Network Security

Prep

- First, reboot your virtual machine:
  - sudo reboot 0
- Run the following commands to install required packages:
  - sudo apt update
  - sudo apt install net-tools
  - sudo apt install tcptraceroute
  - sudo apt install nmap
  - sudo apt install openssh-server
  - sudo apt install apache2
  - sudo apt install wireshark
- If you run into an issue with sudo apt update, check the date on your machine, it may be out of sync, a reboot usually fixes this

Topics

- Overview of Networks
  - Protocols
  - OSI Model
  - Devices
  - Addressing
  - Take Computer Networks for more depth!
- Network Security
  - Firewalls
  - IDS
  - Protocol Attacks
  - Network Zones
  - More attacks than we can cover!
- We will explore protocols and attacks on each protocol

What is a Network?

- Many things!
- Hosts/End Systems
- Applications
- Communication Links
- Packets
- Packet Switches
- Link Layer
- Routers
- Transmission Rate (Bandwidth)
- ISP
- TCP/IP

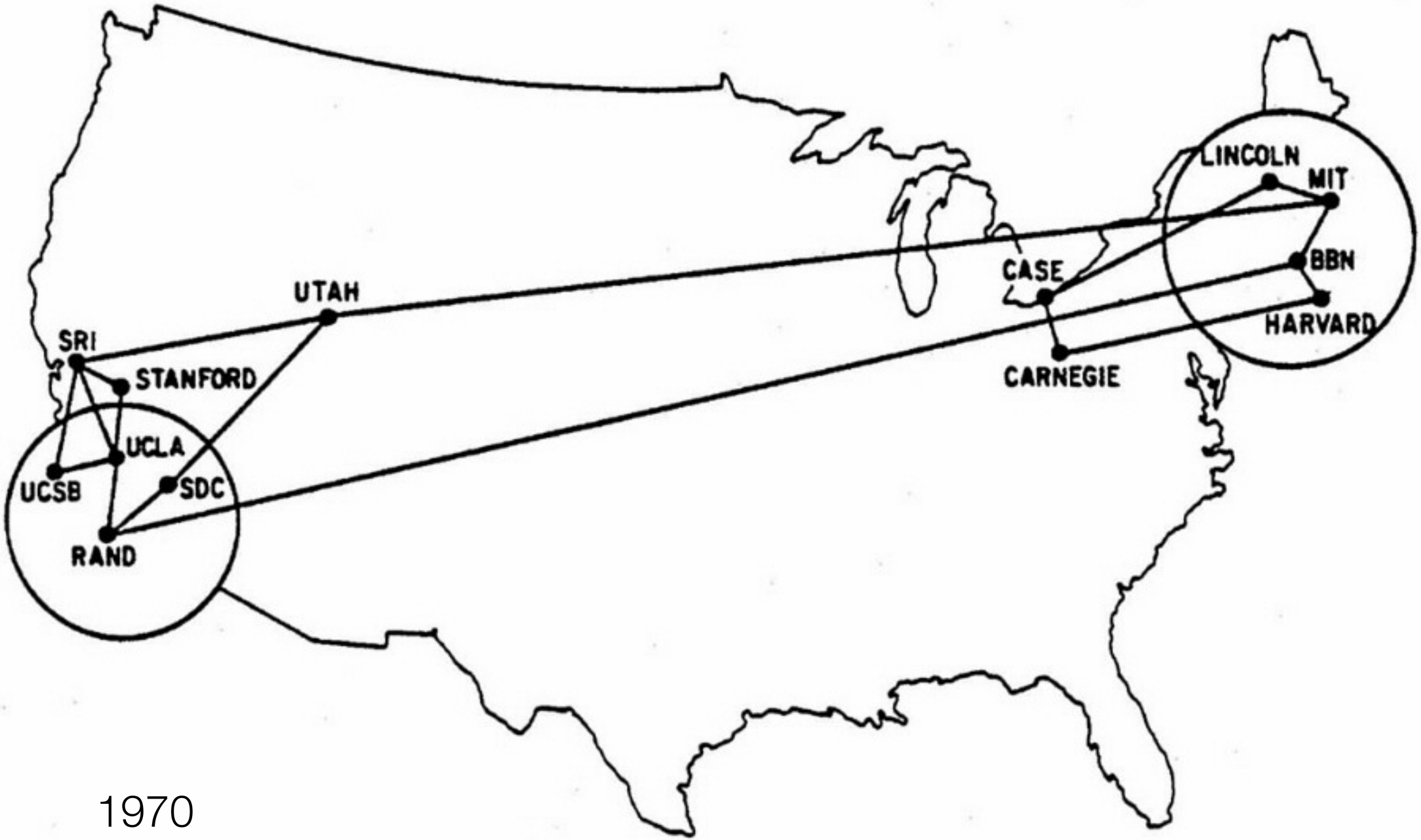
What is the Internet?

- Network of Networks
- Made of Standards
  - Protocols
- Addressing
- Reliable Communication
- Much more …

How the Internet Came to Be

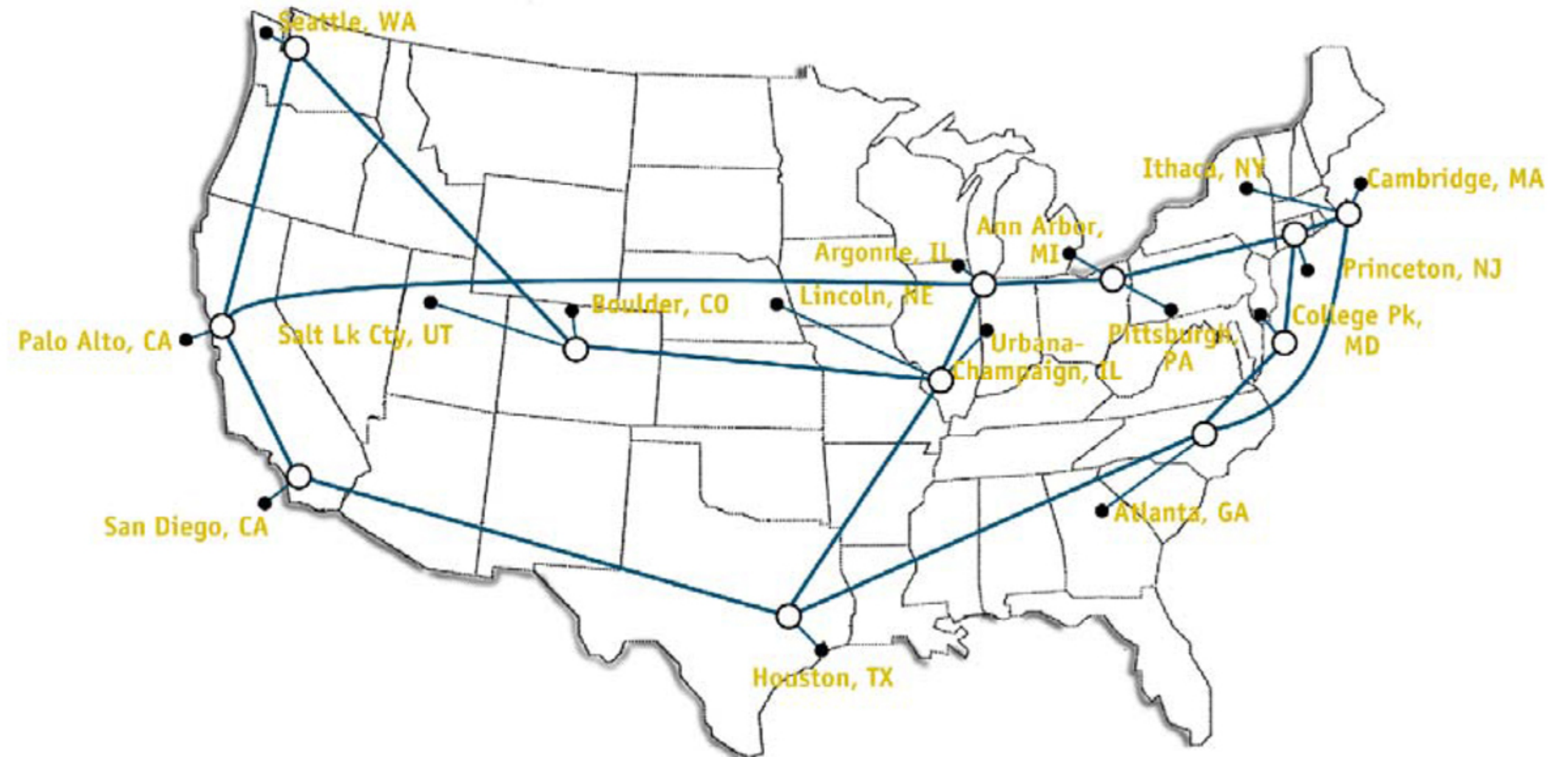
- DARPA – Defense Advanced Research Projects Agency
- Funded ARPANET (Advanced Research Projects Agency Network) (1969)
- Network Military Bases, Universities, and Research Locations
  - UCLA, UCSB, University of Utah
- Packet Switching Network (vs Circuit Switching)
- Goal of Project:
  - Maintain Control of Network and Nuclear Silos from Nuclear Attack
  - Ability to Recover form Network Losses
- Grown to East Coast (Cambridge)
- 1971 – Network Included 23 Universities
- 1989 – World Wide Web Idea – Sir Tim Berners-Lee
- Operated by Military until 1990

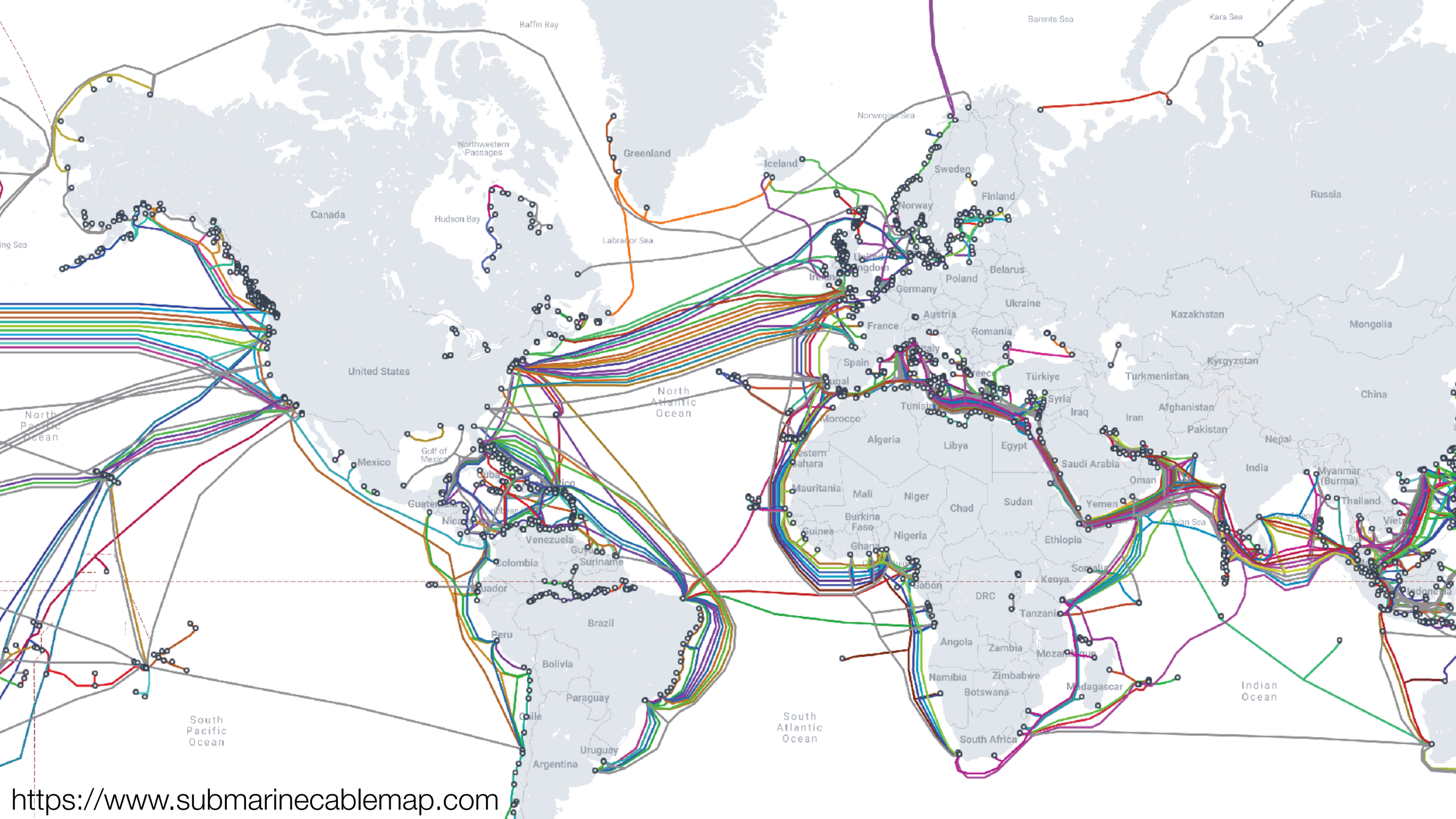
The ARPANET in December 1969


LINCOLN
MIT
BBN
HARVARD
CASE
CARNEGIE
UTAH
SRI
STANFORD
UCLA
UCSB
SDC
RAND

1970

NSFNET T3 Network 1992





https://www.submarinecablemap.com

OSI Layers

- Divide communication into layers of responsibility
- **Application**
- Presentation
- Session
- **Transport**
- **Network**
- **Datalink**
- Physical

Packet

- Application data is segmented into parts to be transmitted on a network
- Original data (.e.g. "GET /") gets additional header information on each layer
  - Transport Layer - Sequence numbers, flow control, etc
  - Network Layer - Source and destination IP is added, TTL, checksum, etc
  - Datalink Layer - Source and destination MAC address, CRC check, etc
- Packets get routed through network to their destination

Internet Layer

- Focus on routing of data from one end to another
- Routing requires addresses to exist
- Think of Postal Service, how do we get envelope from one end to the other
- Most well know protocol: IP

Internet Protocol (IP)

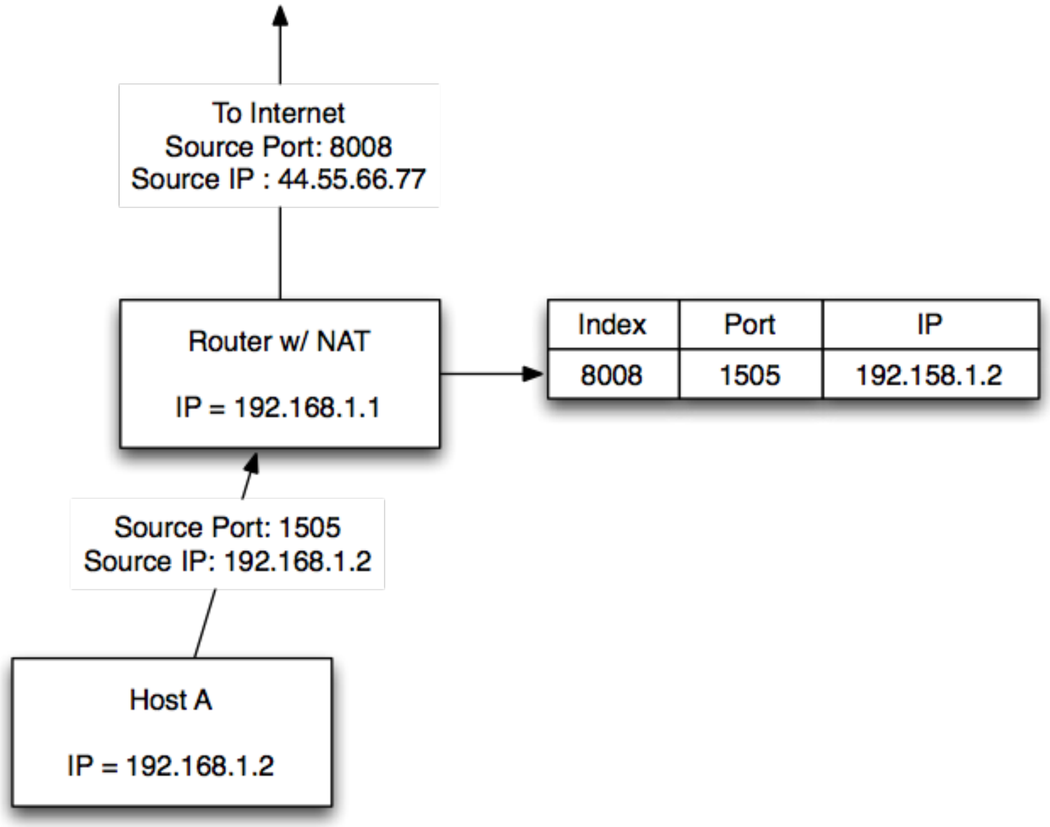
- Focuses on delivery from source to destination
- What is source and destination? IP Address!
- What is an IP address?
- Rule: Each connected device to Internet must have unique IP
- Why?
- Try the following command:
  - ip addr
  - What do you see?
  - Do you have 1 address or more?

IP Addresses

- Private Addresses:
  - 10.0.0.10 → 10.255.255.255
  - 172.16.0.0 → 172.31.255.255
  - 192.168.0.0 → 192.168.255.255
- Classes - Determined by first byte of IP address
  - A: 0-126 - Very large networks
  - B: 128-191 - Large corporations and government networks
  - C: 192-223 - Very common group, includes ISPs
  - D: 224-247 - Reserved for multicasting
  - E: 248-255 - Experimental use
- Subnets
  - Allow you to divide network into different sub networks

Network Address Translation (NAT)

- 2 Problems:
  - Not enough IPv4 Addresses
  - Want addresses to be private
- Use NAT!
- How does it work?



- IP address may not be unique because of NAT. But if router is exposed to internet, it's IP must be unique.
- Helps protect internal network as well

IPv6

- IPv4 - Limited number of addresses!
- Limited address space in IPv4 (32 bits)
- IPv6 - 128 bit address!
- Additional security (IPsec)
- Change to header format (makes processing easier)
- Additional quality of service controls
- No fragmentation in routers

IPv6

- Run: ip -6 addr
- What is your IPv6 Address?
- What number system is used to represent IPv6?
- Note:
  - Double colons (::) represent 0s
  - 0s are omitted
  - Example: 34:dc::ff00:1028:11f0 —> **00**34:**00**dc:**0000:0000:0000**:ff00:1028:11f0

Transport Layer

- Focus on ensuring packets get from one point to another
- Offers various services that control flow of packets
- 2 Well Known Protocols: TCP and UDP

Transport Connection Protocol (TCP)

- Point to Point – One sender, one receiver
- Reliable
- Pipelined
- Send & Receive Buffers
- Full Duplex
- Connection Oriented
- Flow Controlled – Sender won’t overwhelm receiver
- Acknowledgement of Packets

TCP Flow Control

- Sender won’t overwhelm receiver
- Receiver let’s sender know how much data it can receive (rwnd)
- This is the spare room it has on it side

TCP Congestion Control

- Congestion can happen for many different reasons
- End systems sending too much data
- Core network not able to keep up
- Unreliable medium causing packet retransmits
- Sender handles congestion with congestion window (cwnd)
- 3 Principles:
  - Loss segment = congestion, decrease rate
  - Ack segment = good network, increase rate
  - Probe network by increasing and backing off when needed

TCP Connection Setup

- Client sends server TCP SYN segment
- No data, sends random sequence number
- Server responds with SYN ACK segment
- Still no data, sends random sequence number
- Client sends ACK (no more SYN) and optionally sends data

- Try running the following:
  - tcptraceroute -d www.case.edu 80
  - (If your VM is connected to the network as "shared", you might not get anything interesting, you might want to set it to bridge)
  - The -d is debug, it will show us the SYN, SYN ACK

TCP Connection Teardown

- When client is done, it sends a FIN segment
- Server receives FIN, replies with ACK. It puts connection in closing state, then sends FIN.
- Client receives FIN, replies with ACK
- Goes into TIME_WAIT
- Server receives ACK, connection closed

Viewing TCP Traffic

- To view current TCP traffic, you can use tcpdump:
- sudo tcpdump
- What do you see?
- Now try the following:
  - hostname (use this output for the browser step)
  - sudo tcpdump port 80
  - Wait a minute or two, then open a web browser
  - type in hostname.local where hostname is your hostname, e.g: compsec.local
  - What do you see?

User Datagram Protocol (UDP)

- UDP = lightweight, “closer” to network layer
- Why use UDP?
- No handshake, no throttling, why would this be good?

UDP vs TCP

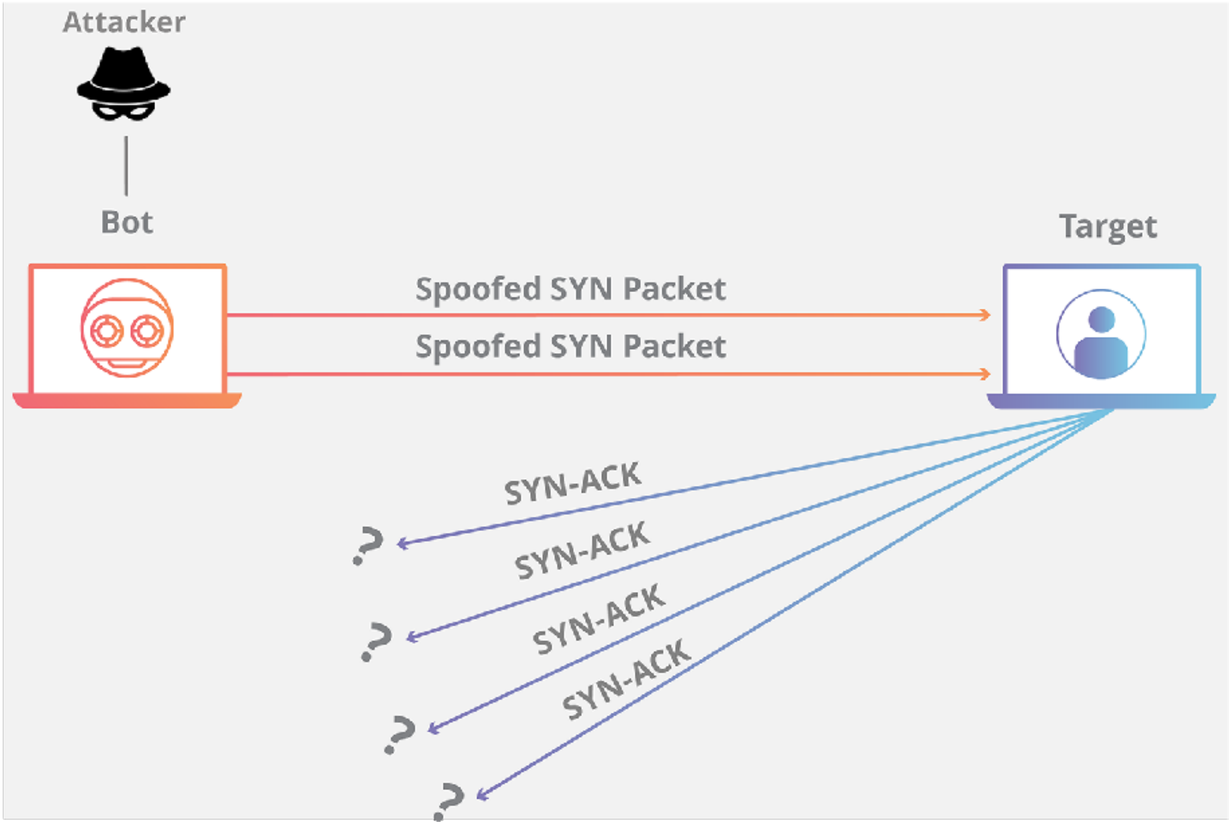
- TCP
  - Provides connection oriented services
  - Provides reliable transfer
  - Bytes in order, no packet left behind!
  - Provides congestion control
  - Traditionally, not good for multimedia
- UDP
  - Lightweight
  - No Handshaking
  - Just send it and see what happens

Denial of Service

- Attack a host or service with requests/responses
- Exhaust server resources
- Reduce availability
- Distributed Denial of Service (DDOS)
  - Distribute the attack from multiple servers or hosts
  - More requests from different sources make it harder to defend

Attacking Server with TCP and IP Protocol

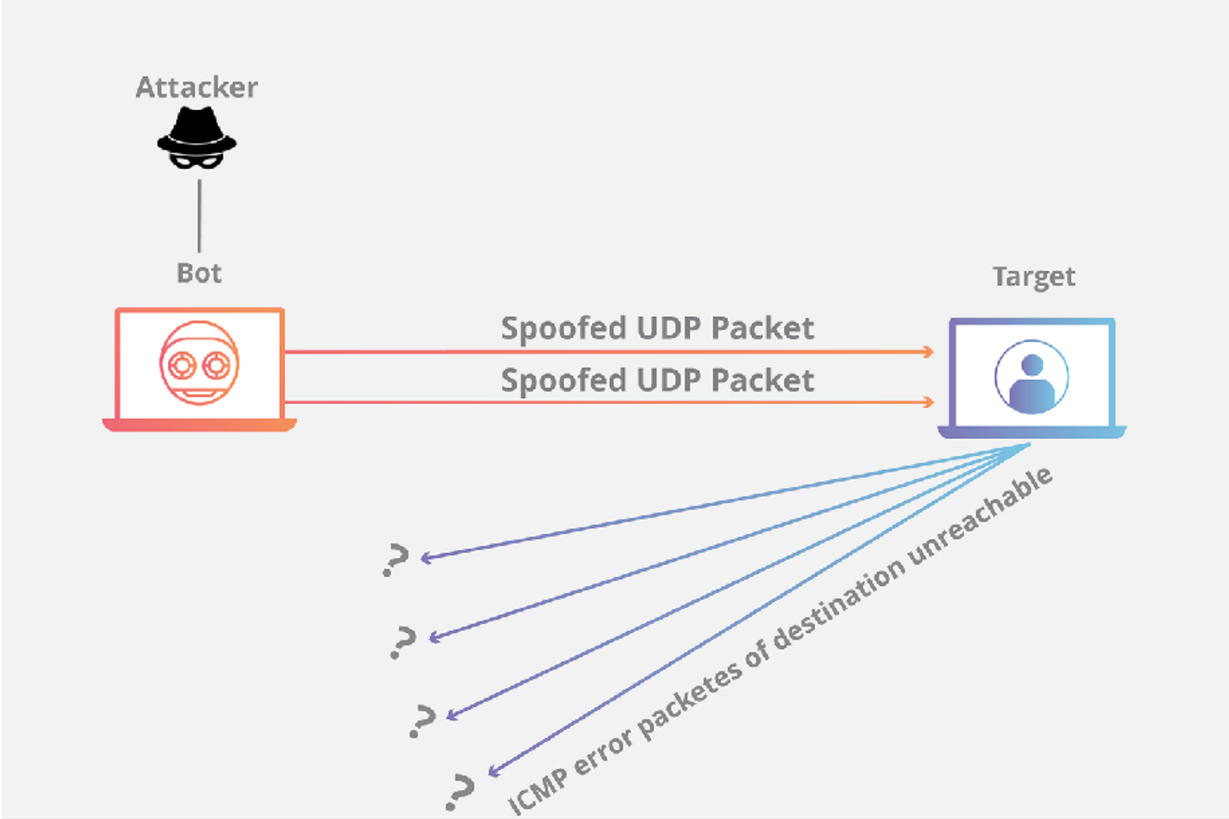
- Various attacks against TCP
- One popular is a SYN flood attack
- Perform a DDOS by spoofing IP address
- IP is not verified, SYN-ACK comes from another server
- https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/



Cloudflare

Attacking Server with UDP and IP Protocol

- UDP is also vulnerable
- Perform a DDOS by spoofing IP address (like TCP)
- IP is not verified, server's resources exhausted, ICMP error goes to server
- https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/



Cloudflare

Ports

- Problem: Message delivered to destination, who is it for? Web Browser? Discord?
- IP determines endpoint, Port determines application
- Used within Transport Layer

- Run the following: netstat -tn
  - Then netstat -t
  - Looks at the difference, what do you notice?

HTTP	80
SSL/TLS	443
SSH	22
FTP	20, 21
DNS	53
SMTP	25

Discovering Ports

- nmap is a popular port scanner
  - Can identify open ports on a server
- **ONLY SCAN YOUR VM!**
  - Please don't get us in trouble with IT!
- Try the following, what do you see?
  - nmap localhost

Probing Ports

- nmap can determine version of software as well
  - nmap -sV localhost
  - Why is this important?
- We can also check strength of ciphers:
  - nmap -p 443 --script ssl-enum-ciphers case.edu

Domain Network Services (DNS)

- Exist within Application Layer, but plays critical role in Internet Layer
- Both a Protocol and a System
- Listens on Port 53
- System is made of hierarchy of DNS servers
- Hierarchy is based on authority
- Request are made over UDP
- Server has records
- Name → IP and IP → Name
- Why DNS? Do you know the IP to case.edu?

DNS Exercise

- host google.com
- dig google.com

- Get IP for google.com and put in browser, what do you see?
- Get IP for gmail.com, and put it in browser, what do you see?
- Try the same for drive.google.com