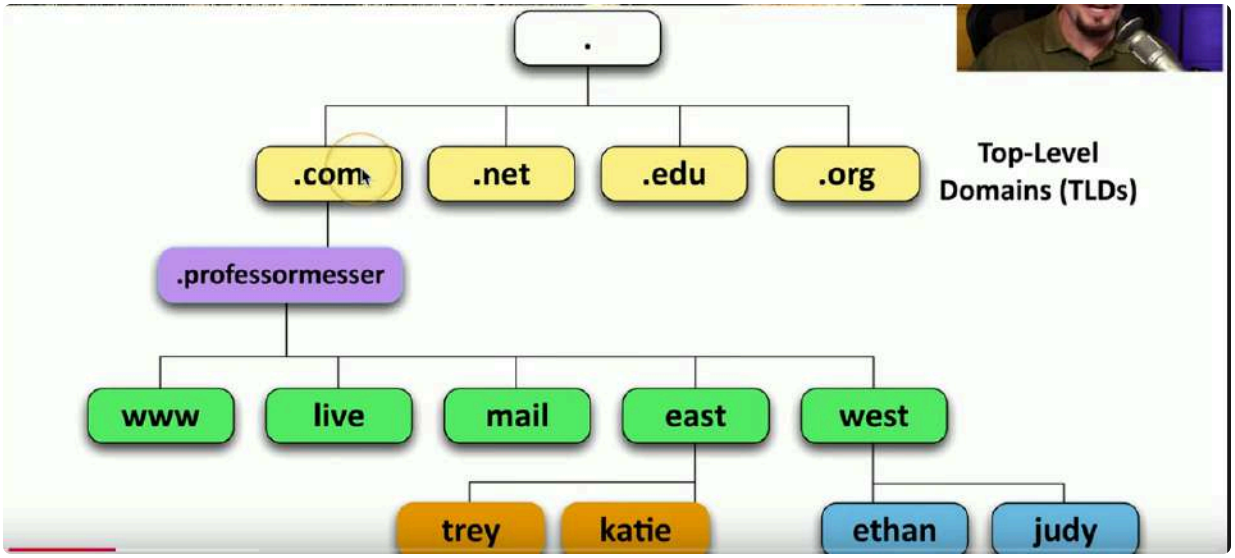
Prefix obtained through Router Solicitation and Advertisement then interface ID generated

- Before using, use NDP's DAD (Duplicate Address Detection)
  - To ensure you are only one with this IPv6 Address

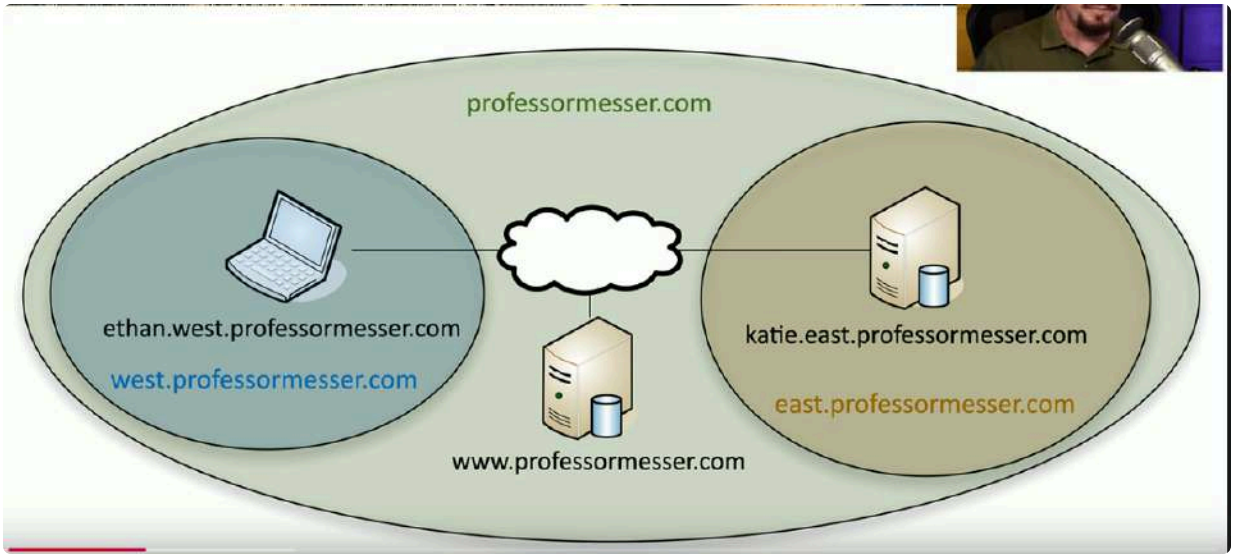
3.4 An Overview of DNS

- Translates human-readable names into computer readable IP addresses
- Hierarchical ->Follow the path
- Distributed Database
  - Many DNS servers -> 13 root server clusters (Over 1,000 actual servers)
  - Hundreds of generic top-level domains (gTLDs) -.com,.org,.net, etc
  - Over 275 country code top-level domains (ccTLDs) -.us,.ca,.uk, etc

DNS Hierarchy



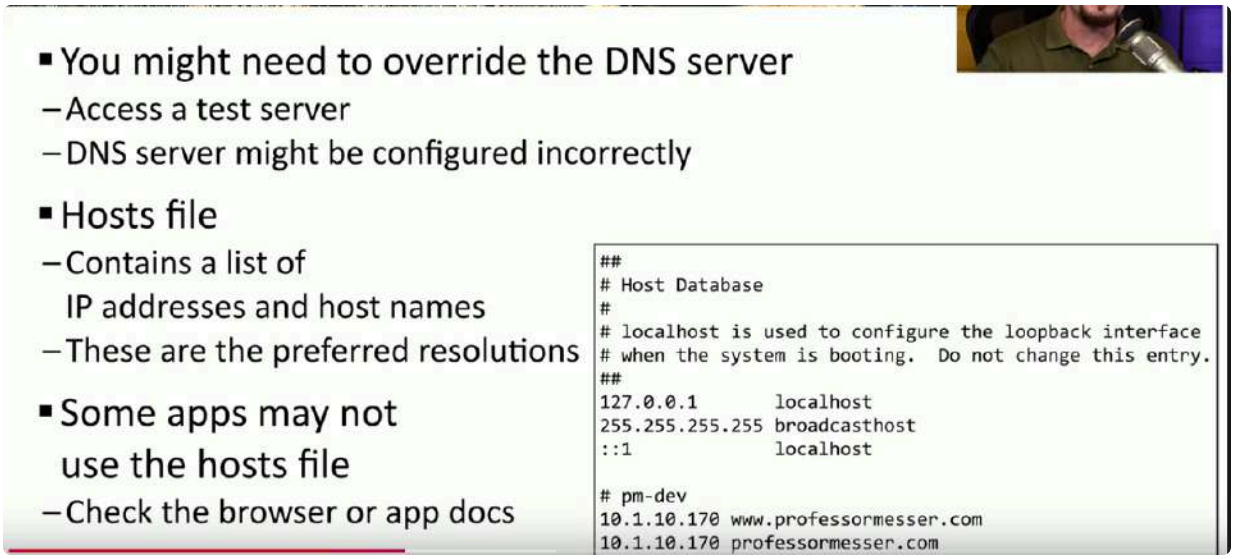
Fully Qualified Domain Name (FQDN)



Primary and Secondary DNS Servers

- Primary ->Contains all zone information for a domain-> Changes made to primary server
- Secondary -> Zone information is read only-> Zone transfers pushed from primary server

Local Name Resolution

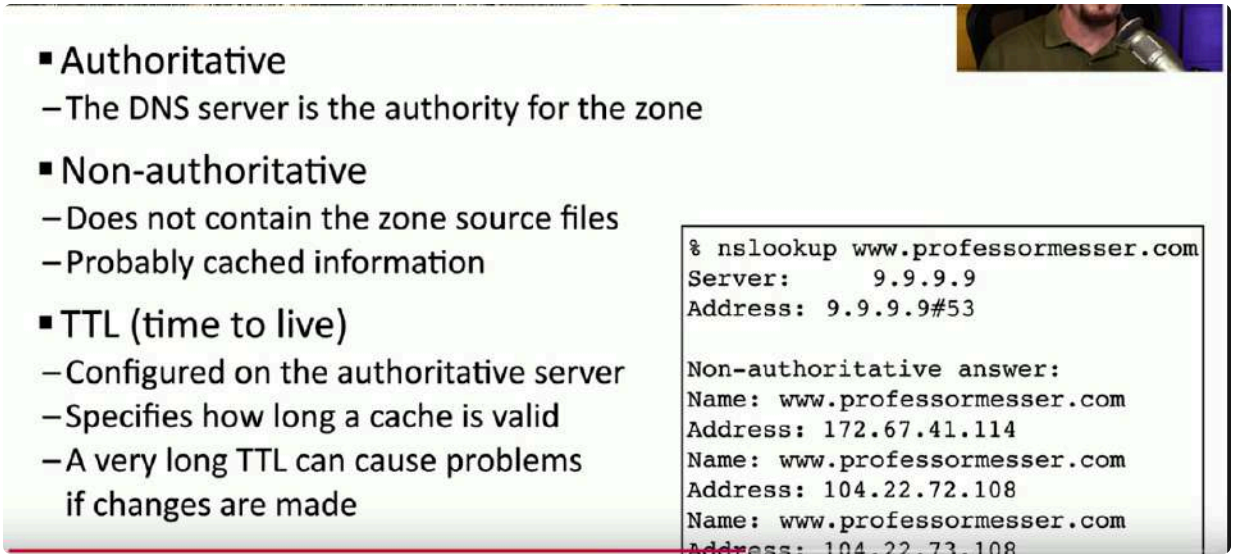


Lookups

- Forward lookup
  - Provides DNS server with an FQDN (Fully Qualified Domain Name)
  - DNS server responds with an IP address
- Reverse DNS

  - Provide DNS server with IP address, DNS returns with an FQDN

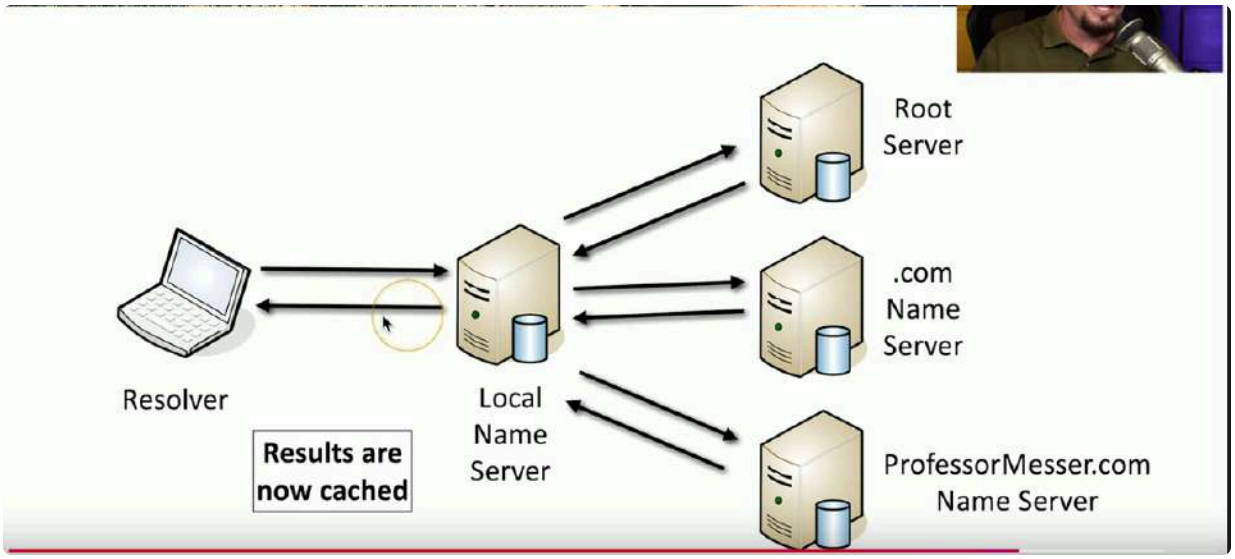
  The authority



Recursive DNS Queries

- Recursive query ->Delegate the lookup to a DNS server
- DNS server does the work and reports back-
  - Large DNS cache provides speed advantage
- Future queries use the local cache

  - Cache entries eventually timeout and are removed



Local Name Server does not know where wanted name server is but knows where root is->Root knows where .com is so returns that location to local name server -> Now local name server looks in .com server which knows where the server containing wanted websites IP is, LNS obtains IP from final name server and caches it for future use as well as returning it to the resolver.

Securing DNS

- DNS is often transmitted in the clear
  - No built in encryption , relatively easy to spoof, redirect email to a different mail server
- Domain Name Security Extensions (DNSSEC)
  - DNS responses from server are digitally signed
  - Forgery would be easily identified
  - Requires additional config of DNS server

  Encrypting DNS
- Sent in clear
- DNS over TLS (DoT)
  - Send DNS traffic over tcp/853 but encrypt it with TLS/SSL
- DNS over HTTPS (DoH)
  - Send DNS traffic in an HTTPS packet
  - Looks like a web server communication over tcp/443
  - Some browser use DoH by default

3.4 DNS Records

- Resource Record (RR)

    - The database record of domain name services
- Over 30 Record types -> IP addresses,certificates,host alias names, etc..

  Start of Authority (SOA)
- Describes the DNS zone details
- Structure

  - IN SOA (Internet zone, Start of Authority) with name of zone

  - Serial number

  - Refresh, retry and expiry timeframes

  - Caching duration/TTL (Time to Live)

```
@ IN SOA example.com.  postmaster.example.com. (
  19990811  ; Serial number
  3600   ; 1 hour refresh
  300  ; 5 minutes retry
  172800 ; 2 days expiry
  43200 ) ; 12 hours minimum
```

  Address records (A) (AAAA)
- Defines the IP address of a host->Most popular query
- A records are for IPv4 addresses-
    - Modify this record to change host name to IP address resolution
- AAAA records are for IPv6 addresses ->Same DNS server, different records

```
www.professormesser.com.    IN A    162.159.246.164  ; Professor Messer
```

  Canonical Name Records (CNAME)
- A name is an alias of another, canonical name

  - One physical server, multiple services

```
; Alias (canonical) names
    chat    IN CNAME mail.example.com.
    ftp     IN CNAME mail.example.com.
    www     IN CNAME mail.example.com.
```

  Mail Exchanger Record (MX)
- Determines the host name for the mail server

  - Not an IP address, it's a name

```
; This is the mail-exchanger.  You can list more than one (if
; applicable), with the integer field indicating priority (lowest
; being a higher priority)
  IN MX   mail.example.com.

; Provides optional information on the machine type & operating system
; used for the server
  IN HINFO  LINUX

; A list of machine names & addresses
    jack.example.com.      IN A    123.12.41.40   ; Windows 10
    mail.example.com.      IN A    123.12.41.41   ; Linux (main server)
    sam.example.com.       IN A    123.12.41.42   ; Windows 11
```

Text Records (TXT)

- Human readable text info ->Useful public info
- SPF Protocol (Sender Policy Framework)
  - Prevent mail spoofing
  - Mail servers check that incoming mail really did come from authorized host
- DKIM (Domain Keys Identified Mail)

  - Digitally sign your outgoing mail
  - Validated by the mail server not usually sen by the end user
  - Put your public key in the DKIM TXT record

```
; SPF TXT records
; owner  class  ttl  TXT "attribute-name=attribute value"
  professormesser.com. 300  IN TXT  "v=spf1 include:mailgun.org ~all"
```

```
; DKIM TXT records
; owner  class  ttl  TXT "attribute-name=attribute value"
1517680427.professormesser._domainkey.professormesser.com. IN 300 TXT
("v=DKIM1;t=s;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDqCUQ5dpKOtwQdE2k8HaCQqV+f"
        "3y30BCzNz75IffEXtk+sTBiDcGWIcapUzkgC4tNOboHBw57APzNInmjH9yZn15TB"
        "TfTavC44nXidUZ8LzsJGWVvYYxoFR5DuBoi/zIOOHv6YDUpDxJa9knZABTOWLS2F"
        "YtK9dWAMaOZdtTBOhQIDAQAB")
```

Name Server Records (NS)

- List the name servers for a domain->NS records point to the name of the server

```
; main domain name servers
                IN      NS      ns1.example.com.
                IN      NS      ns2.example.com.
; mail domain mail servers
                IN      MX       mail.example.com.
; A records for name servers above
ns1             IN      A       192.168.0.3
ns2             IN      A       192.168.0.4
; A record for mail server above
mail            IN      A       192.168.0.5
```

Pointer Record (PTR)

- The reverse of an A or AAAA record
  - Added to a reverse map zone file

```
$TTL 2d ; 172800 secs
$ORIGIN 23.168.192.IN-ADDR.ARPA.
@               IN      SOA   ns1.example.com. hostmaster.example.com. (
                                2003080800 ; serial number
                                12h         ; refresh
                                15m         ; update retry
                                3w          ; expiry
                                3h          ; minimum
                                )
                IN      NS      ns1.example.com.
                IN      NS      ns2.example.com.
; 2 below is actually an unqualified name and becomes
; 2.23.168.192.IN-ADDR.ARPA.
2               IN      PTR     joe.example.com. ; FDQN
....
15              IN      PTR     www.example.com.
....
17              IN      PTR     bill.example.com.
....
```

Here if we were to query the following we would get these names

- 192.168.23.2 -> joe.example.com
- 192.168.23.15 -> www.example.com
- 192.168.23.17 -> bill.example.com

  Note how address is read in reverse from whats written in the PTR record and first char (which is last num of IP) is just substituted depending on the wanted name

3.4 Time Protocols

NTP (Network Time Protocol)

- Switches, routers,firewalls, servers, workstations ->All have its own clock
- Synchronizing these is critical for log files,authentication info, and outage details
- Automatic updates or flexible configured to how you want to update times

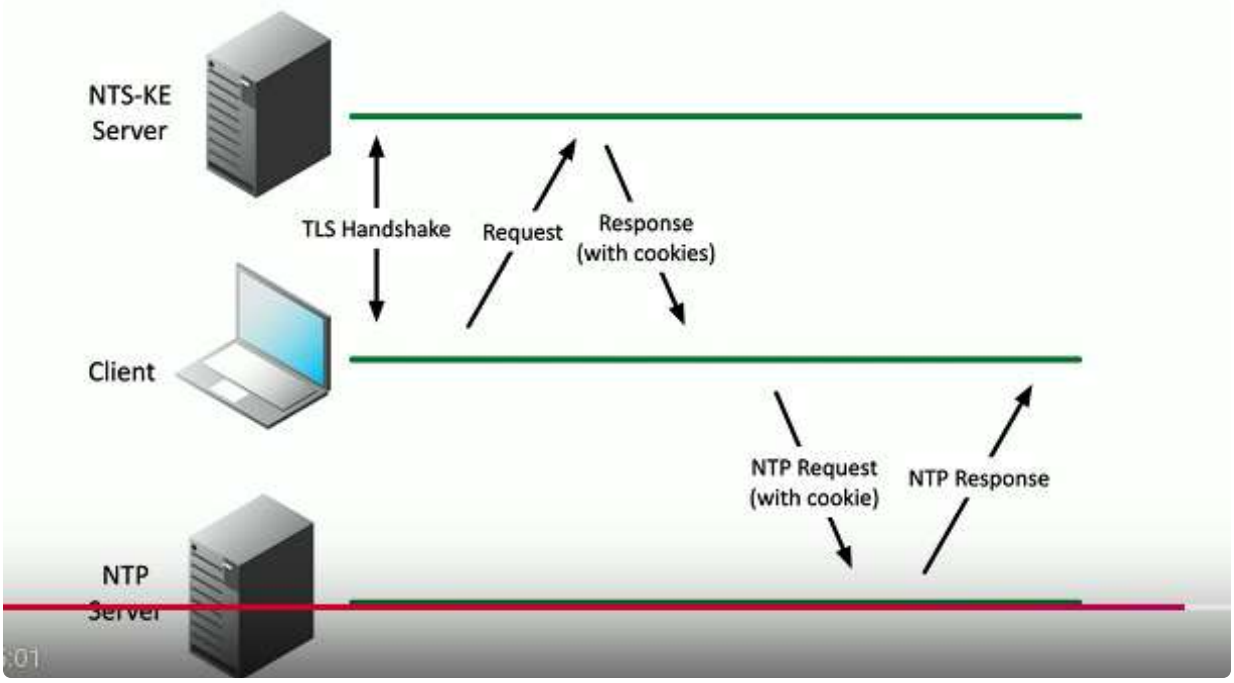
  NTP Clients and Servers
- NTP Server
  - Listens on udp/123, responds to time requests from NTP clients
  - Does not modify their own time
- NTP Client
  - Requests time updates from NTP server
- NTP client/server

  - Requests time updates from an NTP sever

  - Responds to time requests from other NTP clients

  Network Time Security (NTS)
- NTP sends traffic in the clear->Time of day isn't really a secret
- Wrong time however can be a significant problem
  - What if NTP server response is spoofed or can't be trusted
- TLS handshake is used for key exchange
  - Get authroization cookie from an NTS key exchange server
- Connect to an NTP server using this authentication

  - Both requests and responses are validated



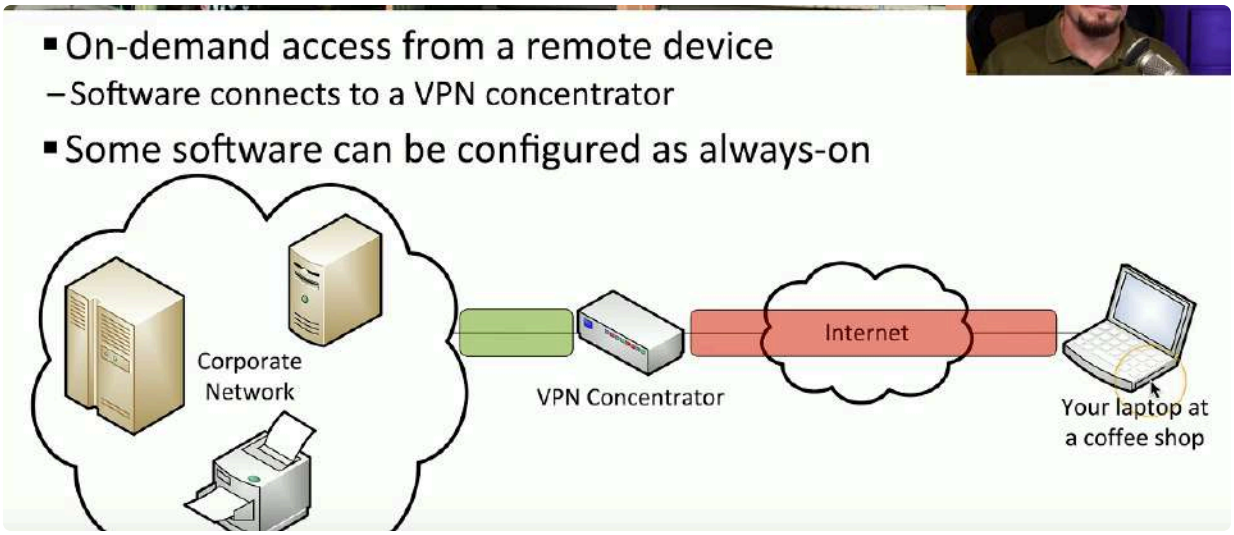
Precision Time Protocol (PTP)

- A more precise time protocol -> Hardware based time synchronization
- Nanosecond granularity ->Important for industrial apps,financial trading etc
- Often implemented as specialized hardware

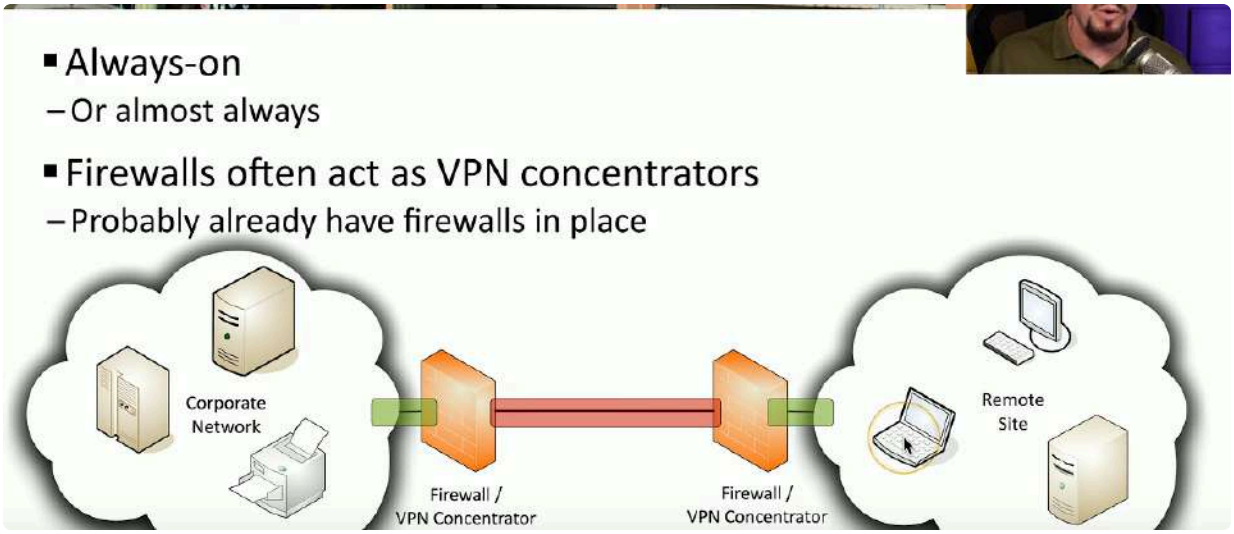
3.5 VPNs

- Virtual Private Networks -> Encrypted(private) data traversing a public network
- Concentrator ->Encryption/Decryption access device
  - Often integrated into firewall

  Client To Site VPN



  Site To Site VPN



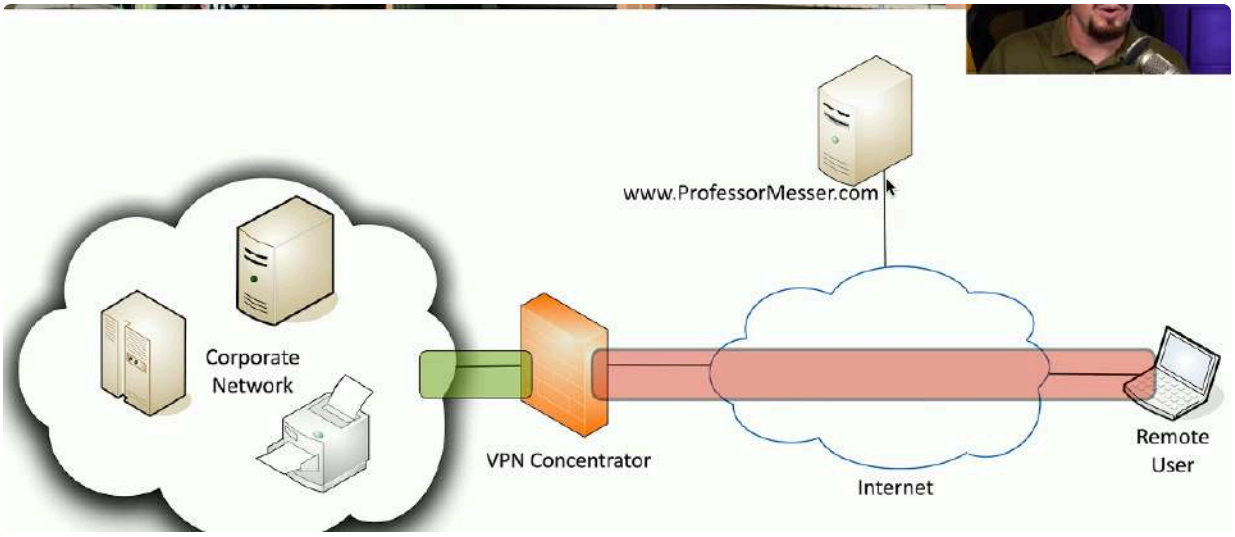
  Clientless VPNs

- HTML version 5-> Commonly used in web browsers
- Includes comprehensive API supports
  - Web cryptography API
- Create VPN tunnel without a separate VPN application

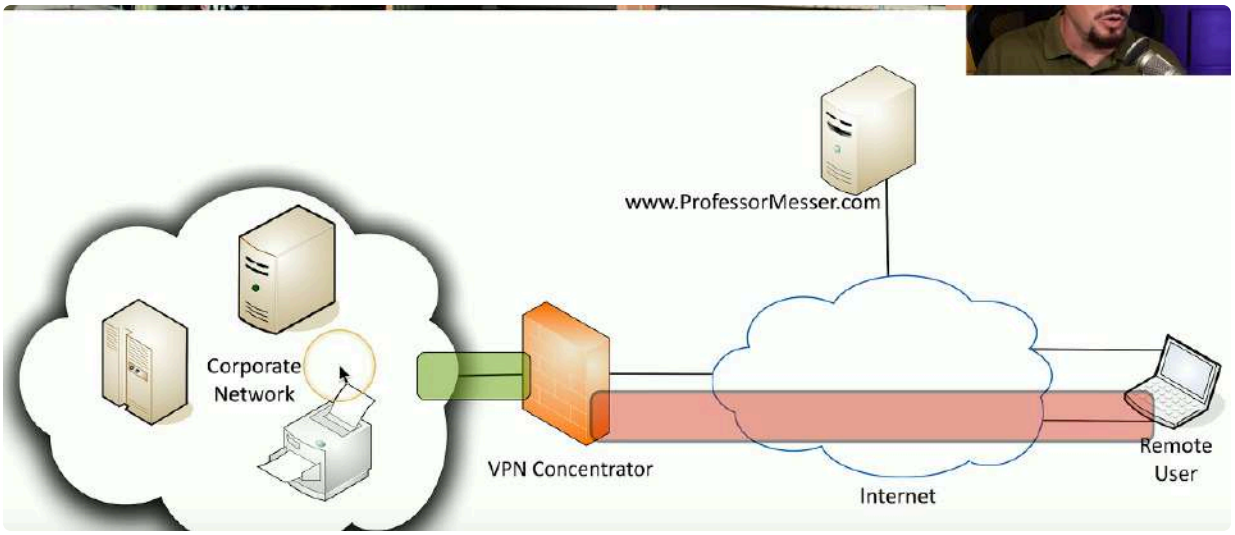
  Split tunnel vs. full tunnel
- Full tunnel
  - All traffic is sent through VPN tunnel
  - Client makes no additional forwarding decisions
  - May require additional routing at the concentrator

- Split tunnel
  - VPN Traffic is sent though the tunnelk
  - Non-VPN taffic is sent normally
  - Configured in VPN software

  Full Tunnel



  Split Tunnel



3.5 Remote Access

SSH (Secure Shell)

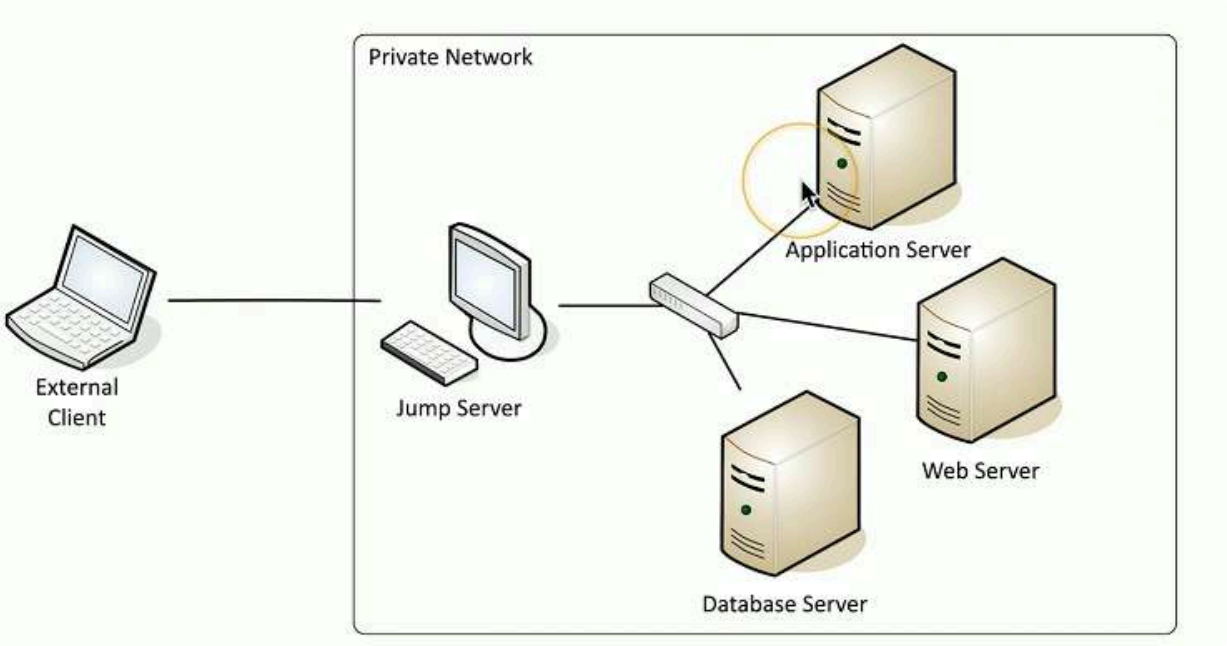
- Encrypted console communication -tcp/22
- Looks and acts the same as Telnet -tcp/23

  GUI
- Share a desktop from a remote location like you are right there
- RDP (Microsoft Remote Desktop Protocol)
  - Clients for Mac OS,Linux and others as well

- VNC (Virtual Network Computing)
  - Remote Frame Buffer (RFB) protocol
  - Client for many operating systems
  - Many are open source

  Console
- Directly connect to the device
  - Traditionally a serial connection
  - DB9 connector, RJ45 serial, USB connection
- When all else fails -> console will be available
  - Text based serial interface ->The console

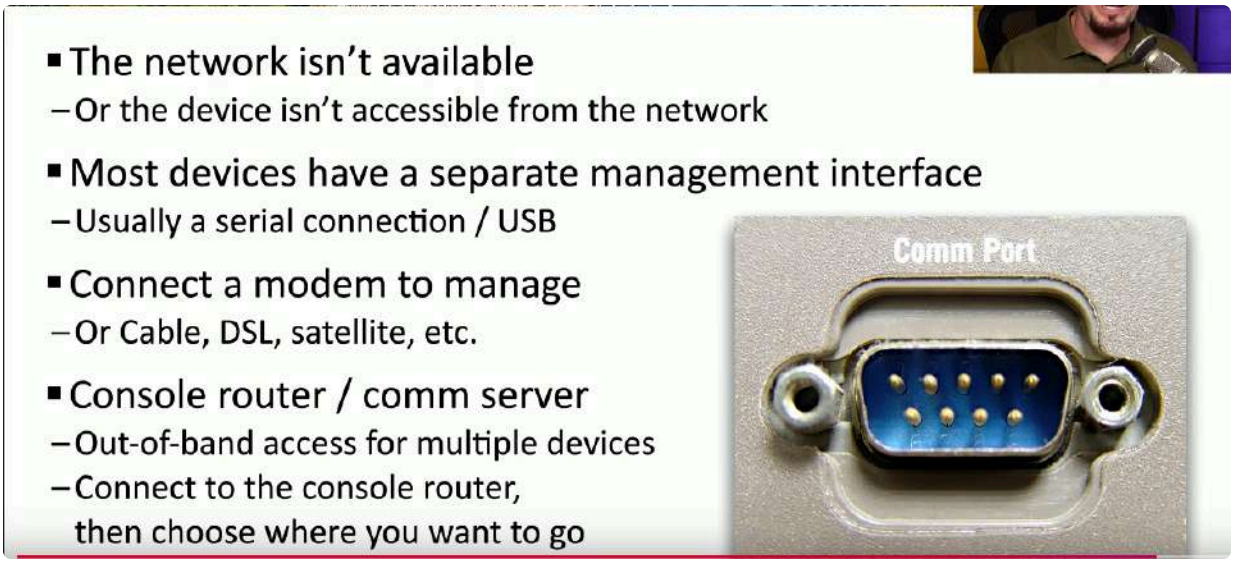
  Jump Box
- Access secure network zones
  - Provides an access mechanism to a protected network
- Highly secured device ->Hardened and monitored
- SSH/Tunnel/VPN to the jump server
  - RDP,SSH or jump from there
- Compromise of jump server is a significant breach and security concern



In-band management

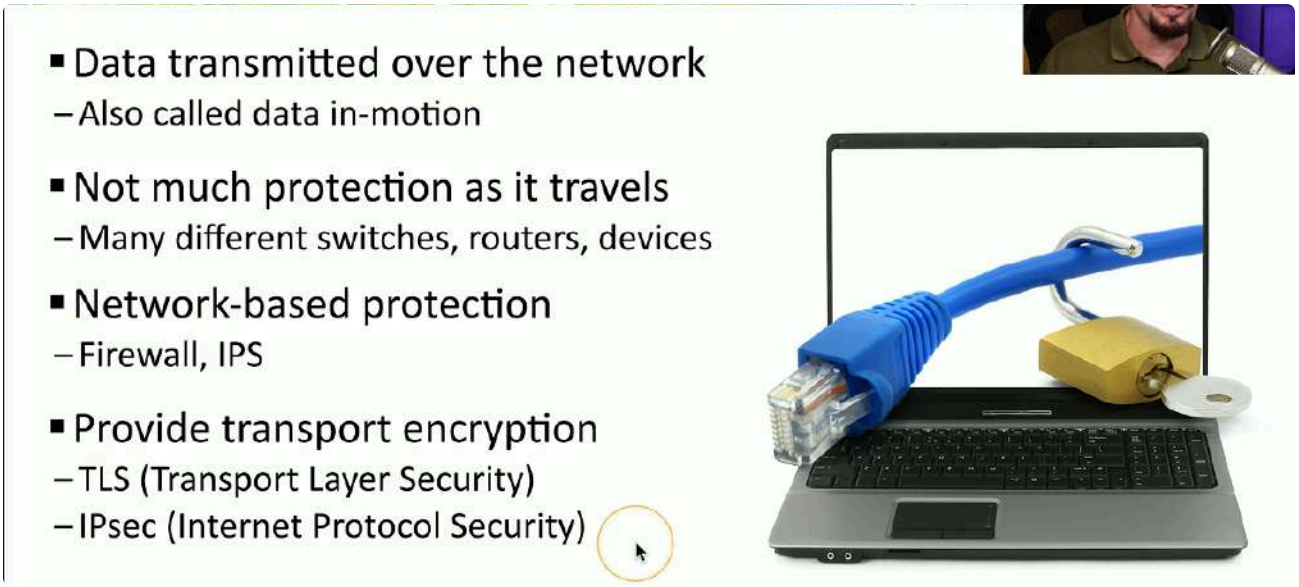
- Assign an IP address to a device ->Switch,router,firewall etc
- May be a separate Ethernet interface ->Often marked on device
  - The IP address is inside the device
- Access the device -> SSH or browser-based console

Out-of-band Management

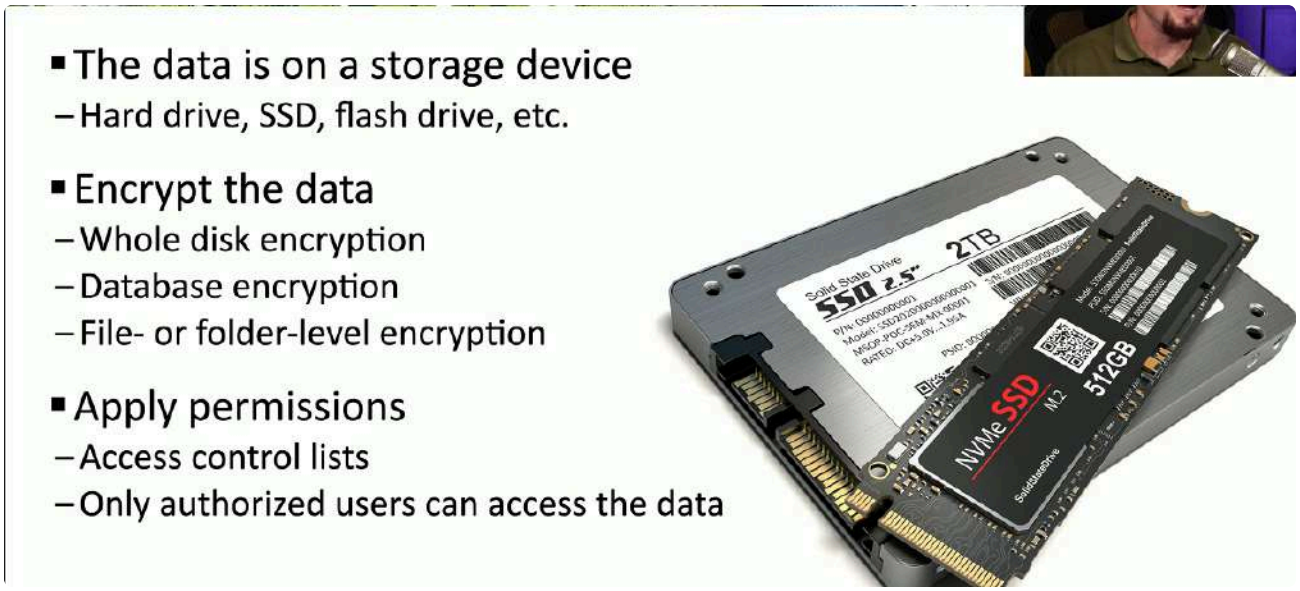


4.1 Security Concepts

Data in Transit



Data at rest



Public Key Infrastructure (PKI)

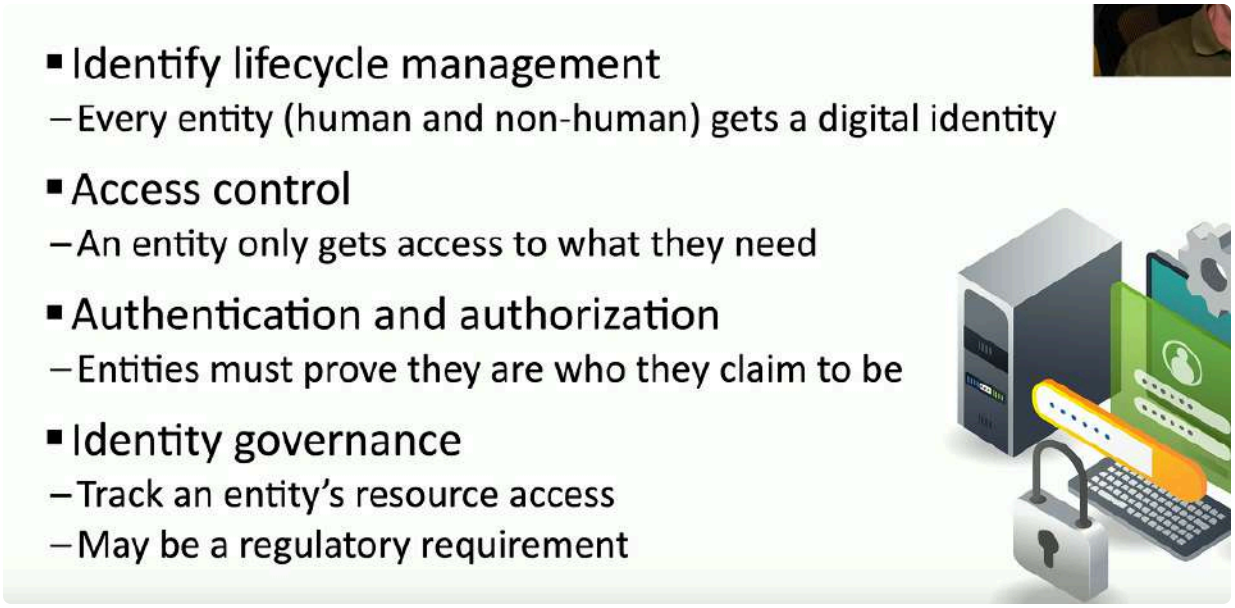
- Policies,procedures,hardware,software, people
  - Digital certificates: create, distribute, manage, store, revoke
- Also refers to the binding of public keys to people or devices
  - The certificate of authority -> It's all about trust

  Digital Certificates
- A public key certificate
  - Binds a public key with a digital signature
  - And other details about the key holder
- Digital signature adds trust
  - PKI uses certificate authorities for additional trust
  - Web of Trust adds other users for additional trust
- Certificate creation can be built into OS
  - Part of Windows Domain services
  - 3rd-party options

  Certificate Authorities
- Certificate Authority (CA) has digitally signed the website certificate
  - You trust the CA therefore you trust the website
  - Real time verification

  Self-signed Certificates

Identity and Access Management (IAM)



Least privilege

- Rights should be set to bare minimum
- All user accounts must be limited

Role based Access Control (RBAC)

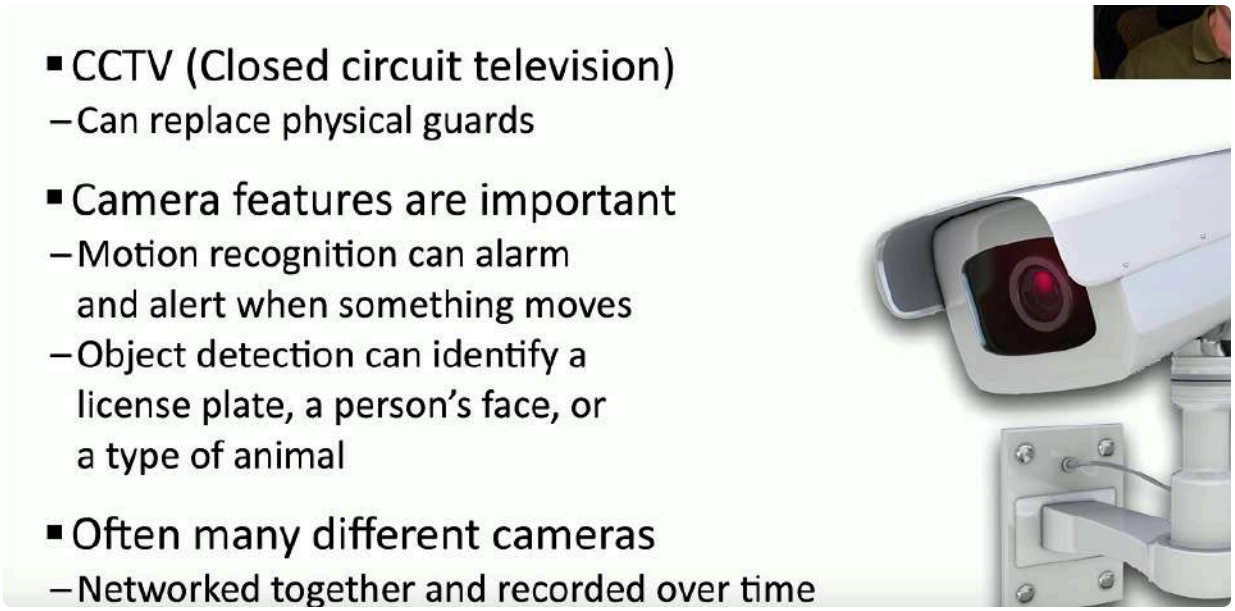
- Give perms based on Role in organization
- In Windows, use Groups to provide role-based access control

Geographic Restrictions

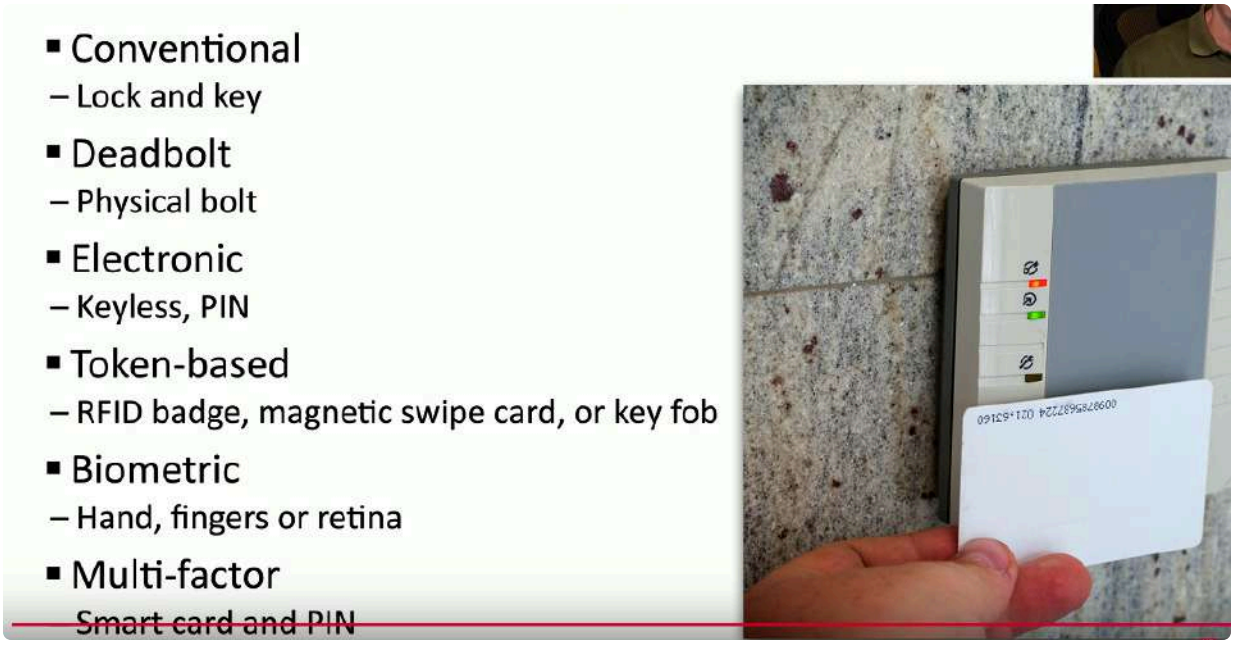
- Geofencing

- Automatically allow or restrict access when the user is in a particular location
- Ex: Don't allow this app to run unless near the office

Cameras



Door locks

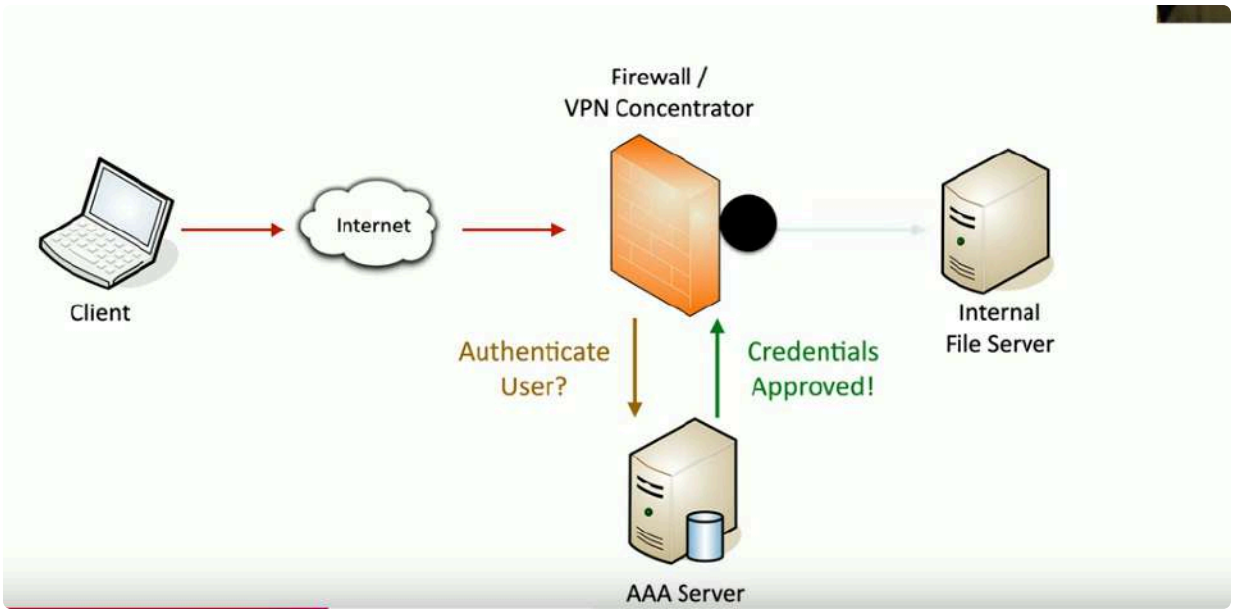


4.1 Authentication

AAA Framework

- Identification -> Who you claim to be -> Usually your username
- Authentication -> Prove you are who you say you are ->Passwords, MFA etc
- Authorization
  - Based on identification and authentication what access do you have
- Accounting

  - Resources used: Login time,data sent and received, logout time



Single Sign On

- Provide credentials one time
  - Get access to all available or assigned resources
  - No additional authentication required
- Usually limited by time -> Can work for 24 hours ->Authenticate again after timer
- Underlying authentication infrastructure must support SSO

  - Not always an option

  RADIUS (Remote Authentication Dial-In User Service)
- One of the more common AAA protocols
  - Supported in wide variety of platforms ->Not just for dial-in
- Centralized authentication for users

  - Routers,switches, firewalls
  - Server authentication
  - Remote VPN access
  - 802.1X network access

  LDAP (Lightweight Directory Access Protocol)
- Protocol for reading and writing directories over an IP network
  - Organized set of records like a phone directory
- X.500 Specification written by ITU (International Telecommunications Union)
- DAP ran on the OSI protocol stack -> LDAP is lightweight
- LDAP is the protocol used to query and update an X.500 Directory

  - Such as Windows Active Directory, Apple Open Directory,Novell eDirectory...

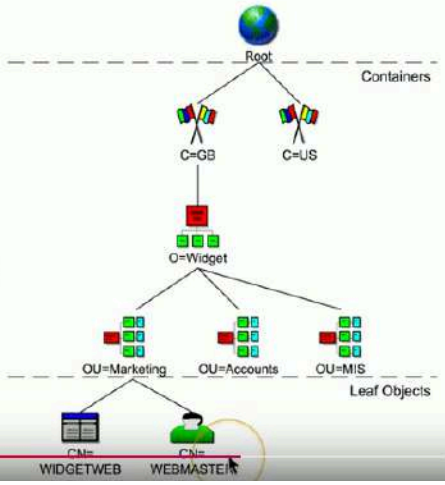
  X.500 Distinguished Names

- *attribute=value* pairs
- Most specific attribute is listed first
  - This may be similar to the way you already think

```
CN=WIDGETWEB, OU=Marketing, O=Widget, L=London, ST=London, C=GB, DC=widget, DC=com
```

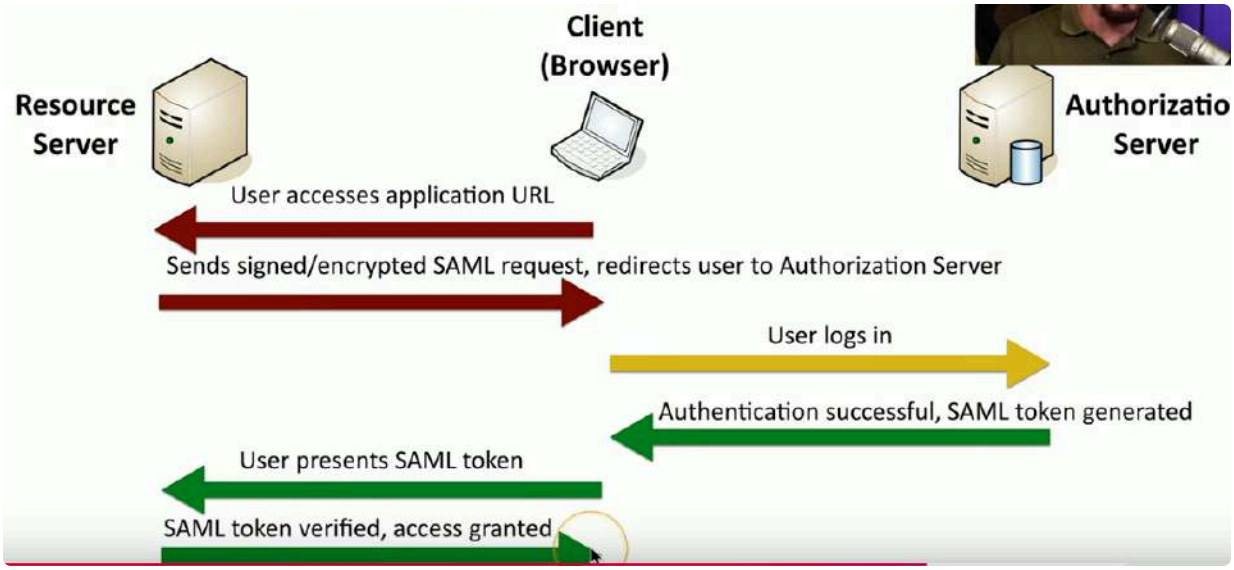
Attribute	Field	Usage
CN	Common Name	Identifies the person or object.
OU	Organizational Unit	A unit or department within the organization.
O	Organization	The name of the organization.
L	Locality	Usually a city or area.
ST	State	A state, province, or county within a country.
C	Country	The country's 2-character ISO code (such as c=US or c=GB).
DC	Domain Component	Components of the object's domain.

- Hierarchical structure
  - Builds a tree
- Container objects
  - Country, organization, organizational units
- Leaf objects
  - Users, computers, printers, files



Security Assertion Markup Language (SAML)

- Open standard for authentication and authorization
  - Can authenticate through a third-party to gain access
- Not originally designed for mobile apps -> SAML's largest roadblock



TACACS

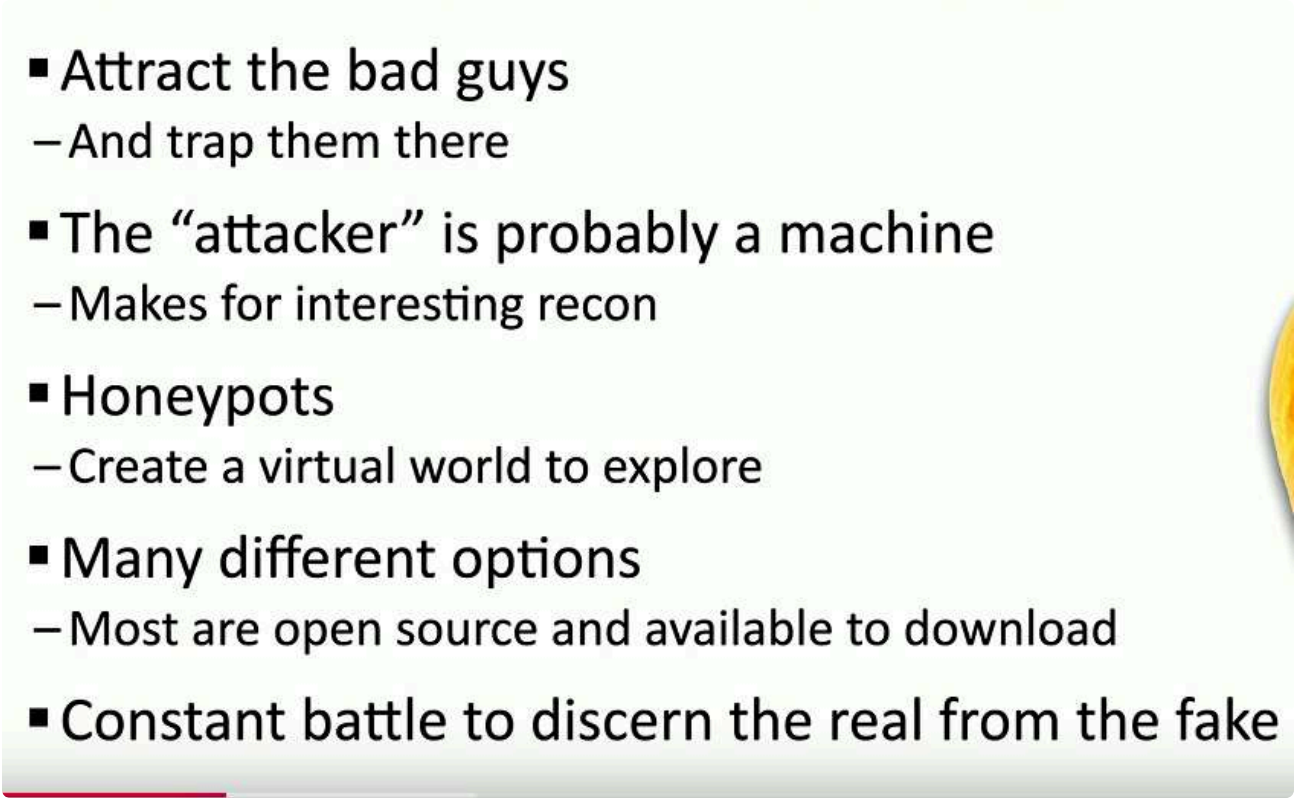
- Terminal Access Controller Access-Control System
  - Remote authentication protocol
  - Created to control access to dial-up lines to ARPANET
- TACACS+

  - Latest version of TACACS ->Not backwards compatible
  - More authentication requests and response codes
  - Released as an open standard in 1993

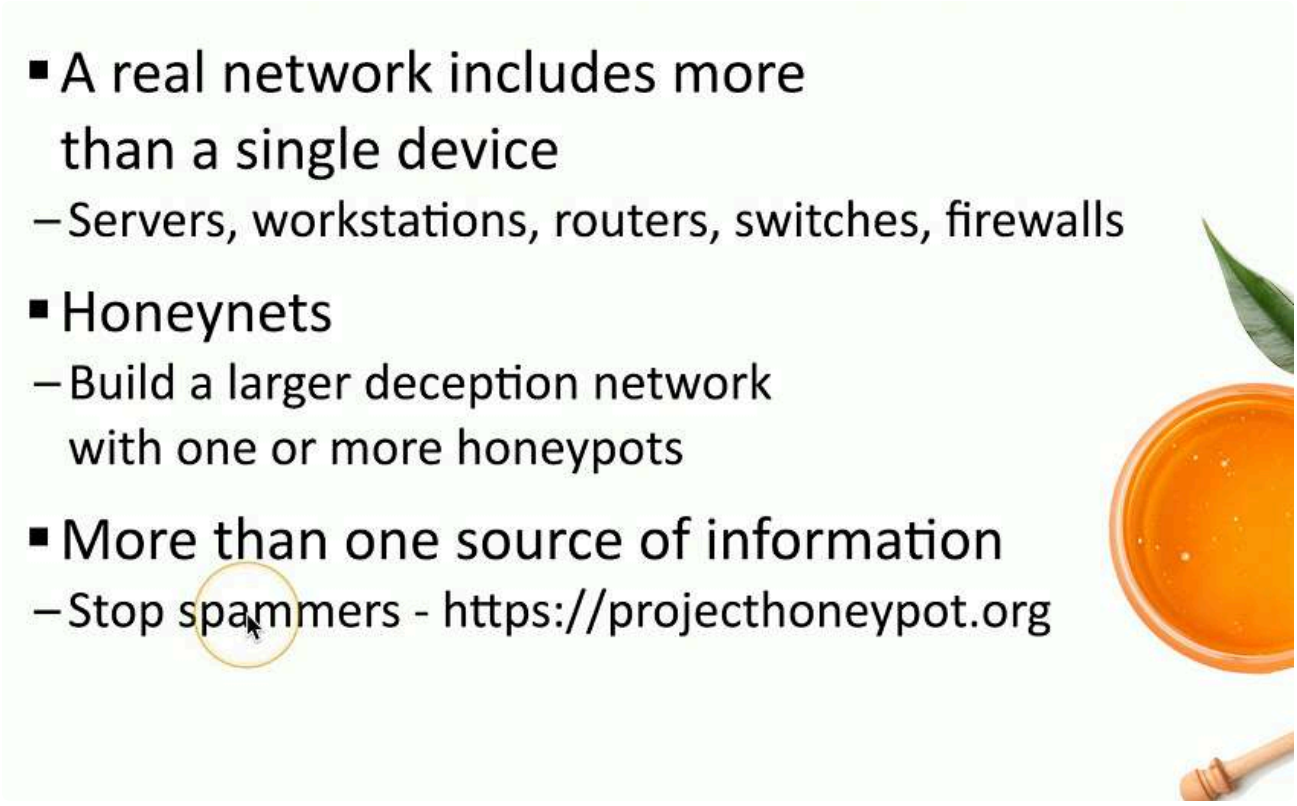
  TOTP
- Time based One-Time Password algorithm
  - Use a secret key and the time of day ->No incremental counter
  - Form of MFA
- Secret key is configured head of time
  - Times are synchronized via NTP

4.1 Security Technologies

Honeypots

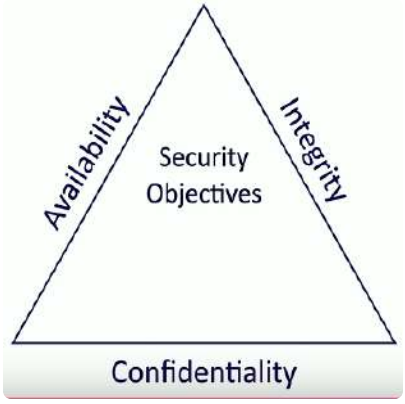


Honeynets



The CIA Triad

- Combination of principles
  - Fundamentals of Security ->Sometimes referenced as the AIC Triad
- Confidentiality, Integrity, Availability (CIA)
- Confidentiality ->Prevent disclosure of information to unauthorized individuals
- Integrity ->Messages can't be modified without detection
- Availability ->Systems and networks must be up and running



4.1 Regulatory Compliance

Compliance

- Meeting the standards of laws, policies and regulations
  Data Localization

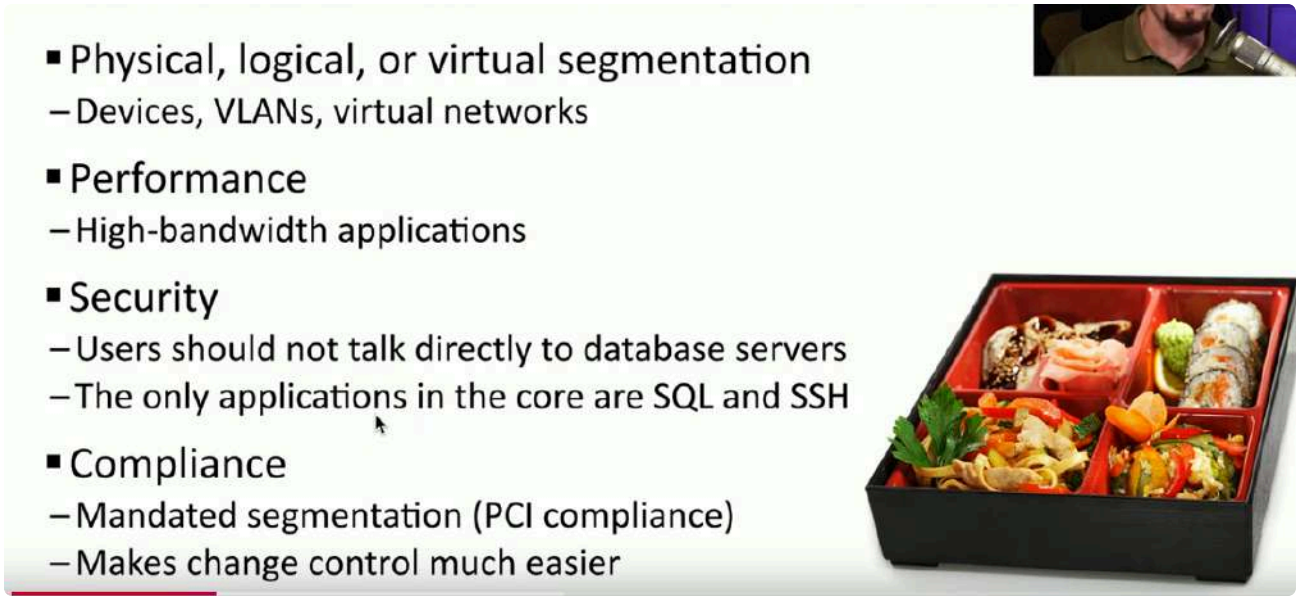
- Data from a region or country is stored within the borders of that region or country
- Laws may prohibit where data is stored
  - GDPR (General Data Protection Regulations)
  - A complex mesh of technology and legalities

  GDPR

PCI DSS

- Payment Card Industry Data Security Standard (PCI DSS)
  - Standard for protecting credit cards
- Six control objectives
  - Build and maintain a secure network and systems
  - Protect cardholder data
  - Maintain a vulnerability management program
  - Implement strong access control measures
  - Regularly monitor and test networks
  - Maintain an information security policy

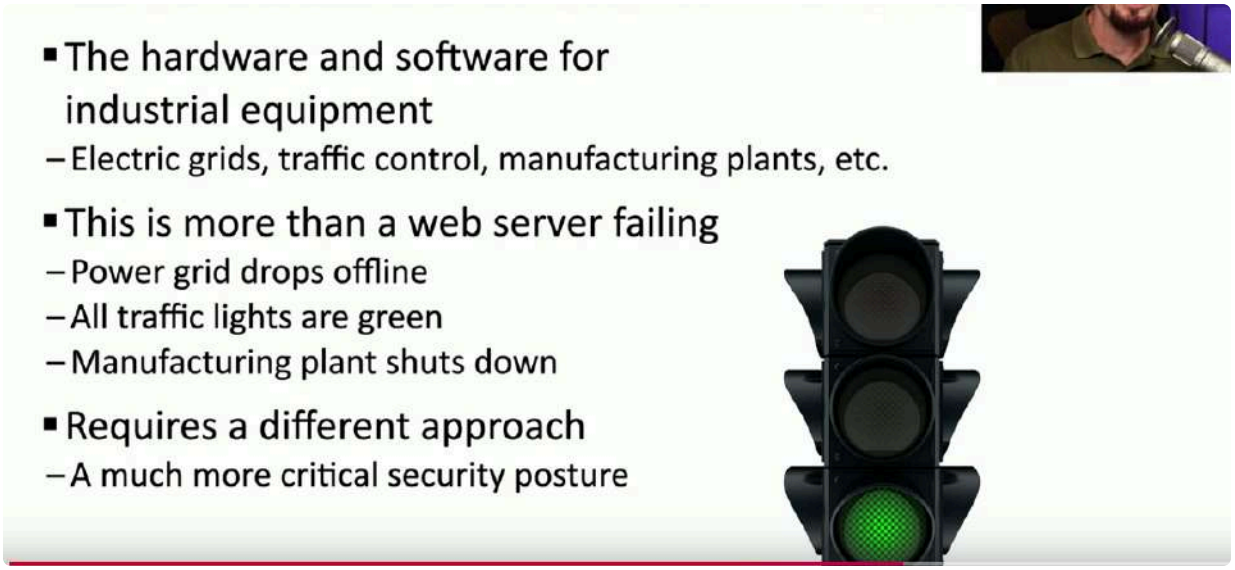
4.1 Segmentation Enforcement



SCADA/ICS

- Supervisory Control and Data Acquisition System
  - Large scale, multi-site Industrial Control Systems (ICS)
- PC manages equipment
  - Power generation,refining, manufacturing equipment
  - Facilities,industrial, energy, logistics
- Distributed control systems
  - Real time info ->System control
- Requires extensive segmentation -> No access from the outside

Operational Technology (OT)



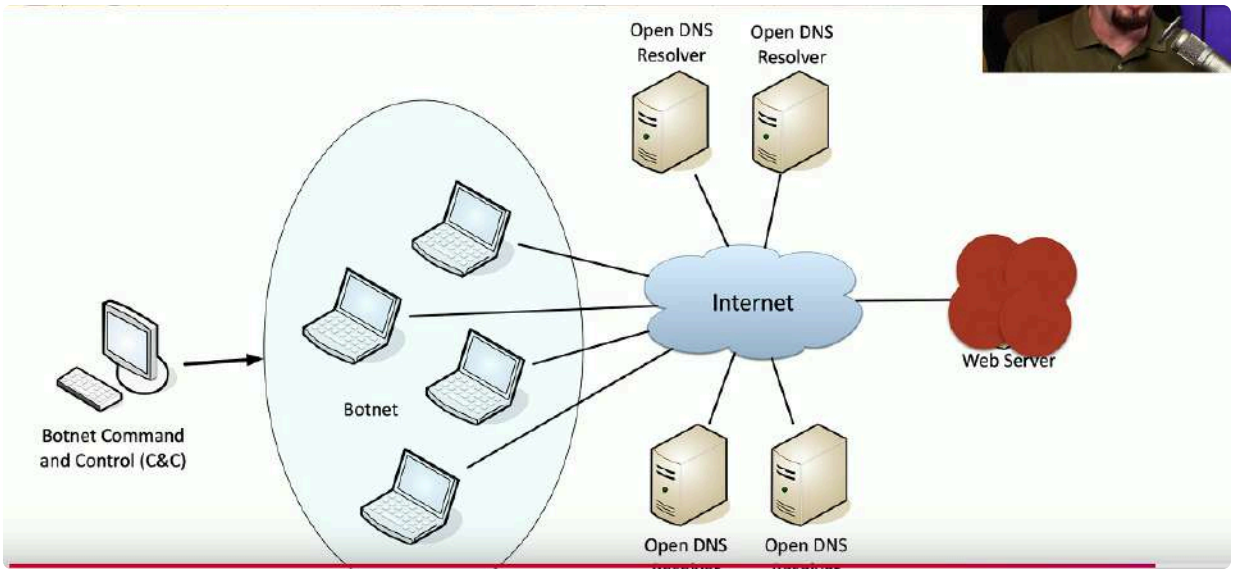
Guest Networks

- A network for visitors ->No access to private network
- Separate wireless network for guests only

- Controlled access -> Password or captive portal
- Firewalled from rest of technology ->Internet access only

4.2 Denial of Service

- Force a service to fail ->Overload the service
- Take advantage of vulnerability
- Create a smokescreen for some other exploit
  - Precursor to a DNS spoofing attack
  Unintentional/Friendly DoS
- Network DoS
  - Layer 2 Loop without STP (Spanning Tree Protocol)
- Bandwidth DoS ->Downloading multi-gigabyte OS distributions over a DSL line
  Distributed Denial of Service (DDoS)
- Launch army of computers to bring down a service
  - Use all bandwidth or resources
- Botnets used for this
- Assymmetric Threat -> Attacker may heave fewer resources than victim
  DDoS Reflection and Amplification
- Turn your small attack into a big attack ->Reflected off another device or service
- Turn internet services against victim
- Uses protocols with little (if any) authentication or checks
  - NTP,DNS,ICMP
  DNS Amplification DDoS



4.2 VLAN Hopping

- Define different VLANs
  - Organization,network engineering, security
- You only have access to your VLAN ->Good security best practice
- Sometimes possible to "Hop" to another VLAN ->This shouldn't happen
- Two primary methods
  - Switch spoofing
  - Double tagging

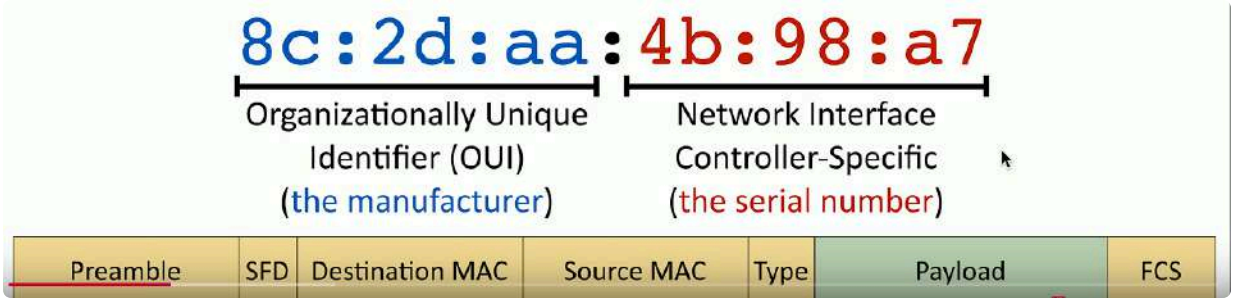
  Switch Spoofing
- Some switches support automatic configuration
  - Is the switch port for a device or is it a trunk?
- No authentication required ->Pretend to be a switch ->Send trunk negotiation
- Now you've got a trunk link to a switch ->Send and receive from any configured VLAN
- Switch admins should disable trunk negotiation
  - Administratively configure trunk interfaces and device/access interfaces

  Double Tagging
- Craft a packet that includes two VLAN tags
  - Takes advantage of the "native" VLAN configuration
- The first native VLAN tag is removed by the first switch
  - Second fake tag is now visible to the second switch
  - Packet is forwarded to the target
- One way trip->Responses don't have a way back to source host ->Good for DoS
- Don't put any devices on the native VLAN
  - Change the native VLAN ID ->Force tagging of the native VLAN

4.2 MAC Flooding

The Mac Address

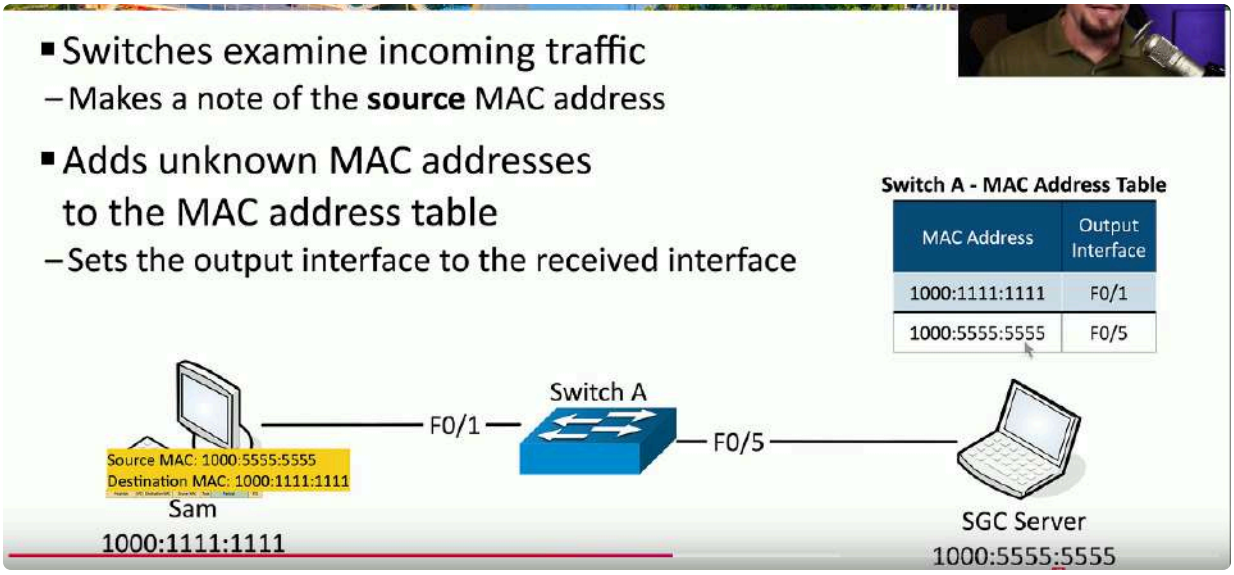
- Ethernet Media Access Control address
  - Physical address of a network adapter -> Unique to a device
- 48 bits/ 6 bytes long -> Displayed in hexadecimal



LAN Switching

- Forward or drop frames ->Based on destination MAC address
- Gather constantly updating list of MAC addresses
  - Builds list based on source MAC address of incoming traffic
  - Age out periodically often in 5 minutes
- Maintain a loop-free environment -> Using a Spanning Tree Protocol (STP)

Switch Learning MAC's



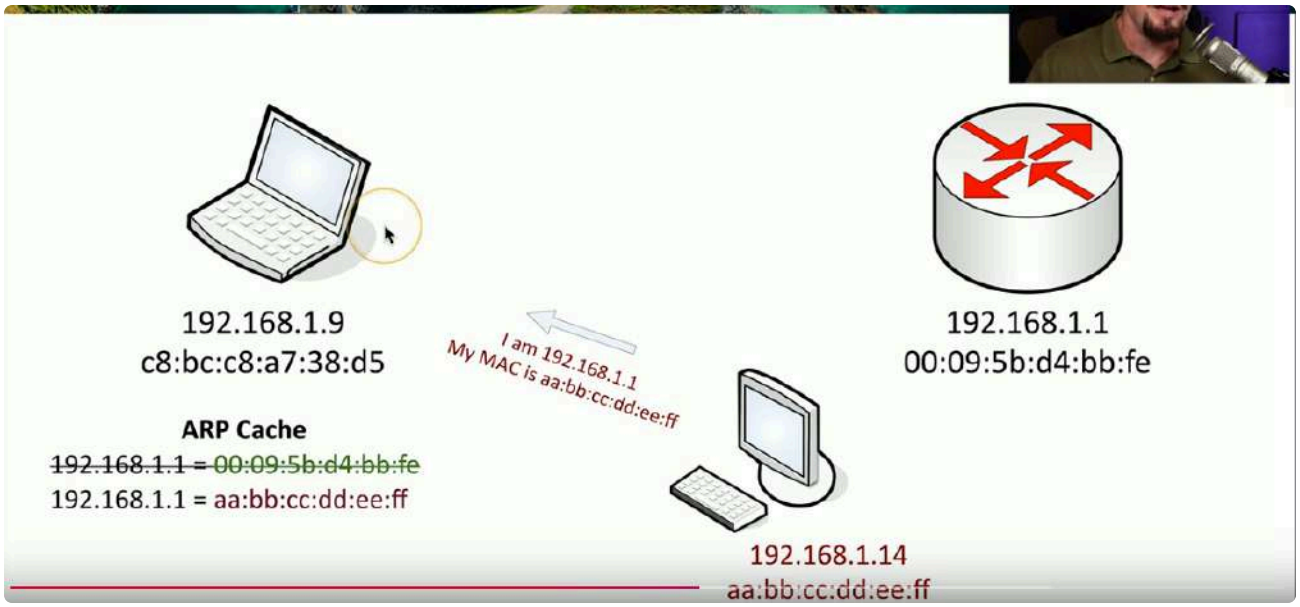
MAC Flooding

- MAC table is only so big
- Attacker starts sending traffic with different source MAC addresses
  - Forcing out legitimate MAC entries
- Table fills up and switch begins flooding traffic to all interfaces
- Effectively turns switch into a hub -> All traffics transmitted to all interfaces
  - No interruption in traffic flaws
- Attacker can easily capture all network traffic
- Flooding can be restricted in the switch's port security settings

4.2 ARP and DNS Poisoning

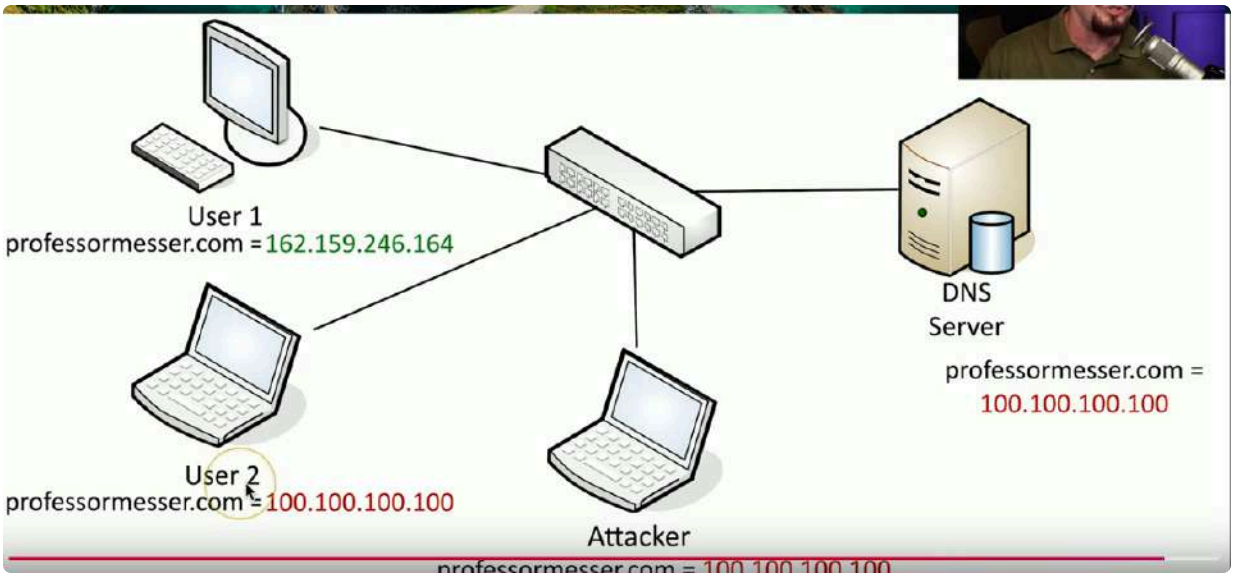
Person pretends to be both end points essentially a man in the middle attack

ARP Poisoning (IP Spoofing)



DNS Poisoning

- Modify the DNS server ->Requires crafty hacking
- Modify the client host file ->Host file takes precedent over DNS queries
- Send a fake response to a valid DNS request
  - Requires redirection of the original request or the resulting response
  - Real time redirection
  - On-Path attack



4.2 Rogue Services

Rogue DHCP Server

- IP address assigned by a non-authorized server ->No inherent security in DHCP
- Client assigned an invalid or duplicate address

    - Intermittent connectivity, no connectivity
- Disable rogue DHCP communication
    - Enable DHCP snooping on your switch
    - Authorized DHCP servers in Active Directory
- Disable the rogue -> Renew the IP leases
  Rogue Access Points
- An unauthorized wireless access point
    - May be added by employee or hacker
    - Significant potential backdoor
- Consider using 802.1X (Network Access Control)
  - Must authenticate regardless of connection type
  Wireless Evil Twins
- Looks legitimate but actually malicious ->Wireless version of phising
- Configure an access point to look like an existing network
    - Same or similar SSID and security settings/captive portal
- Overpower existing access point
- Use HTTPS and a VPN
  On-Path Network Attack
- Formerly known as man in the middle
- Redirects your traffic then passes it on to the destination
- Other on Path attacks
    - Session hijacking
    - HTTPS Spoofing
    - Wi-FI eavesdropping
- Encryption fixes most of these situations

4.2 Social Engineering

Phising

- Social engineering with a touch of spoofing
  Shoulder Surfing
- IRL people peeping into your keystrokes and moves
- Webcam monitoring, binoculars
  Tailgating and Piggybacking
- Uses an authorized person to gain unauthorized access to a building
- Sneaks through when nobody is looking

4.2 Malware

- Malicious software
- Gather information -> Keystrokes and etc
  Types of Malware
- Viruses
- Worms
- Ransomware
- Trojan Horse
- Rootkit
- Keylogger
- Adware/Spyware
- Bloatware
- Logic Bomb

4.3 Device Security

Disable Unnecessary Ports and Services

- Every open port is a possible entry point
  - Closer everything except required ports
- Control access with a firewall ->NGFW would be ideal (New Generation Firewall)
- Use Nmap or similar port scanner to verify->Ongoing monitoring is important
  Change Default Credentials
- Most devices have default user and pass change these
  Port Security
- Prevent unauthorized users from connecting to a switch interface
  - Alert or disable the port
- Based on the source MAC address ->Even if forwarded from somewhere else
  Port Security Operations
- Configure a max number of source MAC addresses on an interface
- You decide how many is too many ->Can also configure specific MAC addresses
- Switch monitors the number of unique MAC addresses
  - Maintains list of every source MAC address
  - Once exceed max port security activates ->Default is to disable interface
  Disabling unused interfaces
- Enabled physical ports ->Conference rooms, break rooms
- Administratively disable unused ports ->More to maintain but more secure

- Network Access Control (NAC) -> 802.1X controls
  - Can't communicate unless authenticated
  MAC Filtering
- Limit access through the physical hardware address -> Keeps neighbors out
  - Additional administration with visitors
- Easy to find working MAC addresses through wireless LAN analysis
  - MAC addresses can be spoofed ->Free open-source software
- Security through obscurity ->If you know the method you can easily defeat it
  Key Management System
- Services are everywhere ->On premises, cloud based
  - Many different keys for many different services
- Manage all keys from a centralized manager
  - Separate the encryption keys from the data
- All key management from one console
  - Create keys for a specific service or cloud provide (SSL/TLS,SSH,etc.)
  - Associate keys with specific users
  - Rotate keys on regular intervals
  - Log key use and important events

4.3 Security Rules

Access Control Lists (ACLs)

- Allow or disallow traffic
  - Grouping of categories
  - Source IP, Destination IP, port number, time of day, application etc
- Restrict access to network devices
  - Limit by IP address or other identifier
- Can be implemented in many ways ->Router,firewall,OS Policies, etc
  Firewall rules
- A logical path ->Usually top to bottom
- Can be very general or very specific ->Specific rules usually at the top
- Implicit deny ->Most firewalls include a deny at the bottom
  - Even if you didn't put one

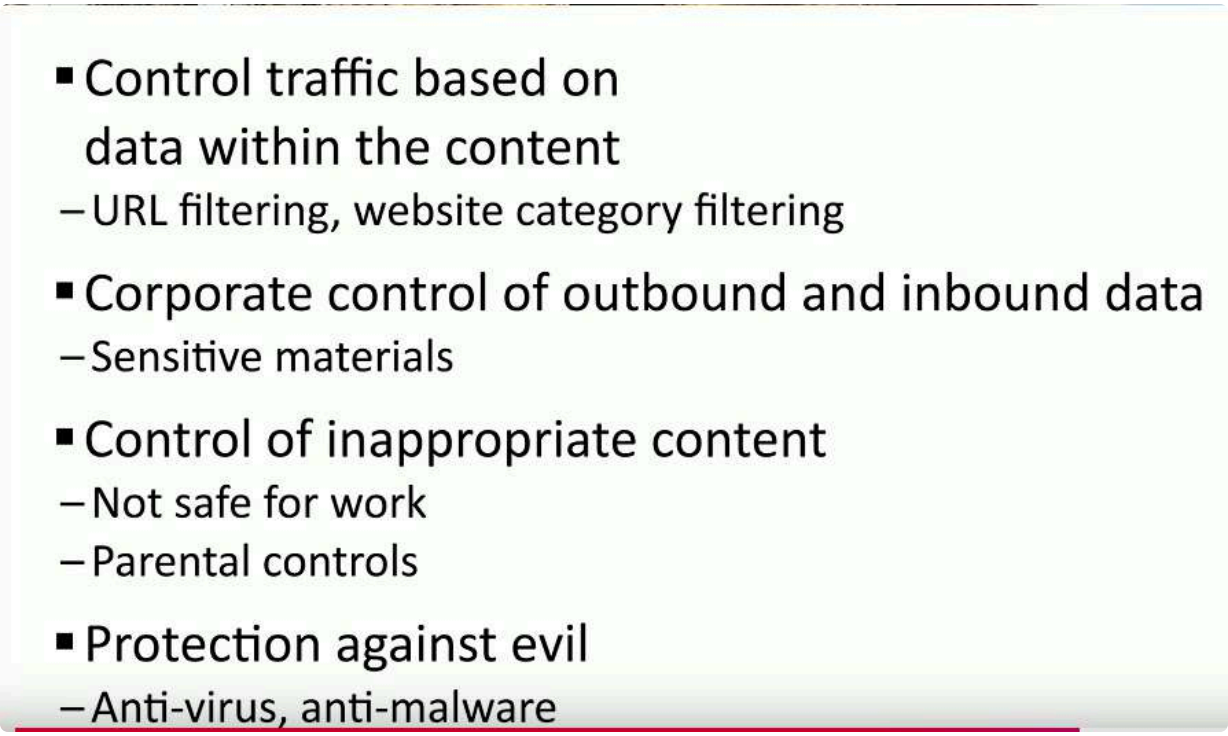
Rule Number	Remote IP	Remote Port	Local Port	Protocol	Action
1	All	Any	22	TCP	Allow
2	All	Any	80	TCP	Allow
3	All	Any	443	TCP	Allow
4	All	Any	3389	TCP	Allow
5	All	53	Any	UDP	Allow
6	All	123	Any	UDP	Allow
7	All			ICMP	Deny

URL Filtering

- Allow or restrict based on Uniform Resource Locator (URL)
  - Allow List/Block List
- Managed by Category ->Auction,Hacking,Malware,Travel etc.
- Can have limited control -> URLs not only way to surf
- Often integrated into an NGFW (New Generation Firewall)

- Filters traffic based on category or specific URL

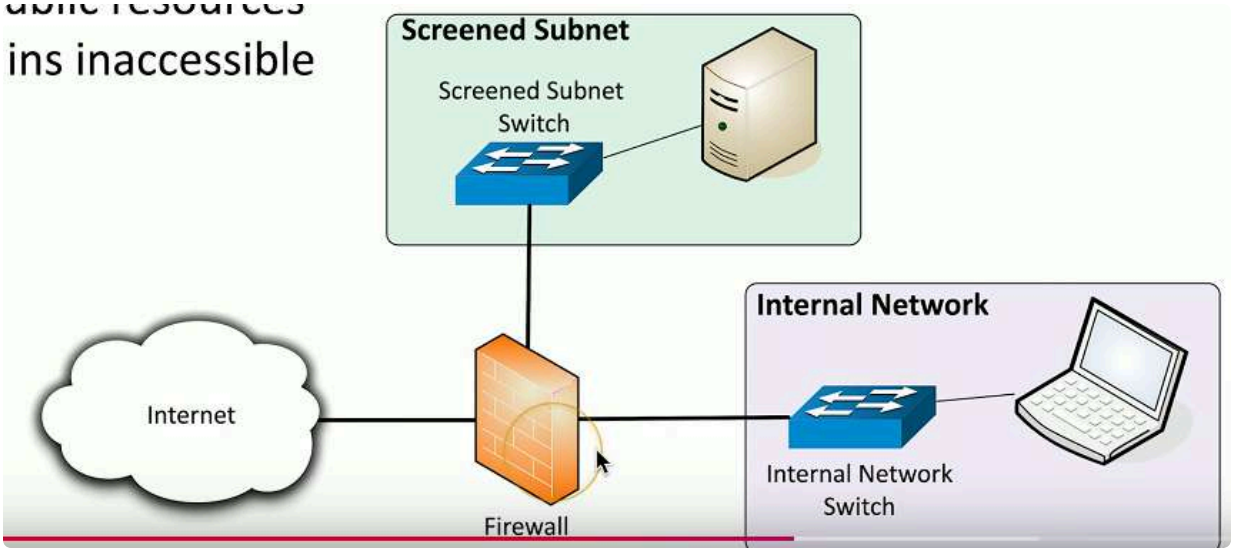
Content Filtering



Screened subnet

- An additional layer of security between you and the Internet
- Public access to public resources

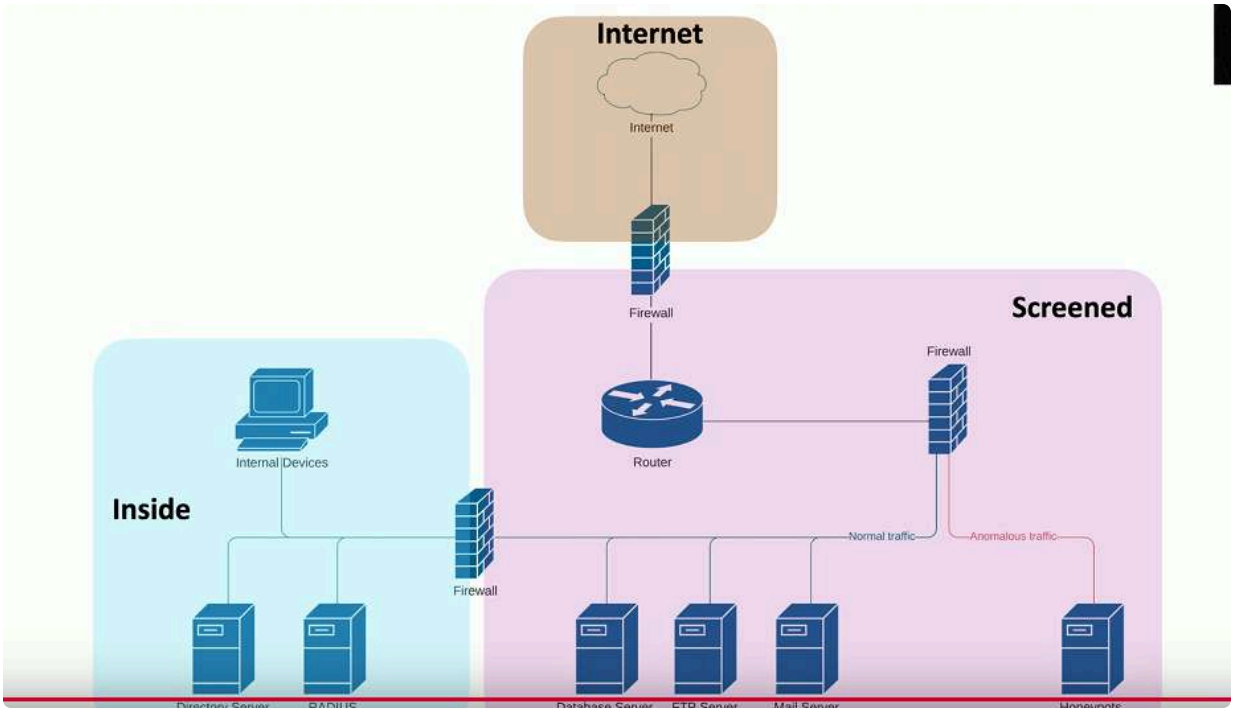
- Private data remains inaccessible



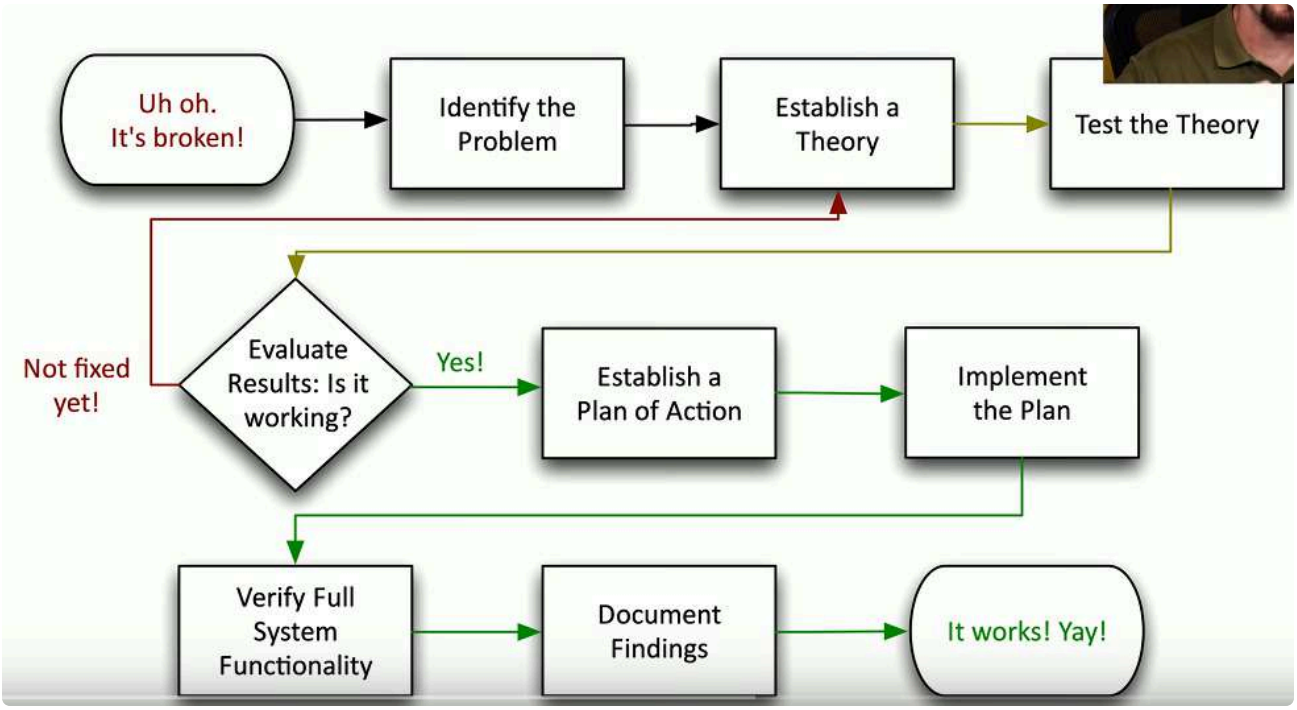
Security Zones

- Zone-based security technologies
  - More flexible and secure than IP address ranges
- Each area of the network associated with a zone
  - Trusted,untrusted
  - Internal, external
  - Inside,Interenet, Servers, Databases, Screened
- Simplifies security policies

  - Trusted to untrusted
  - Untrusted to Screened
  - Untrusted to Trusted



5.1 Network Troubleshooting Methodology



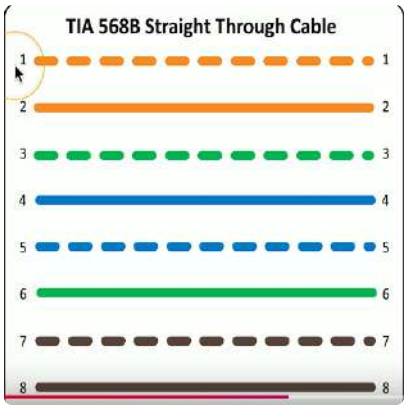
5.2 Cable Issues

Ethernet Standard	Cable Category	Maximum Supported Distance
1000BASE-T	Category 5	100 meters
1000BASE-T	Category 5e (enhanced)	100 meters
10GBASE-T	Category 6	Unshielded: 55 meters Shielded: 100 meters
10GBASE-T	Category 6A (augmented)	100 meters
10GBASE-T	Category 7 (Shielded only)	100 meters
40GBASE-T	Category 8 (Shielded only)	30 meters

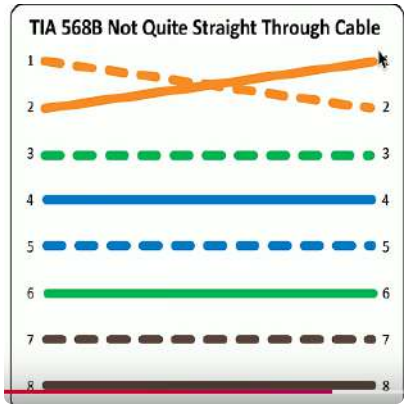
Crosstalk (XT)

- SIgnal on one circuit affects another circuit-> In a bad way

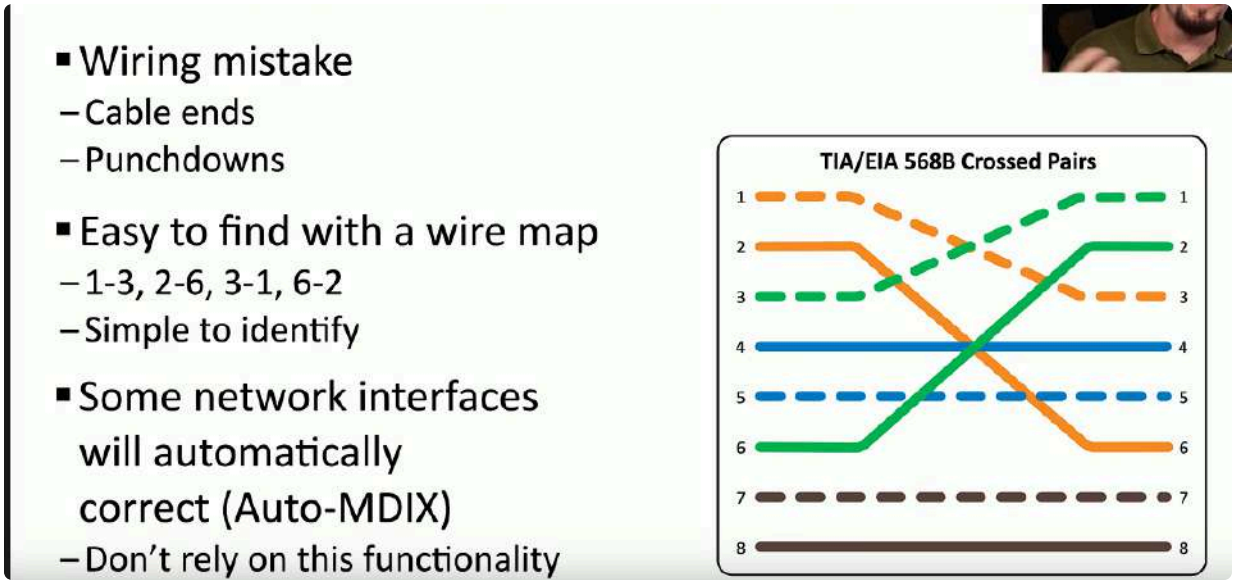
- Leaking of signal ->Can sometimes hear
- Measure XT with cable testers
  Crosstalk Metrix
- Near End Crosstalk (NEXT)
  - Interference measured at the transmitting end ->The near end
- Far End Crosstalk (FEXT)
  - Interference measure at away from the transmitter
- Alien Crosstalk (AXT)
  - Interference from other cables
- Attenuation to Crosstalk Ratio (ACR)
  - Difference between insertion loss and NEXT
  - Signal to Noise Ratio (SNR)
  Troubleshooting crosstalk
- Almost always a wiring issue ->Check your crimp
- Maintain your twists ->Twist helps avoid crosstalk
- Category 6A increases cable diameter->Increased distance between pairs
  Avoiding EMI and interference
- Electromagnetic interference
- Cable handling
  - No twisting->Don't pull or stretch
  - Watch your bend radius
  - Don't use staples, watch your cable ties
- EMI and interference with copper cables
  - Avoid power cords,fluorescent lights, electrical systems and fire prevention components
  Attenuation
- Usually gradual ->Signal strength diminishes over distance
- Loss of signal intensity as signal moves through a medium
  Troubleshooting termination
- Cables can foul up a perfectly good plan
  - Test cables prior to implementation
- Improper termination
  - Near and far pins in cables aren't where they are supposed to be
  - Pin 1 goes to pin 1, pin 2 to pin 2, etc..
  - Error in this may drop connection speed or not connect at all
  Correct:



Wrong:



Reversing Transmit and Receive



5.2 Interface Issues

Monitoring the interface

- Often your first sign of trouble -> Local problems are easy to attack
- Can sometimes indicate a bigger issue
  - Problem with a switch or congestion in network
- Link status

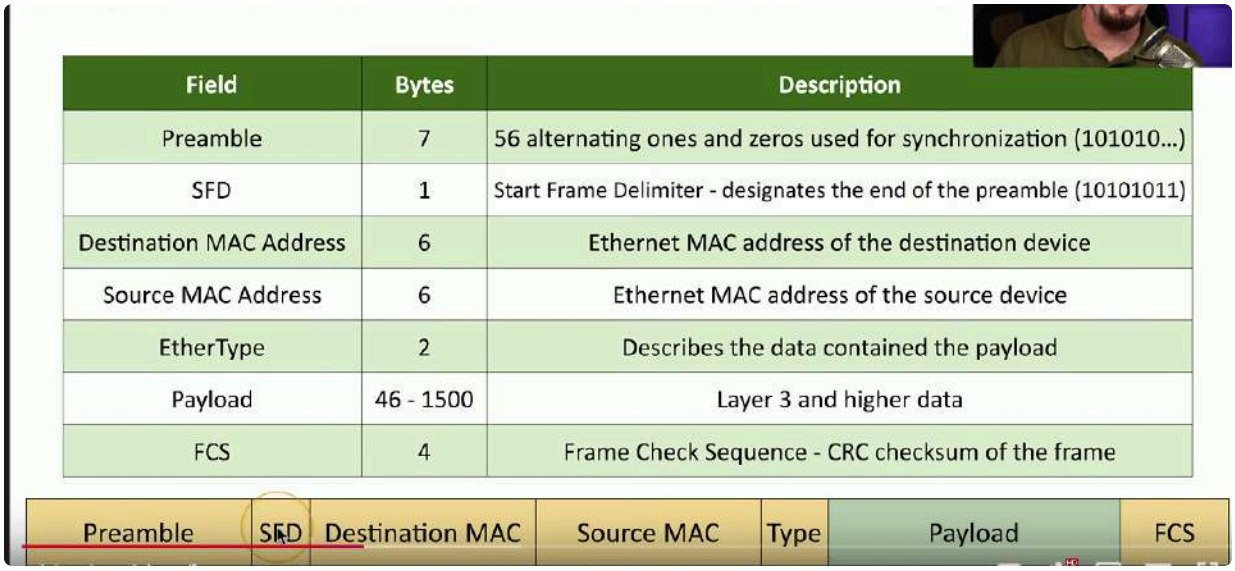
- Link up or link down? May be a problem on the other end of the cable

- Utilization ->Per interface network usage
  - Run bandwidth tests to view throughput
- Error rate

  - Problems with the signal

  - CRC errors, runts, giants, drops

  The Ethernet Frame

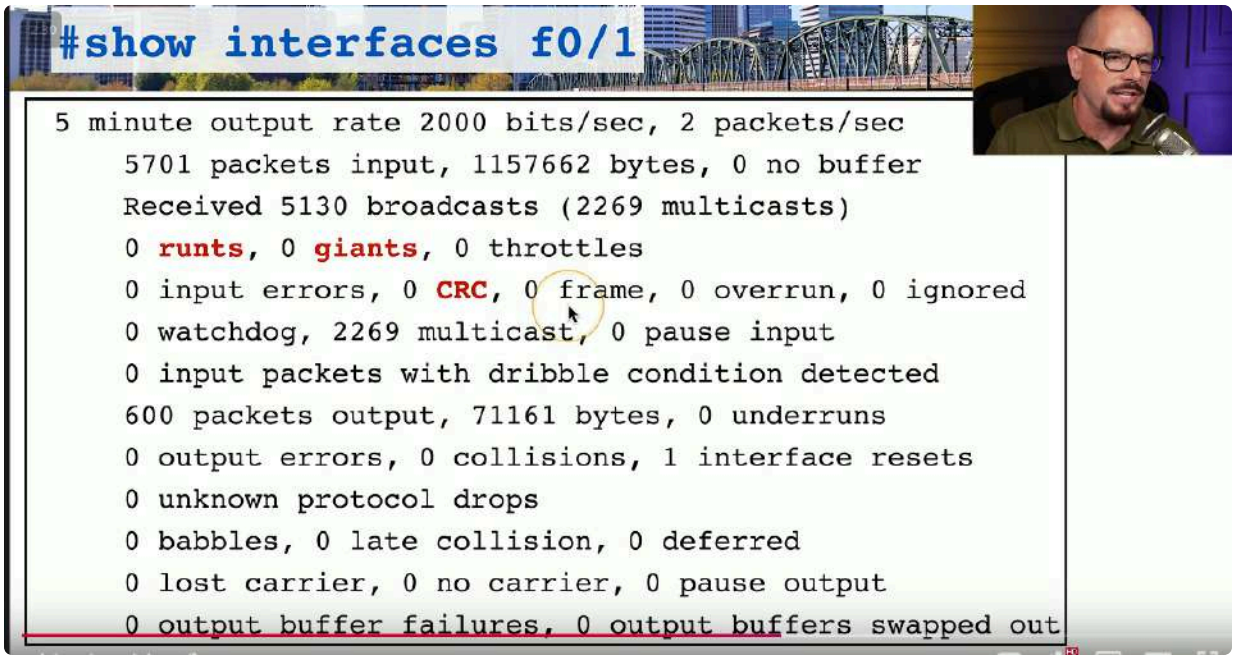


Field	Bytes	Description
Preamble	7	56 alternating ones and zeros used for synchronization (101010...)
SFD	1	Start Frame Delimiter - designates the end of the preamble (10101011)
Destination MAC Address	6	Ethernet MAC address of the destination device
Source MAC Address	6	Ethernet MAC address of the source device
EtherType	2	Describes the data contained the payload
Payload	46 - 1500	Layer 3 and higher data
FCS	4	Frame Check Sequence - CRC checksum of the frame

  Counting The Errors

- CRC (Cyclic Redundancy Check) error detecting
  - Add a frame check sequence to an Ethernet frame
  - Receive the frame, recalculate the CRC and compare to the original
  - Non-matching CRC is an error
- Runts - Frames that are less than 64 bytes ->May be a result of collision
- Giants - Frames that are more than 1518 bytes
  - Or more than the configured maximum frame size
- Drops - Frames not transmitted or received due to contention

  Way to View Errors on Interface



Error Disabled

- Disable automatically after encountering an error
- Many different reasons->Link flapping(up/down), port security violations, etc
- Must be administratively re-enabled ->Intervention is required

Port Status

- Administrative Down
  - The device admin has "turned off" an interface -> This was intentional
  - Does not work again until administratively enabled
- Suspended
  - The configuration is not compatible with the current connection
  - Similar function to "error disabled" but occurs immediately
  - Possible Cause
    - Set LACP(Link Aggregation Control Protocol) on one side but not the other sending device into suspended state

5.2 Hardware Issues

Power over Ethernet (PoE)

- Power provided on an Ethernet cable
  - One wire for both network and electricity
  - Phones, cameras, wireless access points
  - Useful in difficult-to-power areas
- Power provided at the switch
  - Built-in power - Endspans
  - In-line power injector - Midspans

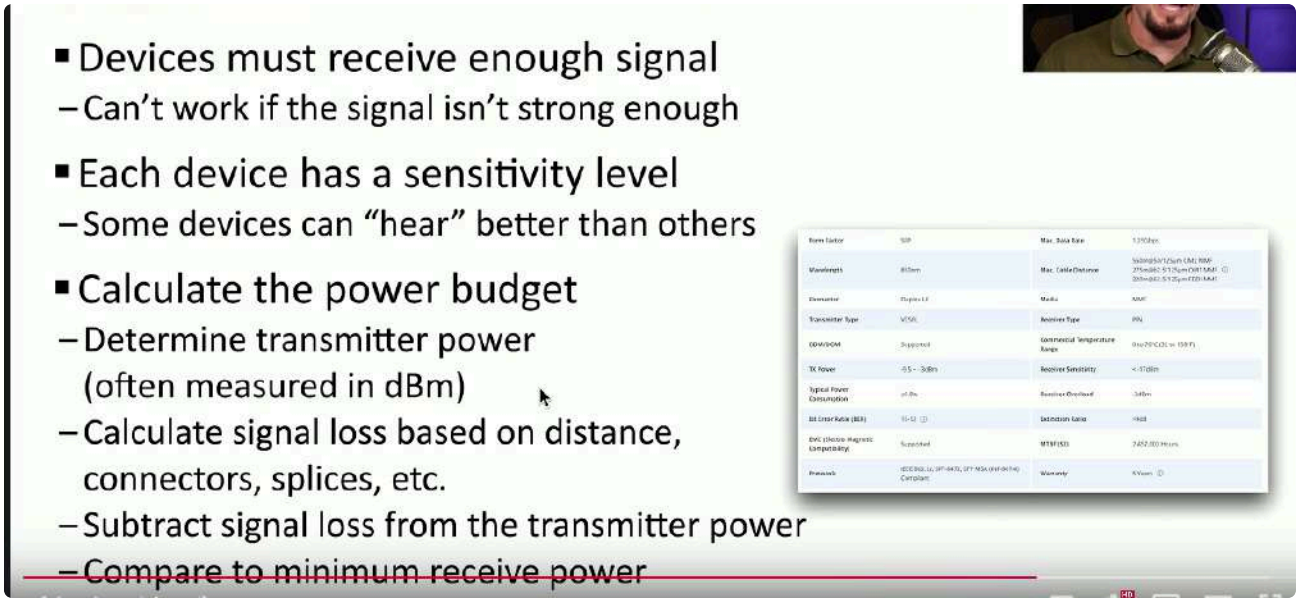
PoE, PoE+, PoE++

- PoE
  - The original PoE specification
  - 15.4 watts DC power, 350 mA max current
- PoE+
  - 25.5 watts DC power, 600 mA max current
- PoE++
  - 51 W (Type 3), 600 mA max current
  - 71.3 W (Type 4), 960 mA max current
  - PoE with 10GBASE-T
- Compare the device with the switch support
  - PoE+ won't power a PoE++ device

Single Mode vs Multimode

- Transceivers have to match the fiber
  - Single mode transceiver connects to single mode fiber
- Transceiver needs to match the wavelength
  - 850nm, 1310nm, etc.
- Use the correct transceivers and optical fiber
  - Check the entire link
- Signal loss
  - Dropped frames, missing frames

Transceiver Signal Strength

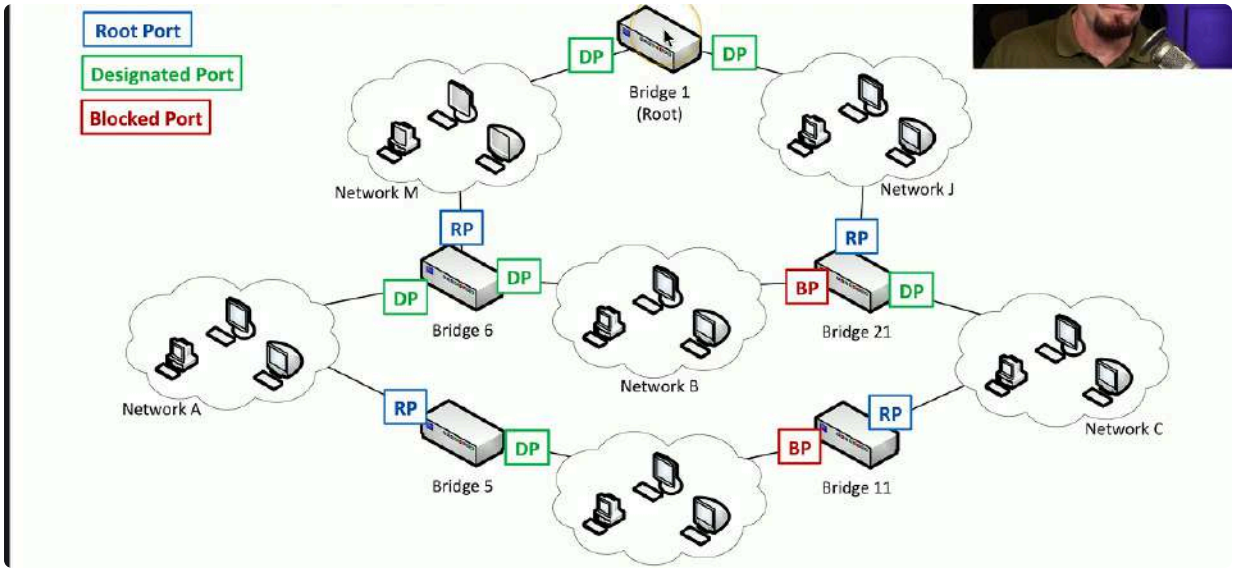


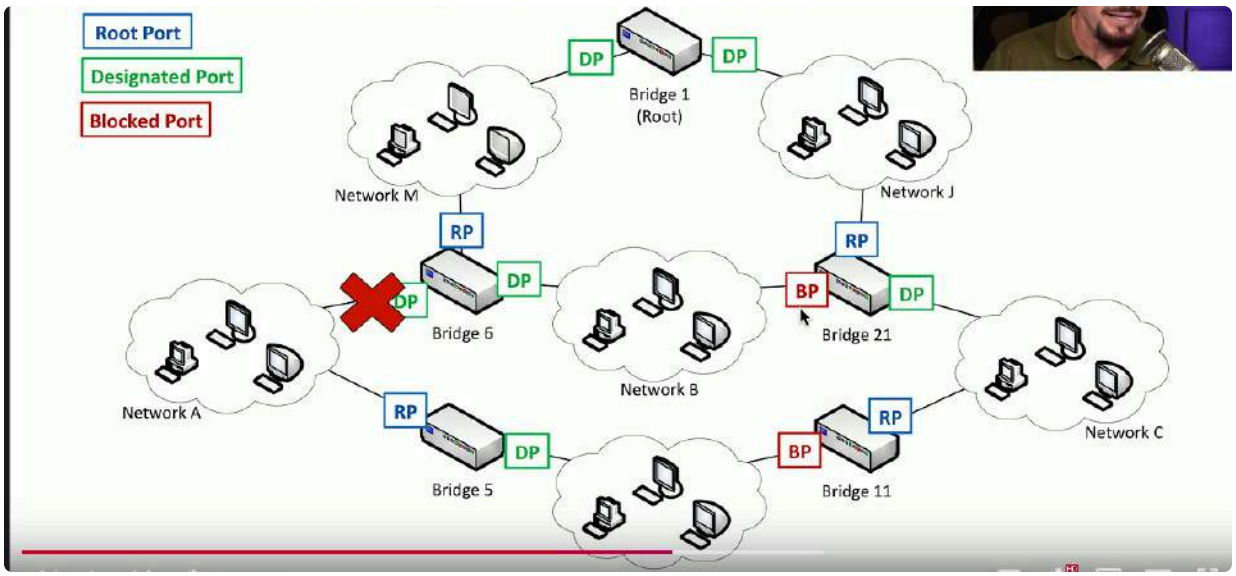
5.3 Switching Issues

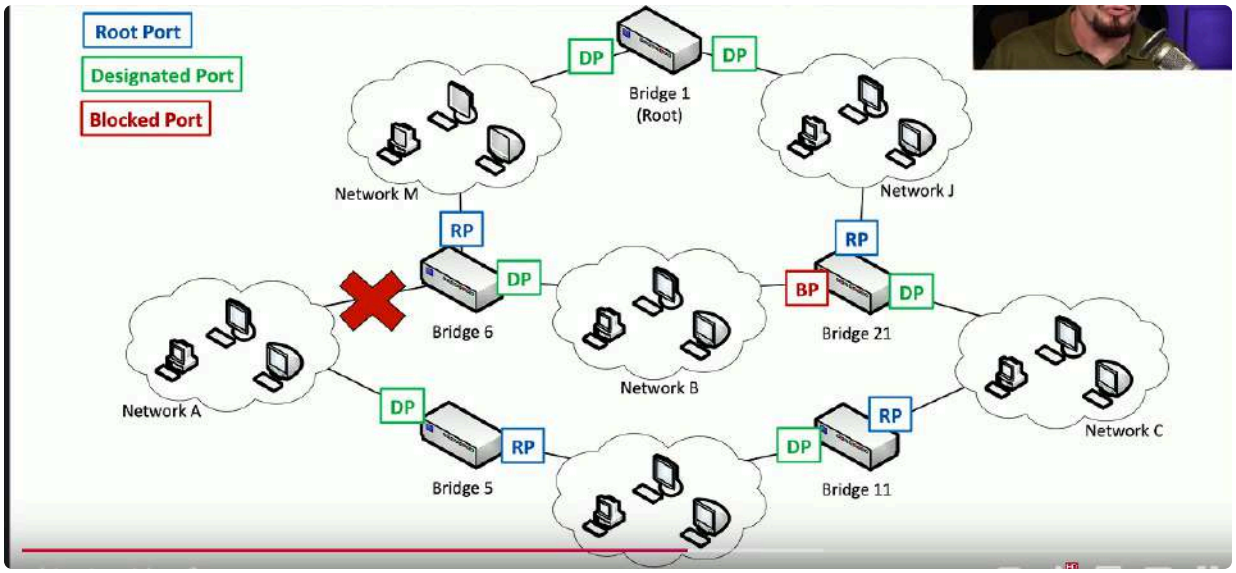
Switching Loops

- A fear of every network admin
  - Spanning Tree Protocol often configured to prevent this
- Broadcasts and multicasts are sent to all
  - Broadcasts repeated to all switch ports
- Nothing at MAC address level to identify loops->IP has TTL(Time to Live)
  Spanning Tree Protocol (STP)
- Bridges are always talking to each other
  - Uses MAC-layer Multicasts
  - Bridge Protocol Data Unit(BPDU)
  - Sends configuration and any topology changes
- Default "hello" interval is 2 seconds
  - Miss three of these and link is considered down
  Root Bridge Selection
- When starting, the bridges elect a root bridge
  - All other bridges choose the best connection to the root
- All bridges/switches are assigned a bridge ID between 0 and 61440
  - Lowest ID = root
  - If there's a tie lowest MAC address number wins

- Each bridge assigns a port role to each interface ->Root,designated or blocked







Spanning Tree Detects the Block at Bridge 6 not allowing Network A to reach Network M and instantly updates its port roles so that Network A can once again reach network M

STP Port States

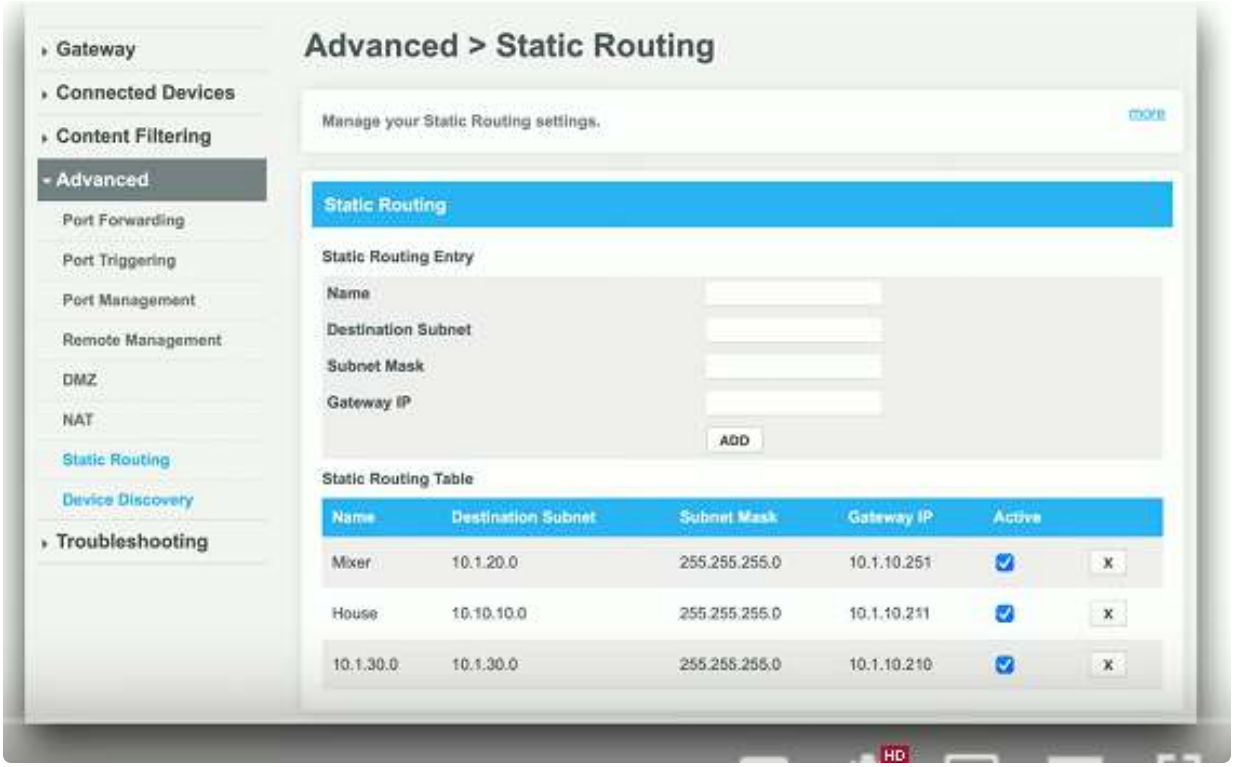
- Blocking/Discarding ->Not forwarding to prevent a loop
- Listening->Not forwarding and cleaning the MAC table
- Learning->Not forwarding and adding to the MAC table
- Forwarding->Data passes through and is fully operational
- Disabled->Administrator has turned off the port
  VLAN Assignment
- Network link is active and IP address is assigned
  - No access to resources or limited functionality
- Every switch interface is configured as an access port or a trunk port
  - Each access port is assigned to a VLAN
- Confirm the specific switch interface ->Check the VLAN assignment
  ACLs Break Perfectly Good Networks
- Clients working ->DHCP is assigning correct IP Addresses->Routing table looks correct
- Packets are still dropping
- Everything could be configured perfectly
  - ACLs would still break the traffic flow
- Always include an ACL check when troubleshooting
  ACL Best Practices
- More granular rules should be first
  - Very similar to firewall
  - The ACL stops evaluating after a mtch
  - Broader rules at the top would prevent more specific rules from firing
- Best practice: Before editing an ACL, disable on an interface
  - Adding an access list without any rules will filter all traffic
    - ACLs deny all by default

5.3 Routing and IP Issues

Routing tables

- Digital version of asking for directions
  - Know how to get from point A to B
- Can answer questions like:
  - Default gateway
  - Manually configured static routes

- Know which way data will flow ->Network Map might help
- Refer to every router ->Routing loops and missing routes are common



Missing Route

- A route to the destination network does not exist ->Packet will be dropped
- ICMP host unreachable message will be sent to source address
  - Source device will be informed of error

  Gateway of Last Resort
- Destination IP has to match a routing table entry
  - If not its dropped
- Adding a static default route can simplify your routing table
  - If it doesn't match an entry use this route
- Add in global router configuration
  - Create a route to 0.0.0.0/0

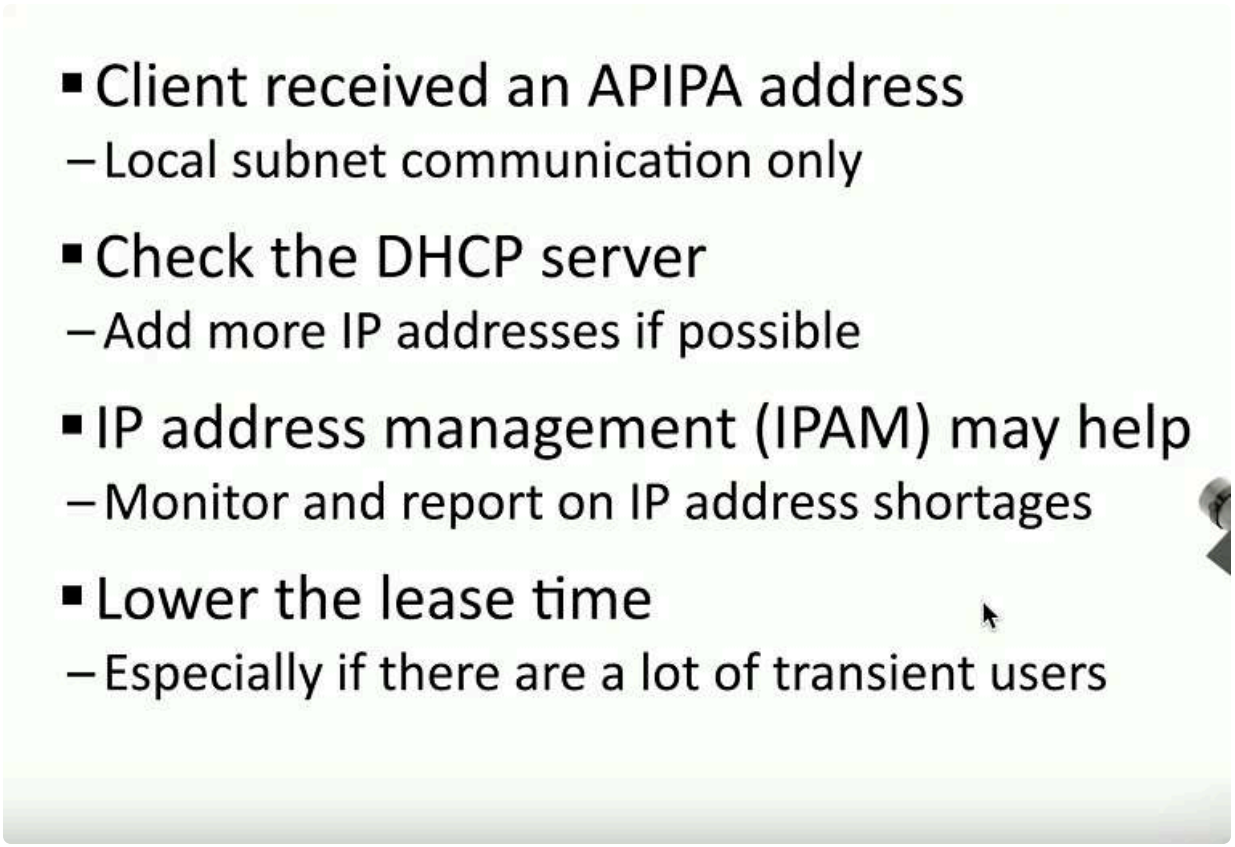
```
Router1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BG
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.50.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C       10.10.10.0/24 is directly connected, GigabitEthernet0/0
L       10.10.10.1/32 is directly connected, GigabitEthernet0/0
S       10.10.20.0/24 [1/0] via 10.10.40.2
R       10.10.30.0/24 [120/1] via 10.10.50.2, 00:00:22, Serial0/3/1
C       10.10.40.0/24 is directly connected, Serial0/3/0
L       10.10.40.1/32 is directly connected, Serial0/3/0
C       10.10.50.0/24 is directly connected, Serial0/3/1
L       10.10.50.1/32 is directly connected, Serial0/3/1
S*   0.0.0.0/0 [1/0] via 10.10.50.2
```

Gateway of Last Resort set by: S* 0.0.0.0/0 [1/0] via 10.10.50.2

Address Pool Exhaustion



Duplicate IP Addresses

- Static address assignments ->Must be very organized or can cause issues quick
- DHCP isn't a panacea (remedy for all problems)
  - Static IP Addressing
  - Multiple DHCP servers overlap
  - Rogue DHCP servers

- Intermittent connectivity
  - Two addressed "fight" with each other
- Blocked by the OS ->Checks when it starts

5.4 Performance Issues

Bottlenecks

- There's never just one performance metric ->Series of technologies working together
- I/O bus, CPU speed, storage access speed, WAN bandwidth, local network speeds etc
  - One of these can slow all the others down.
- You must monitor all of them to find the slowest one

  Bandwidth Usage
- The fundamental network statistic ->Amount of network use over time
- May also wanna measure:
  - Throughput->Amount of data successfully transferred through the network
- Many different ways to monitor:

  - SNMP,NetFlow,sFlow,IPFIX,Protocol analysis, Software agent

  Latency
- A delay between request and response -> Waiting Time

  Packet Loss
- Discard,packet drops
  - No errors in the packet but system could not transmit or receive the data
- Packets are lost ->Corrupted during transmission->Dropped after validation
- Data must be retransmitted->Overall communication is delayed

  - Uses additional resources

  Jitter
- Most real time media is sensitive to delay
  - Data should arrive at regular intervals
  - Voice communication, live video
- If you miss a packet no retransmission ->No time to rewind your call
- Jitter is the time between frames ->Excessive jitter can cause "choppy" calls
  - Ideally want uniform Jitter, with small delay between packets

5.4 Wireless Issues

Client Disassociation Issues

- A denial of service attack

    - Takes advantage of older 802.11 management frame transmission
- Device keeps dropping from the wireless network or never connects
- Disassociation frames can be clearly seen in a packet capture
    - Grab the 802.11 frame information with wireshark
- Remove device performing the disassociation or upgrade to new 802.11 standard
  https://www.youtube.com/watch?v=UO3G_OJhBS4&list=PLG49S3nxzAnl_tQe3kvnmeMid0mjF8Le8&index=83

5.5 Software Tools

Protocol Analyzers

- Solve complex application issues ->Get into details
- Gathers frames on the network ->Or in the air
    - Sometimes built into device
- Ex: Wireshark
- View traffic patterns ->Identify unknown traffic->Verify packet filtering and security controls

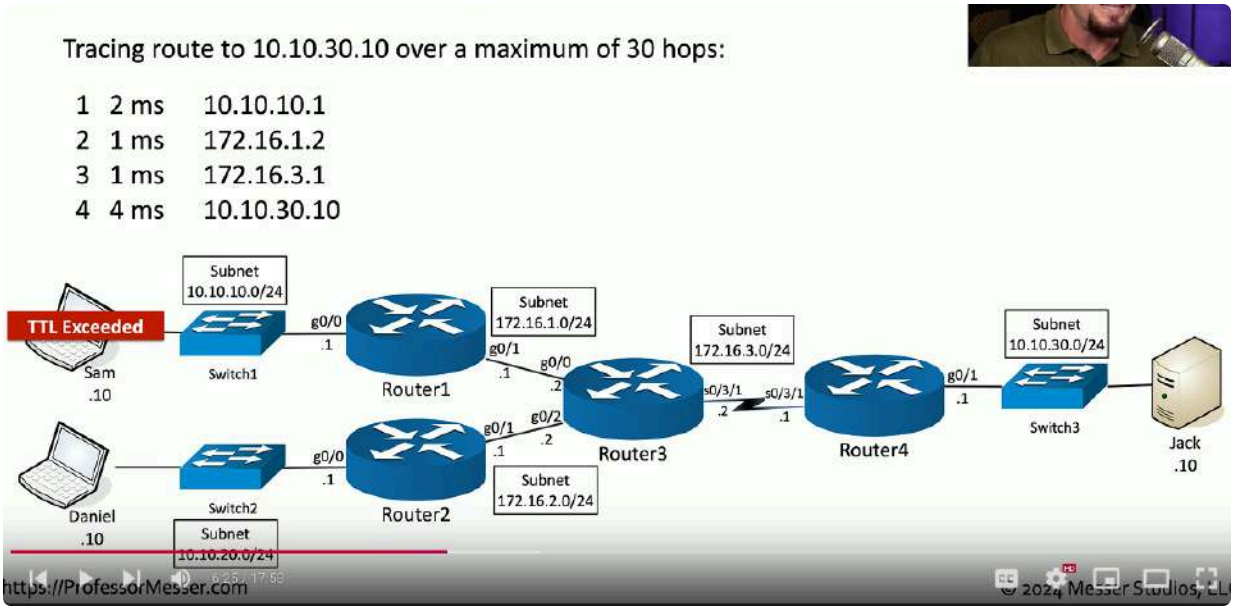
  Nmap
- Network mapper
    - Find and learn more about network devices
- Port scan
    - Find devices and identify open ports
- OS Scan and Service Scan + Additional Scripting Engine
- Active -scan for IP addresses and open ports
- Pick a range of IP addresses ->See who responds to scan
- Rogue system detection ->Hard to hide from a layer 2 ARP

  Discovering Network Devices
- Switched networks can be a challenge->Many different interfaces
    - Each interface can have a very different configuration
    - Identify the port number, MAC address, VLAN ID, etc.
- Can use CDP - Cisco Discovery Protocol
- LLDP - Link Layer Discovery Protocol
    - Vendor neutral, more common discovery method

5.5 Command Line Tools

ping

- Test reachability ->Determine round-trip time ->Uses ICMP
  - Internet Control Message Protocol
  traceroute
- Determine the route a packet takes to a destination
  - Map the entire path
  - tracert(windows) or traceroute(Unix/Linux/MacOS)
- Takes advantage of ICMP Time to LIve Exceeded error message
  - TTL refers to hops not seconds or minutes when using IP
  - TTL=1 is the first router, TTL=2 is the second router etc.
- Not all devices reply with ICMP Time Exceeded messages
  - Some firewalls filter ICMP
  - ICMP is low priority in many devices

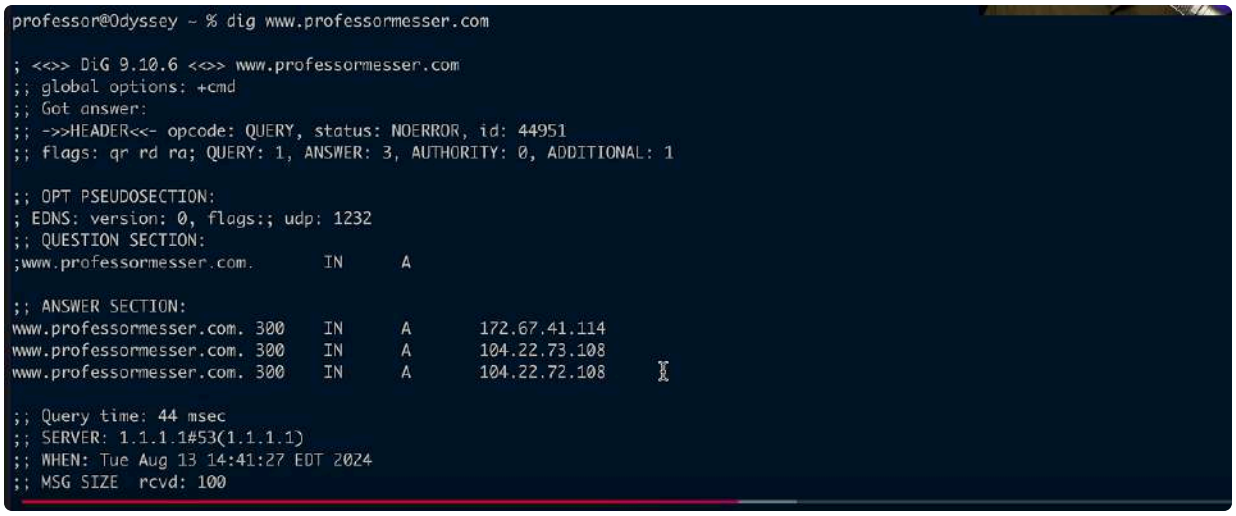



```
professor@Odyssey ~ % traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 64 hops max, 52 byte packets
 1  10.1.10.1 (10.1.10.1)  4.425 ms  2.265 ms  0.963 ms
 2  96.120.58.137 (96.120.58.137)  10.129 ms  9.254 ms  9.102 ms
 3  96.110.208.117 (96.110.208.117)  9.154 ms  10.026 ms  9.202 ms
 4  ae-11-ar01.mckeithen.fl.tallah.comcast.net (68.85.236.65)  10.164 ms  9.782 ms  12.268 ms
 5  be-33666-cr02.dallas.tx.ibone.comcast.net (68.86.90.221)  30.559 ms  29.703 ms  29.966 ms
 6  be-12495-pe03.1950stemmons.tx.ibone.comcast.net (68.86.85.194)  30.034 ms  29.930 ms  28.873 ms
 7  as15169-2-c.111eighthave.ny.ibone.comcast.net (23.30.206.126)  28.636 ms
    66.208.232.42 (66.208.232.42)  28.496 ms  234.191 ms
 8  * * 108.170.252.161 (108.170.252.161)  29.805 ms
 9  172.253.78.227 (172.253.78.227)  29.101 ms
    72.14.236.139 (72.14.236.139)  29.017 ms
    108.170.226.57 (108.170.226.57)  28.643 ms
10  dns.google (8.8.8.8)  28.444 ms  28.097 ms  29.291 ms
professor@Odyssey ~ %
```

In traceroute command above we can see the 10 routers mapped from 1 to 10 as well as their IP's until we eventually reached our wanted 8.8.8.8 destination

nslookup and dig

- Lookup information from DNS servers
  - Canonical names, IP addresses, cache timers, etc
- nslookup is deprecated use dig instead
- dig (Domain Information Groper)
  - More advanced domain information



tcpdump

- Capture packets from the command line ->Very convenient
- Apply filters, view in real time
- Save the date use in another application ->Written in standard pcap format

netstat

- Network statistics ->Many different operating systems
- netstat -a ->Show all active connections
- netstat -b ->Show binaries (Windows)
- netstat -n ->Do not resolve names

ipconfig/ifconfig/ip

- Ping your local router/gateway
- Determine TCP/IP and network adapter information
- ipconfig -> Windows TCP/IP config | ifconfig -> Linux interface config
- ip address -> The latest Linux utility

arp -a

- Determine a MAC address based on an IP address
- arp-a ->View local ARP table

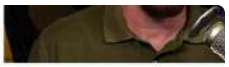
5.5 Hardware Tools

Tone Generator

- Where does that wire go?
  - Follow the tone
- Tone generator
  - Puts an analog sound on the wire
- Inductive probe
  - Doesn't need to touch the copper
  - Hear through a small speaker

- Easy wire tracing
  - Even in complex environments
- Connect the tone generator to the wire
  - Modular jack
  - Coax
  - Punch down connectors
- Use the probe to locate the sound
  - The two-tone sound is easy to find

Cable Testers

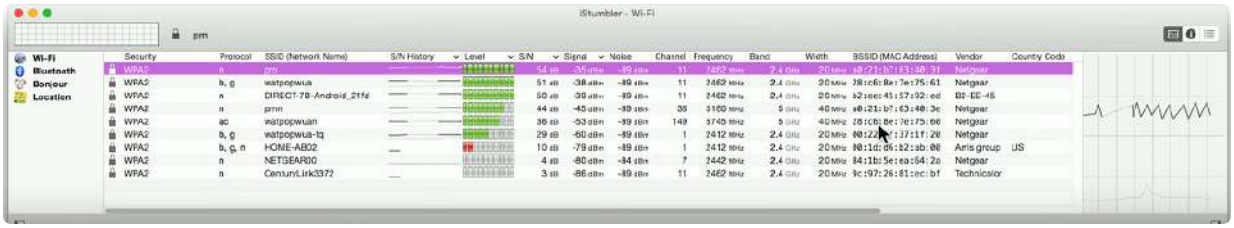


- Relatively simple
  - Continuity test
  - A simple wire map
- Can identify missing pins
  - Or crossed wires
- Not usually used for frequency testing
  - Crosstalk, signal loss, etc.

Taps and Port Mirrors

- Intercept network traffic
  - Send a copy to a packet capture device
- Physical taps ->Disconnect the link, put a tap in the middle
  - Can be an active or passive tap
- Port Mirror
  - Port redirection, SPAN (Switched Port Analyzer)
  - Software-based tap
  - Limited functionality but can work well in a pinch

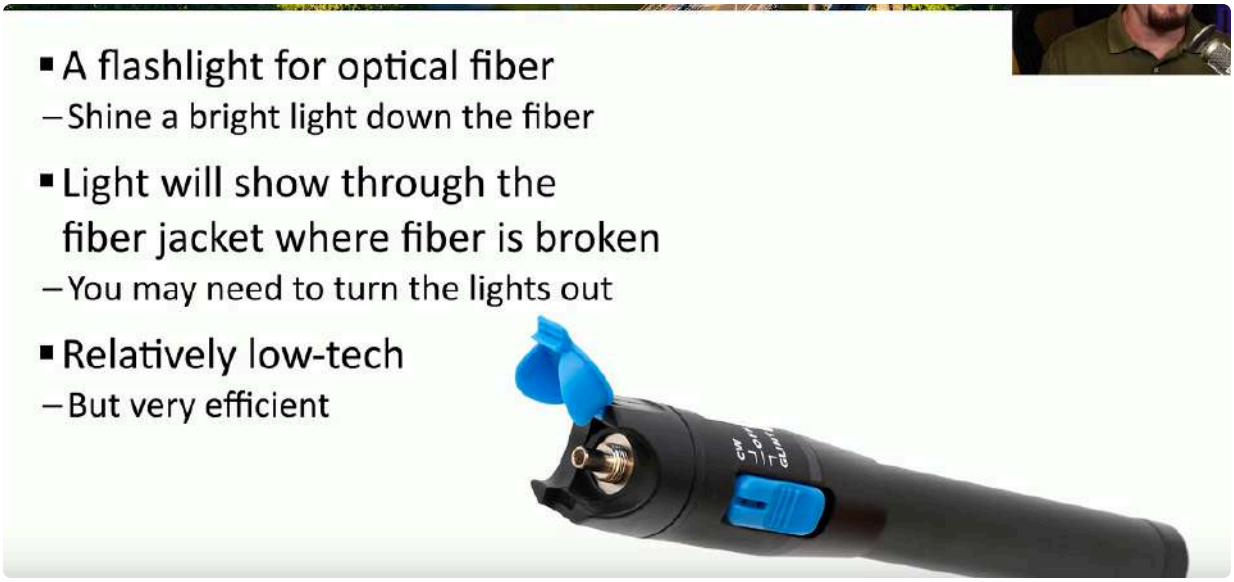
  Wireless Survey Tools
- Signal Coverage
- Potential interference
- Built in tools or 3rd-party tools



Wi-Fi Analyzer

- Hardware-based Wi-Fi analysis
  - Avoids OS limitations
  - View all of 802.11 information in the air
- View information like: Frequencies/channels,signal strength,access points, interference, wireless devices
- Get frequency information from a spectrum analyzer
  - Useful when many different devices part of bigger picture

  Visual Fault Locator



5.5 Basic Network Device Commands

show mac-address-table

- All switches maintain a MAC address table
- Switch forwarding uses this table -> This MAC address is connected to this interface

```
Switch>show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.9748.1e23    DYNAMIC     Fa0/1
   1    0002.16c9.387c    DYNAMIC     Fa6/1
   1    0003.e489.7495    DYNAMIC     Fa8/1
   1    0006.2a41.44be    DYNAMIC     Fa3/1
   1    000a.41de.e134    DYNAMIC     Fa2/1
   1    0050.0f4c.ded3    DYNAMIC     Fa9/1
```

show route

- Routers maintain a list of next hops ->The routing table
- View the current routing table
  - Dynamic routes can change
  - Static routes must be manually configured
- Use list to find errors in routes

  - Or use table to manually determine the next hop

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    1.0.0.0/8 [120/1] via 20.20.0.2, 00:00:22, Serial3/0
C    10.0.0.0/8 is directly connected, Serial2/0
C    20.0.0.0/8 is directly connected, Serial3/0
R    128.168.0.0/16 [120/1] via 20.20.0.2, 00:00:22, Serial3/0
R    192.168.1.0/24 [120/1] via 10.10.0.1, 00:00:26, Serial2/0
R    192.168.2.0/24 [120/1] via 10.10.0.1, 00:00:26, Serial2/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet1/0

Router#
```

show interface

- The status of an interface
  - Up,down,connected,disabled,speed,duplex etc.
- Identify Errors
  - Problems with interface, CRC errors, drops,input and output errors
- View overall performance

  - Total frames, broadcasts, queue capacity

```
Router#show interfaces FastEthernet 0/0
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0090.2bdb.2a22 (bia 0090.2bdb.2a22)
  Internet address is 192.168.3.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 100Mb/s, media type is RJ45
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 50 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     172 packets output, 28740 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

show config

- Every device has a configuration -> View the device settings
- Display the currently running config

  - Or configuration settings stored on the device ->Everything in one place

```
Router#show running-config
Building configuration...

Current configuration : 830 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
ip cef
no ipv6 cef
!
interface FastEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 192.168.4.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial2/0
 ip address 10.10.0.2 255.0.0.0
!
interface Serial3/0
 ip address 20.20.0.1 255.0.0.0
!
```

show arp

- View ARP protocol information
  - Address Resolution Protocol
- Useful when troubleshooting connectivity

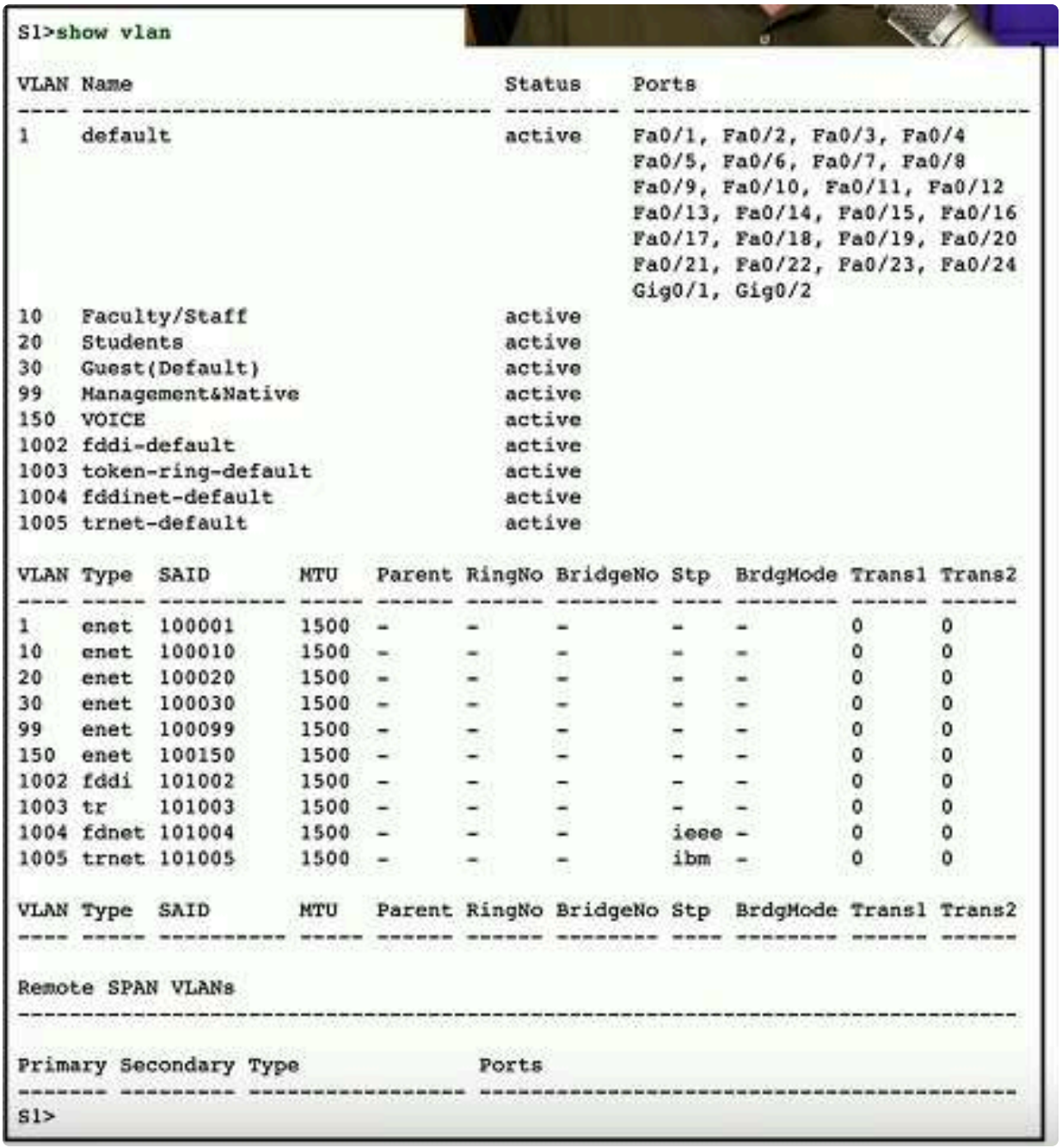
  - Do we see the MAC address associated with an IP address?

```
Router>show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.20.1.1             -   0002.4ADA.0558  ARPA   FastEthernet4/0
Internet  172.20.1.2             2   0000.0C36.315D  ARPA   FastEthernet4/0
Internet  192.168.1.1            -   00D0.BA64.88D1  ARPA   FastEthernet0/0
```

show vlan

- View the VLANs associated with switch interfaces
- Virtual Local Area Network ID
- View default VLAN ID and assigned VLAN ID numbers

  - Confirm assignment for each interface



```
S1>show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   Faculty/Staff                     active
20   Students                          active
30   Guest(Default)                    active
99   Management&Native                 active
150  VOICE                             active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0
150  enet  100150     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
S1>
```

show power

- Display power-related information
  - Power supply status, Power over Ethernet usage
- Monitor power usage->Available,used and remaining power

- Manage PoE devices->Plan for future PoE Devices and troubleshoot power issues

```
Switch#show power inline
Available:370.0(w)  Used:40.0(w)  Remaining:330.0(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa0/1     auto   off        0.0     n/a                 n/a   15.4
Fa0/2     auto   on         10.0    IP Phone 7960       3     15.4
Fa0/3     auto   on         10.0    IP Phone 7960       3     15.4
Fa0/4     auto   on         10.0    IP Phone 7960       3     15.4
Fa0/5     auto   on         10.0    IP Phone 7960       3     15.4
Fa0/6     auto   off        0.0     n/a                 n/a   15.4
Fa0/7     auto   off        0.0     n/a                 n/a   15.4
Fa0/8     auto   off        0.0     n/a                 n/a   15.4
Fa0/9     auto   off        0.0     n/a                 n/a   15.4
Fa0/10    auto   off        0.0     n/a                 n/a   15.4
Fa0/11    auto   off        0.0     n/a                 n/a   15.4
Fa0/12    auto   off        0.0     n/a                 n/a   15.4
```

References

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