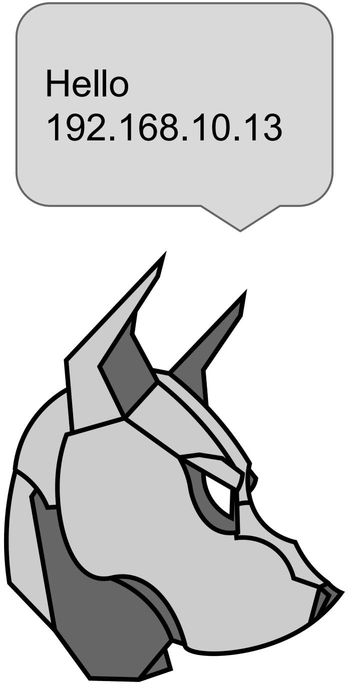
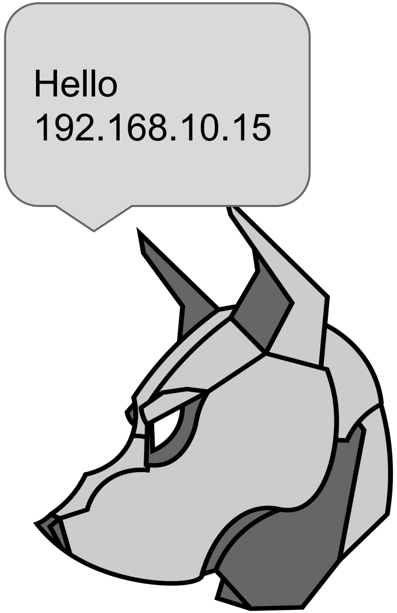
Cyber Defense Organization



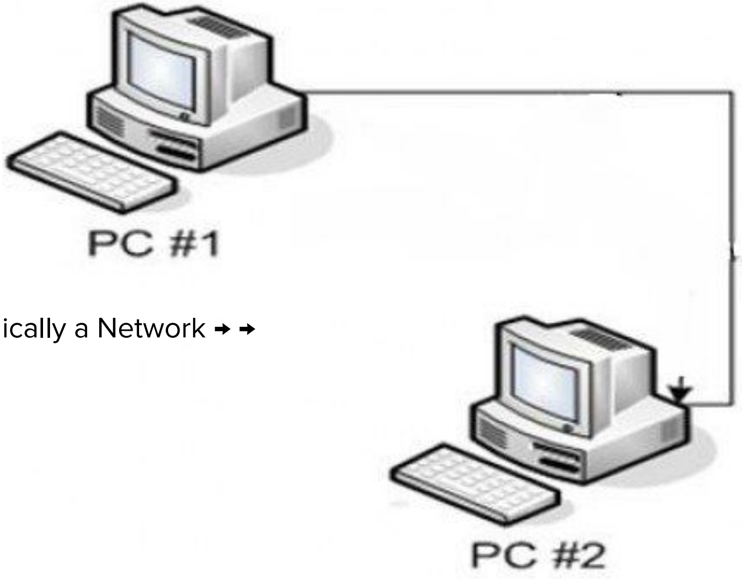
Fall 2019 - Networking



What is a Network?

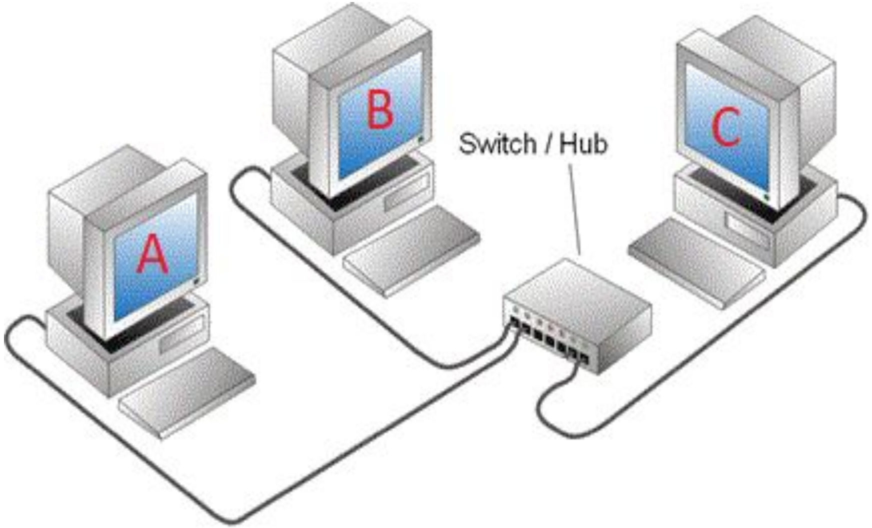
- A Network is 2+ nodes communicating with each other
- A node can be…
  - A computer
  - A phone
  - A printer
  - Etc.
- As long as 2 devices are connected via someway, could be a simple wire of wifi, that is a network!
- But what if you want more than 2 nodes…

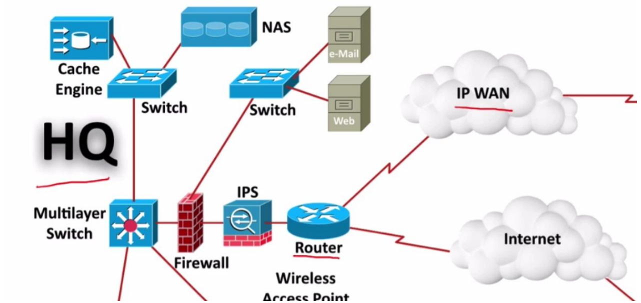
Technically a Network → →



Routers v Hubs v Switches

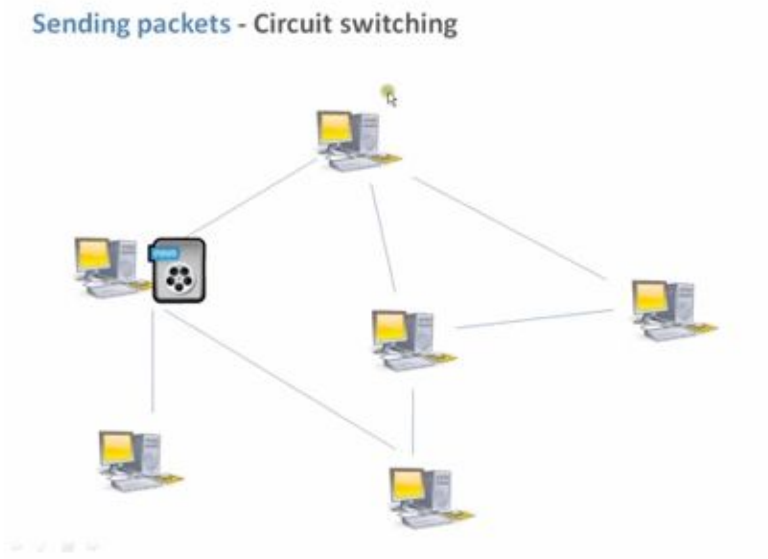
- Routers, Hubs, and Switches serve similar purposes....
- **Switches** are simple devices that use MAC addresses to communicate.
- **Hubs** are generally not used anymore… simple like switches, but don't care about MAC addresses
  - They replicate the data and send it to all nodes
- **Routers** are like a more advanced switch that uses IP addresses instead of MAC
  - Can be used to connect out to the internet





Packets and Encapsulation

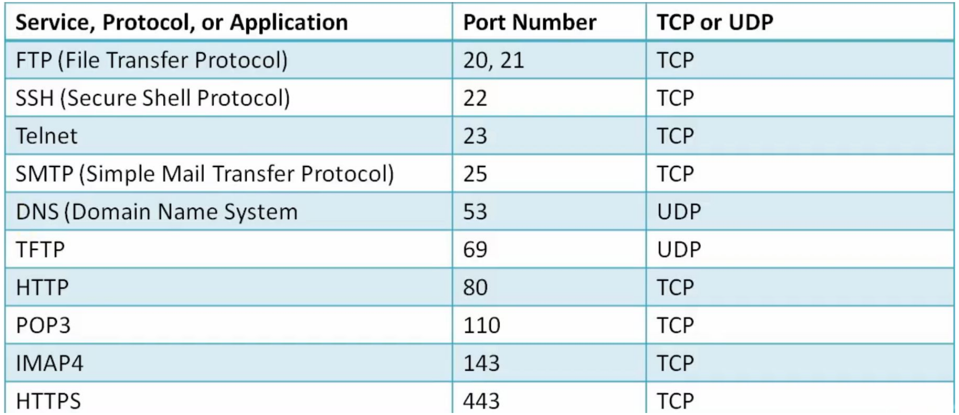
- The info sent across networks are called **Packets**
- They need to be disassembled and reassembled when they reach the target destination
    - This is done for efficiency and not to overload the traffic
- **Encapsulation** is what you do if you need to transfer packets from one IP Protocol to another IP Protocol



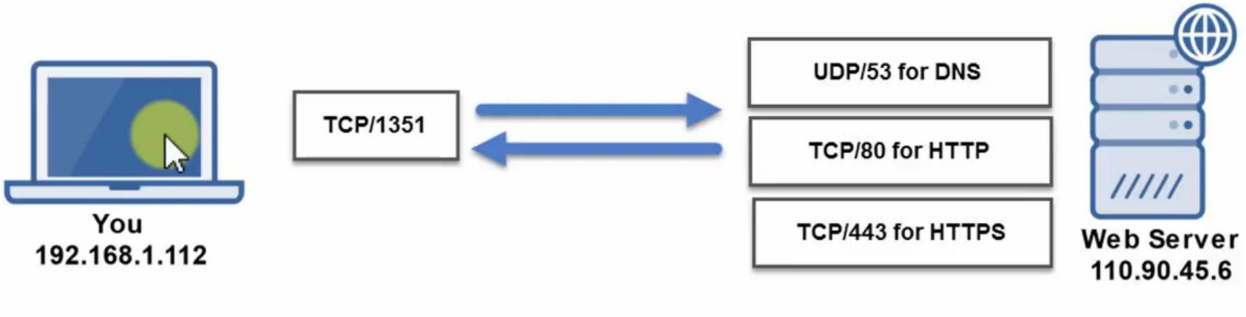
Sending packets - Circuit switching

IP Protocols and Ports

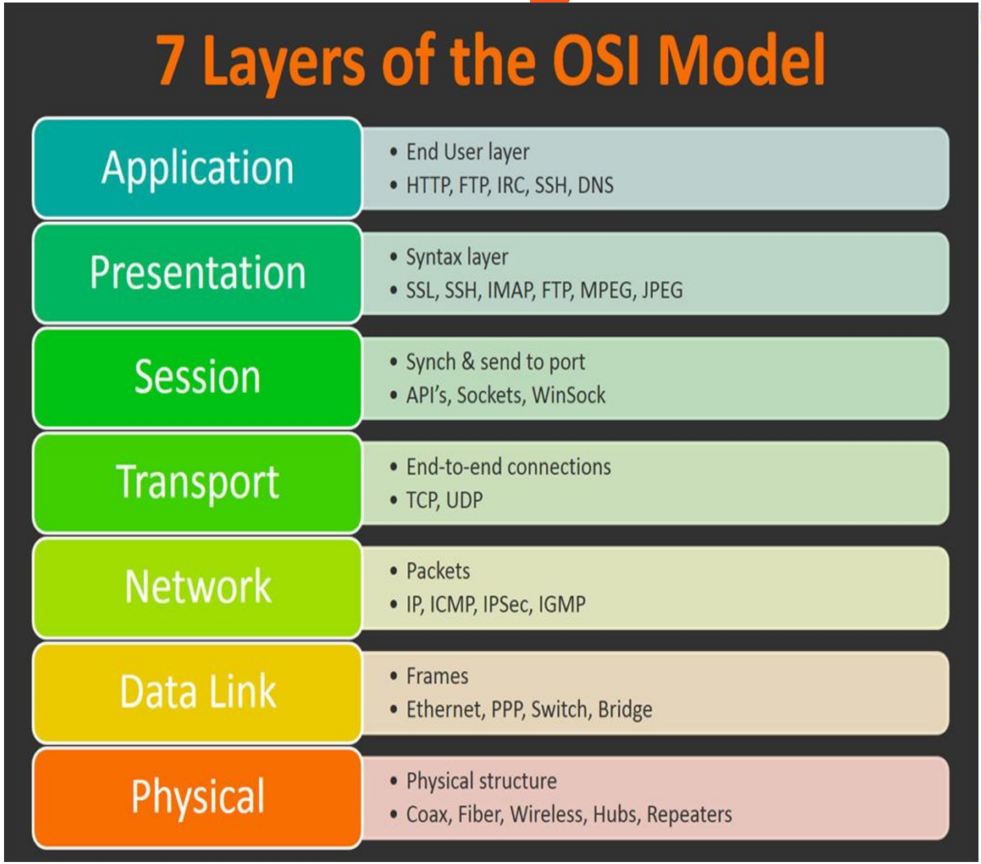
- **IP Protocols** is how the internet communications
  - IP stands for Internet Protocols
- Ports allow your computer to multitask.
- If you have multiple things going, such as email, FTP, and an internet browser, and they all want to communicate with your IP address rather than have them all wait in line they each have their own channel of communication.



Service, Protocol, or Application	Port Number	TCP or UDP
FTP (File Transfer Protocol)	20, 21	TCP
SSH (Secure Shell Protocol)	22	TCP
Telnet	23	TCP
SMTP (Simple Mail Transfer Protocol)	25	TCP
DNS (Domain Name System	53	UDP
TFTP	69	UDP
HTTP	80	TCP
POP3	110	TCP
IMAP4	143	TCP
HTTPS	443	TCP

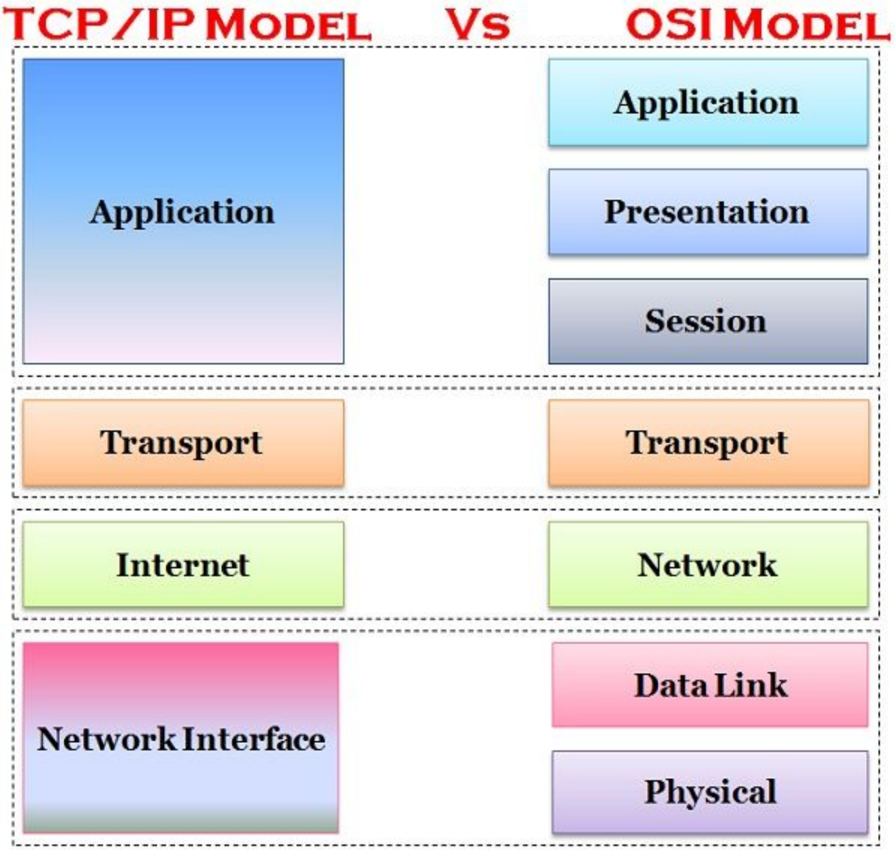


Networking Models



7 Layers of the OSI Model

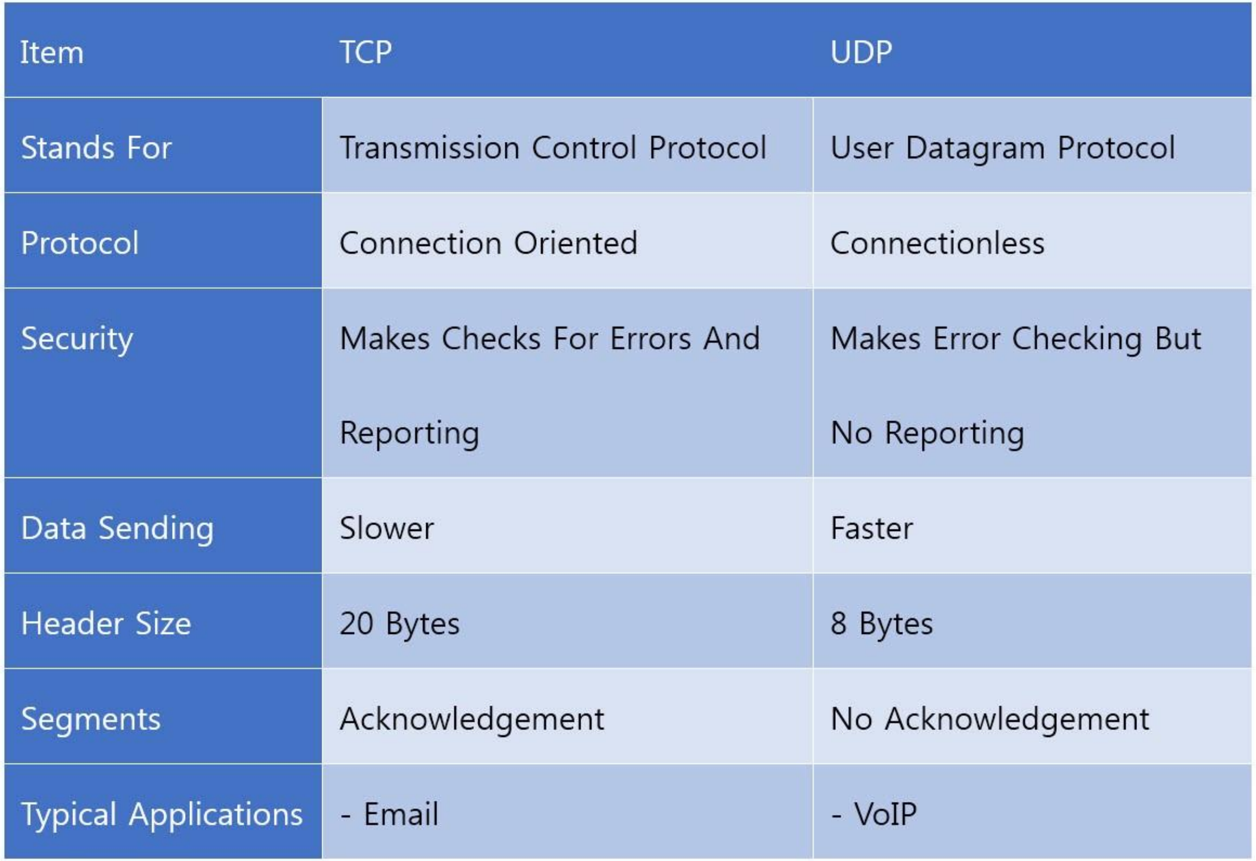
Application	• End User layer • HTTP, FTP, IRC, SSH, DNS
Presentation	• Syntax layer • SSL, SSH, IMAP, FTP, MPEG, JPEG
Session	• Synch & send to port • API's, Sockets, WinSock
Transport	• End-to-end connections • TCP, UDP
Network	• Packets • IP, ICMP, IPSec, IGMP
Data Link	• Frames • Ethernet, PPP, Switch, Bridge
Physical	• Physical structure • Coax, Fiber, Wireless, Hubs, Repeaters



TCP/IP MODEL	Vs	OSI MODEL
Application		Application
		Presentation
		Session
Transport		Transport
Internet		Network
Network Interface		Data Link
		Physical

Know your protocols!

TCP VS UDP



Item	TCP	UDP
Stands For	Transmission Control Protocol	User Datagram Protocol
Protocol	Connection Oriented	Connectionless
Security	Makes Checks For Errors And Reporting	Makes Error Checking But No Reporting
Data Sending	Slower	Faster
Header Size	20 Bytes	8 Bytes
Segments	Acknowledgement	No Acknowledgement
Typical Applications	- Email	- VoIP

TCP VS UDP

TCP is stable so you get all the water

UDP is just throwing water at yourself and if you get it, then great, but some will be lost

TCP

UDP

ICMP

- Used for pinging two machines
- Does not have a TCP or UDP port
- Main use case is diagnostics and testing to ensure machines are available

FTP

- Stands for File Transfer Protocol
- Unencrypted Protocol that is used to transfer files between two computers
- Encrypted version is SFTP (FTP using SSH)
- Uses TCP **port 20 & 21** for reliability and error checking

I HAVE A VERY SPECIFIC SET OF SKILLS, LIKE DOWNLOADING FILES OVER FTP
AND UPLOADING FILES OVER FTP, AND SOMETIMES DOWNLOADING AND UPLOADING AT THE SAME TIME. OVER FTP.
erator.net

ARP

- Address Resolution Protocol
- The ARP maps IP and MAC addresses together.
- This is used in LAN networks so that the two devices can communicate.
- The IP address just directs devices to each other on networks and the MAC is the identifying number

DNS

- Domain Name System or The “Phone Book” of the Internet
- DNS servers are vital to how we use the internet today. Without them we would need to memorize all of the IP addresses of the websites that we wanted to visit.
- DNS maps IP addresses to names that we can easily remember.
- Google.com has two public DNS servers, 8.8.8.8 and 8.8.4.4
- Uses **TCP/UDP Port 53**

skillcrush.com
216.172.190.36
tumblr.com
216.162.190.37
facebook.com
223.172.190.38

DHCP

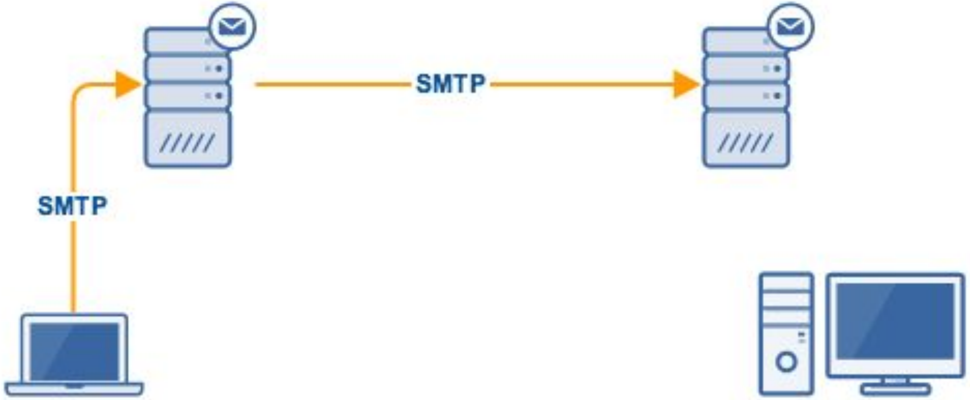
- You know how your IP changes when you go from place to place?

- DHCP servers are responsible for dynamically assigning IP addresses to devices on the network

- The scope of the DHCP service defines the range of IP addresses it can give out. This is done by setting a starting and ending IP address, which can be adjusted to whatever the network needs.

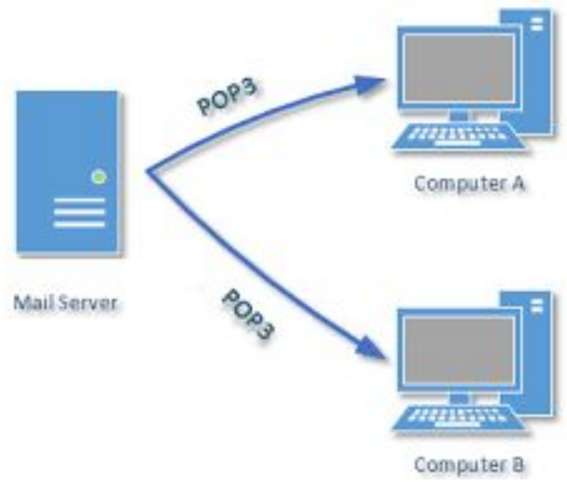
SMTP

- Stands for Simple Mail Transfer Protocol
- Used to send email messages from a client machine to a server
- Also used to send email messages from one server to another server
- Commonly uses these TCP ports: 25 & 587
- Port 25 is for transmitting emails between servers
- 587 is for new email submissions (when you hit send)



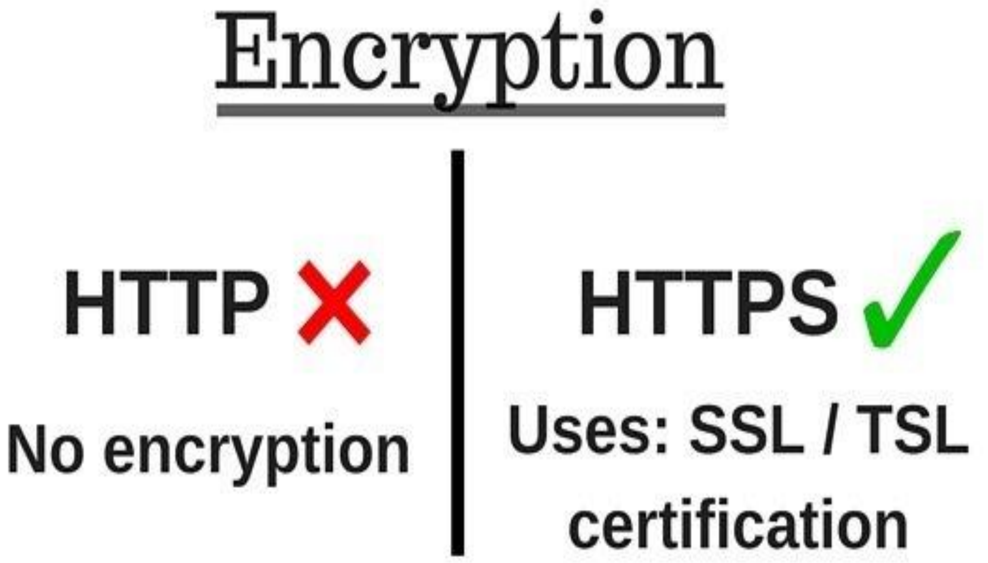
POP3

- Third version of Post Office Protocol (most commonly used)
- Used to deliver finished emails from a server to the recipient
- Uses TCP port 110 for unencrypted and 995 for encrypted



HTTP/HTTPS

- Stands for Hyper Text Transfer Protocol
- The main protocol for transmitting webpages and communicating to web servers on the internet
- Initiated by the recipient of the data (the person browsing the web)
- Uses port 80 for unencrypted traffic and port 443 for encrypted (HTTPS)



Encryption

HTTP ✗

No encryption

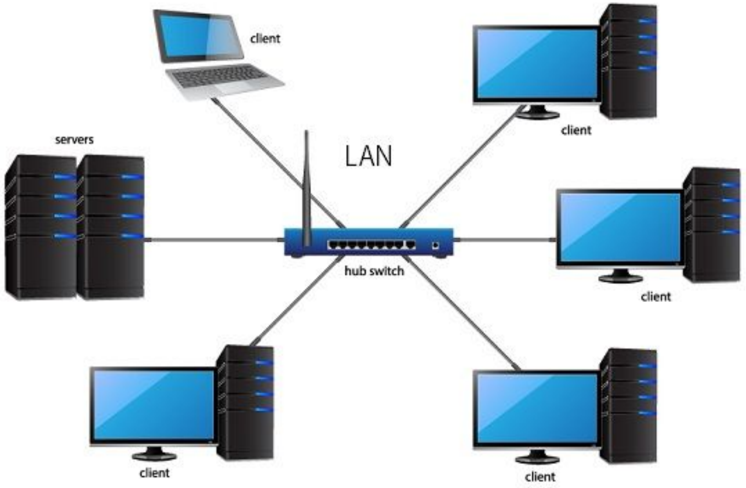
HTTPS ✓

Uses: SSL / TSL certification

Network Architecture

Local Area Network (LAN)

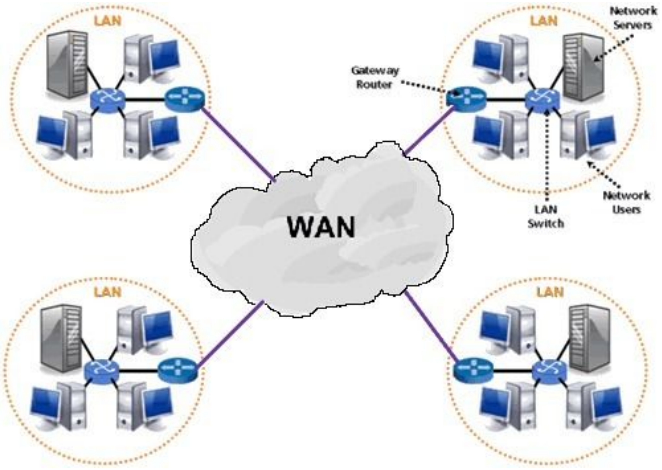
A Local Area Network (LAN) is a group of computers and other network connected devices that fit within the scope of a single physical network. (EX. office building)



Wide Area Network (WAN)

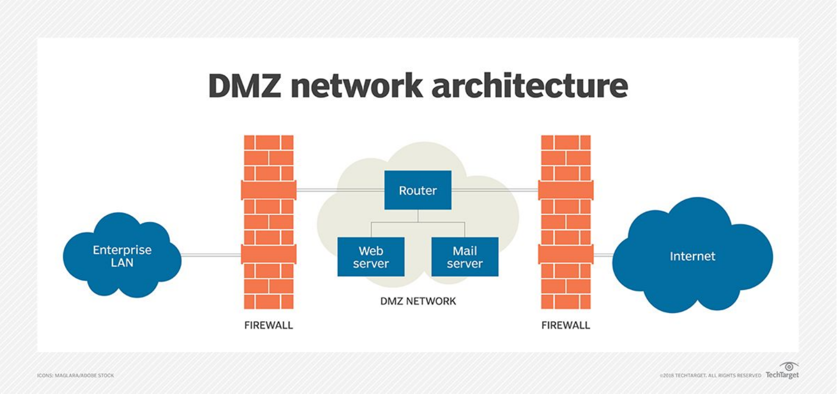
A Wide Area Network (WAN) is a internetwork that connects multiple sites that cover large geographical regions. (EX. Campus)

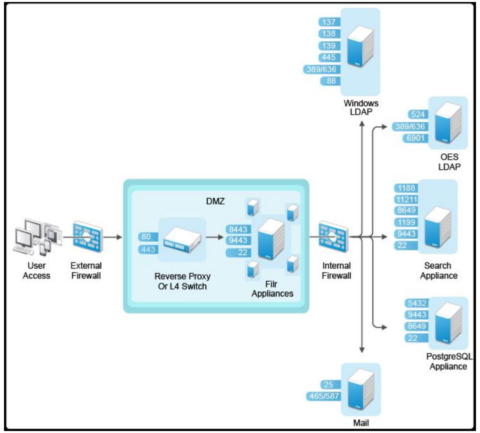
Multiple LANs = 1 WAN



DMZ

The DMZ (Demilitarized Zone) is a sub-network that contains most of a network's externally connected services which connect to the Internet. If somebody gains access to your network they do not have access to your whole network only the outward facing parts.

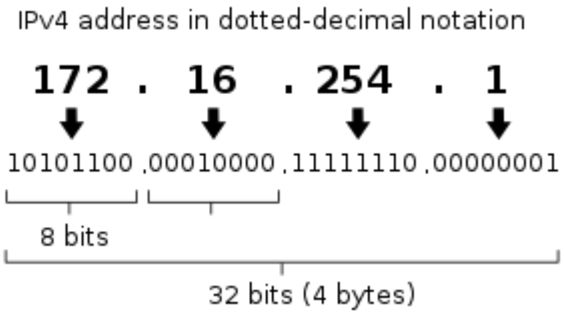




IP Addressing

IPv4 VS IPv6

- 32 bits (4 Bytes) and uses binary
- What you’re use to seeing
  - Need this to connect to your Minecraft Server
- Looks like this



IPv4 address in dotted-decimal notation

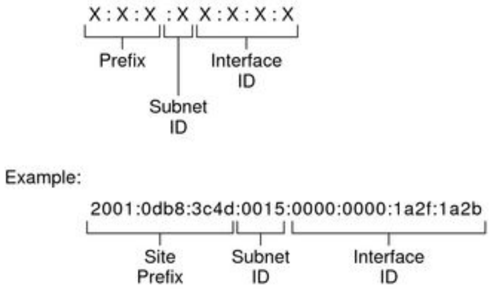
172 . 16 . 254 . 1

10101100 .00010000 .11111110 .00000001

8 bits

32 bits (4 bytes)

- 128 bits (16 bytes) and uses Hex
- Not super popular atm
- It was created to circumvent the problem of eventually running out of IPv4 addresses
- Looks like this
  - xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx where each x is a hexadecimal digit



X:X:X :X X:X:X:X

Prefix

Subnet ID

Interface ID

Example:

2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b

Site Prefix

Subnet ID

Interface ID

Static IP Addressing

- These devices will never change their IP address unless you do it
- Usually used for LAN and big websites
- Example- 8.8.8.8 is Google’s primary DNS server

Static IP

Dynamic IP Addressing

- Dynamic IP addresses are temporary IP addresses that change and are being constantly assigned and reassigned
- Done by a DHCP server (Dynamic Host Config Protocol)
- Example
    - You walk into a restaurant and want to connect to their Wifi.
      When you enter the password to get the Wifi,
      you have just joined that network.
      So that devices on that network can talk to you,
      and so that you can talk out to the internet,
      you are given a temporary IP address.

Dynamic IP

Wireshark

- Try to find the protocols we talked about in Wireshark
- Go here!

https://tinyurl.com/CDONetworking2019

Hivestorm!

- Teams of 2-4, November 1st-2nd
- Log into remote Linux and Windows machines to secure them!
- **Practice security, forensic, configuration, and system administration tasks!**
- **Prepare for other Cyber Defense Competitions!**
- **More information at hivestorm.org!**

- **https://tinyurl.com/CDOHivestorm19**

Add us on Social Media!

Twitter: **@ualbanyCDO**

Instagram: **ualbany_cdo**

Website: **uacyber.org**

Myinvolvement: **Cyber Defense Org**

We have a discord!

Cya Next Time!

Next time on DBZ....Introduction to pfSense firewalls with Jonathan Matza!