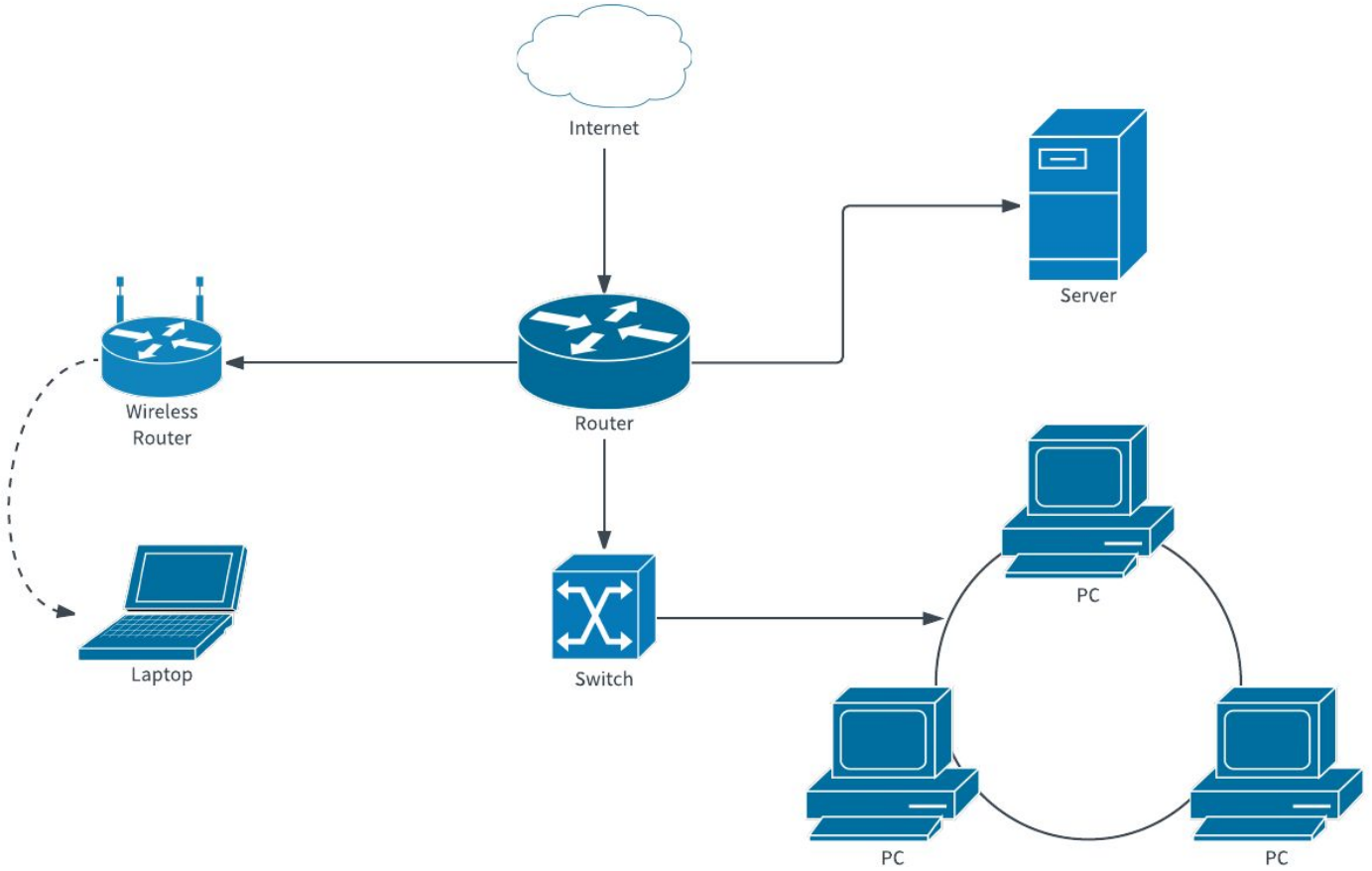
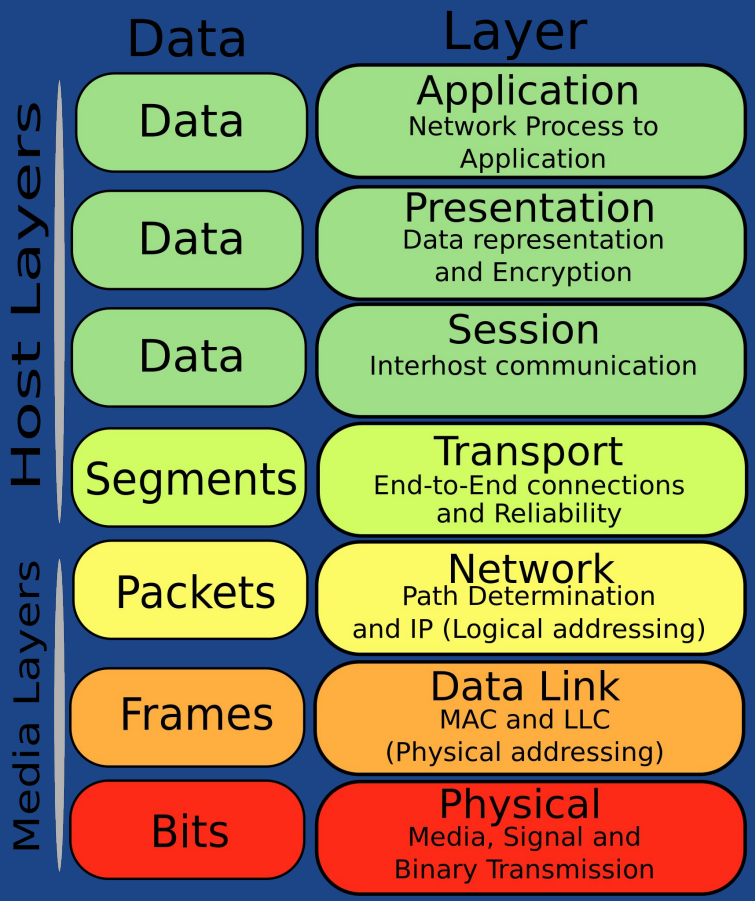
intro to networking*

*computer networking


Internet
Server
Wireless
Router
Router
Laptop
Switch
PC
PC
PC

OSI Model


Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data representation and Encryption
Data
Session
Interhost communication
Segments
Transport
End-to-End connections and Reliability
Packets
Network
Path Determination and IP (Logical addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal and Binary Transmission

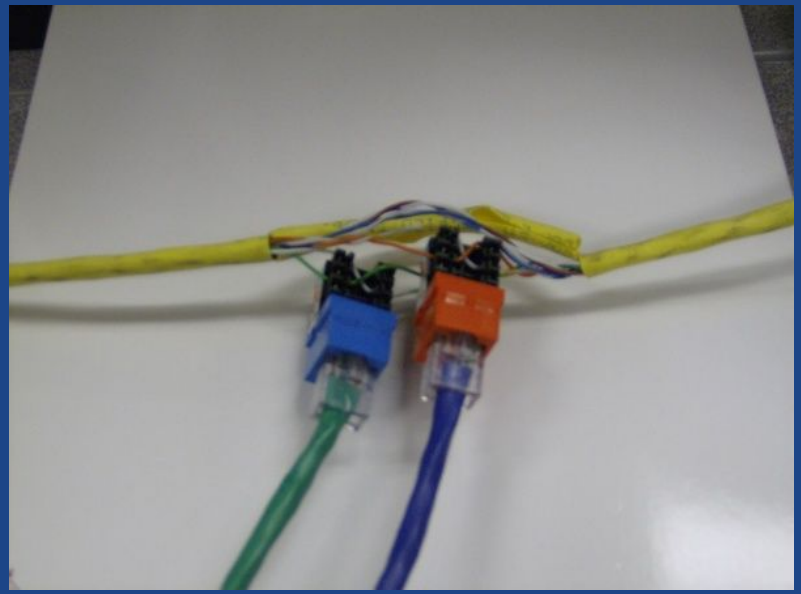
Physical Layer

- Ethernet
- Wifi

Why do we care?

Exploiting the Physical Layer

Passive Ethernet Taps

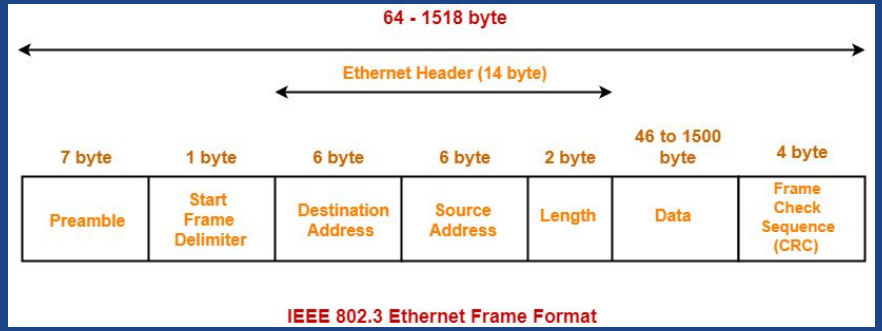


WiFi

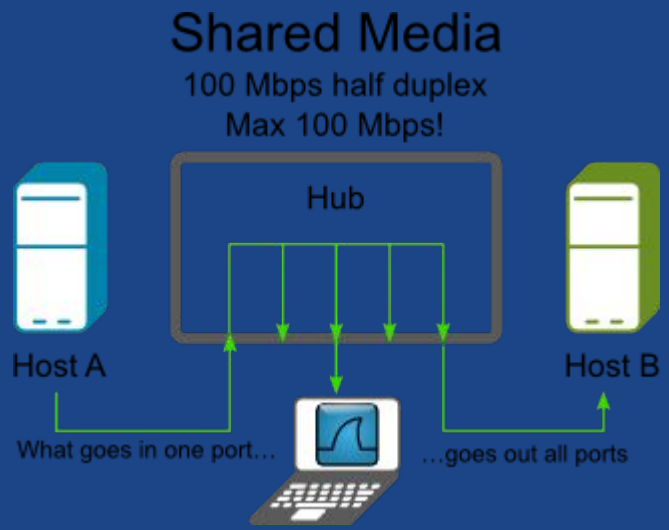
Spooky Shit

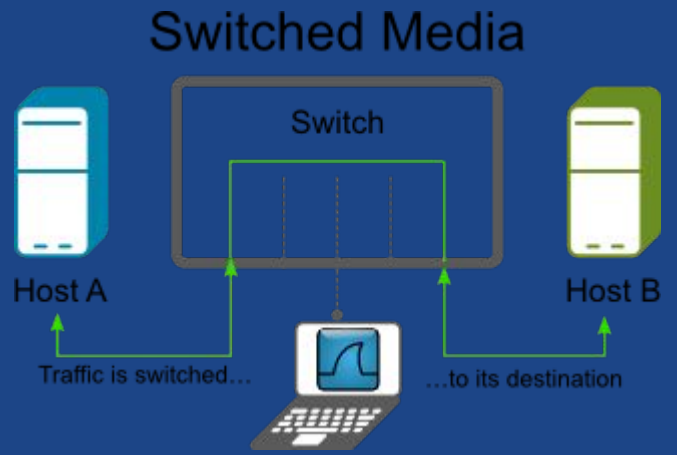
Data Link Layer

- Frames & MAC Addresses
- Shared vs Switched Ethernet
- Topology Protocols
  - Spanning Tree Protocol
  - Shortest Path Bridging



Hubs vs. Switches



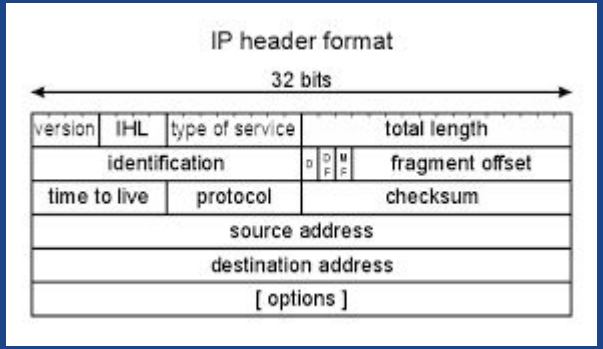


Exploiting the Data Link Layer

- MAC Spoofing
- MAC Flooding
- Denial of Service with STP

Network Layer (IP)

- Like the Data Link, but not restricted to your local network
- Packets, IP Addresses, and Subnets
- Gateways and Broadcasts



- IP Routing (Routing tables)

ARP - the most ambitious protocol crossover

How do I send data from one IP to another IP?

Address Resolution Protocol.

Request - Who has *IP?*

Response - *IP* is *MAC*

ARP Poisoning

ARP Spoofing

- Similar to MAC Spoofing, except we spoof an IP address

Denial of Service

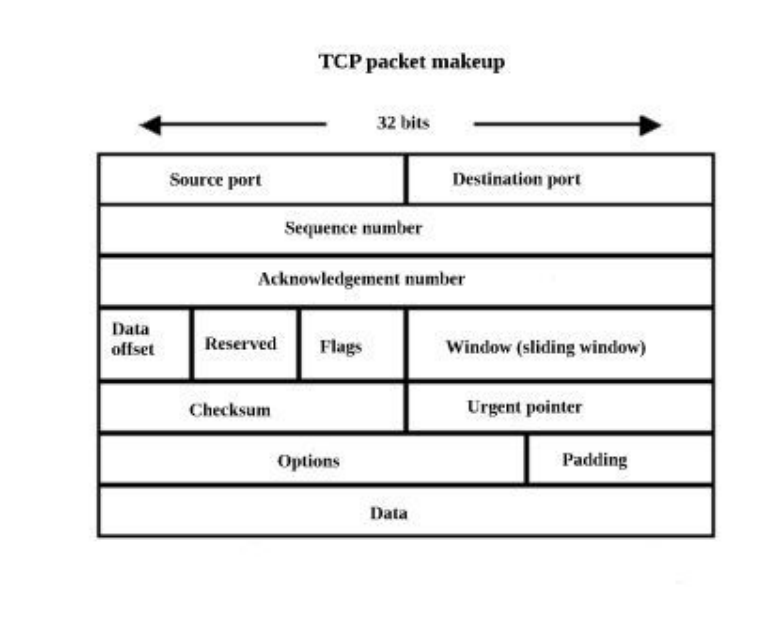
- Spoof Gateway IP to be the broadcast MAC Address

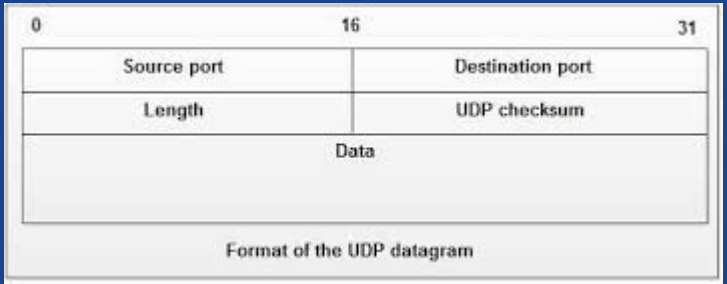
Transport Layer

- Transmission Control Protocol (TCP) - Accurate and Reliable
  - Connection Abstraction - provides a *stream of data*
  - Same Order Delivery - arrive in same order as sent
  - Reliability - lost packets are resent/checksums
  - Flow Control - consider receiver's buffer size when sending
  - Congestion Avoidance - consider network infrastructure when sending
  - Multiplexing - multiple connections to a single IP (ports)

- User Datagram Protocol - Fast
  - Data Integrity - checksums
  - Multiplexing - multiple connections to a single IP (ports)

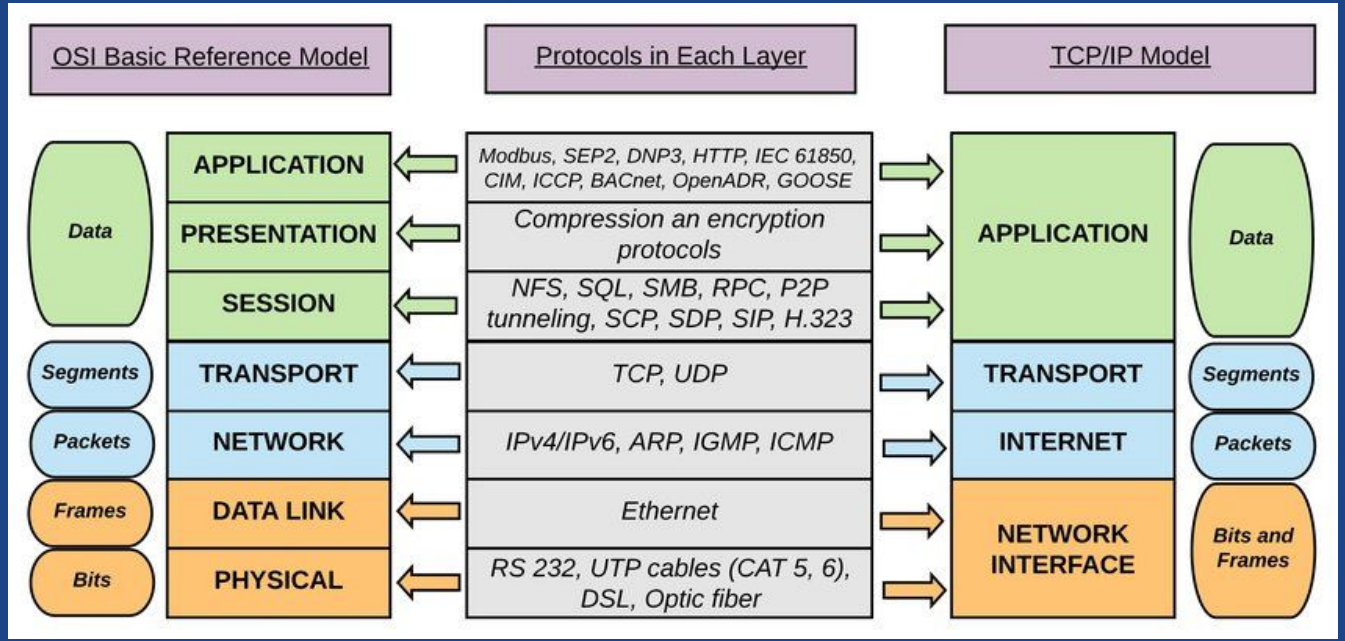
TCP Segments vs. UDP Datagrams



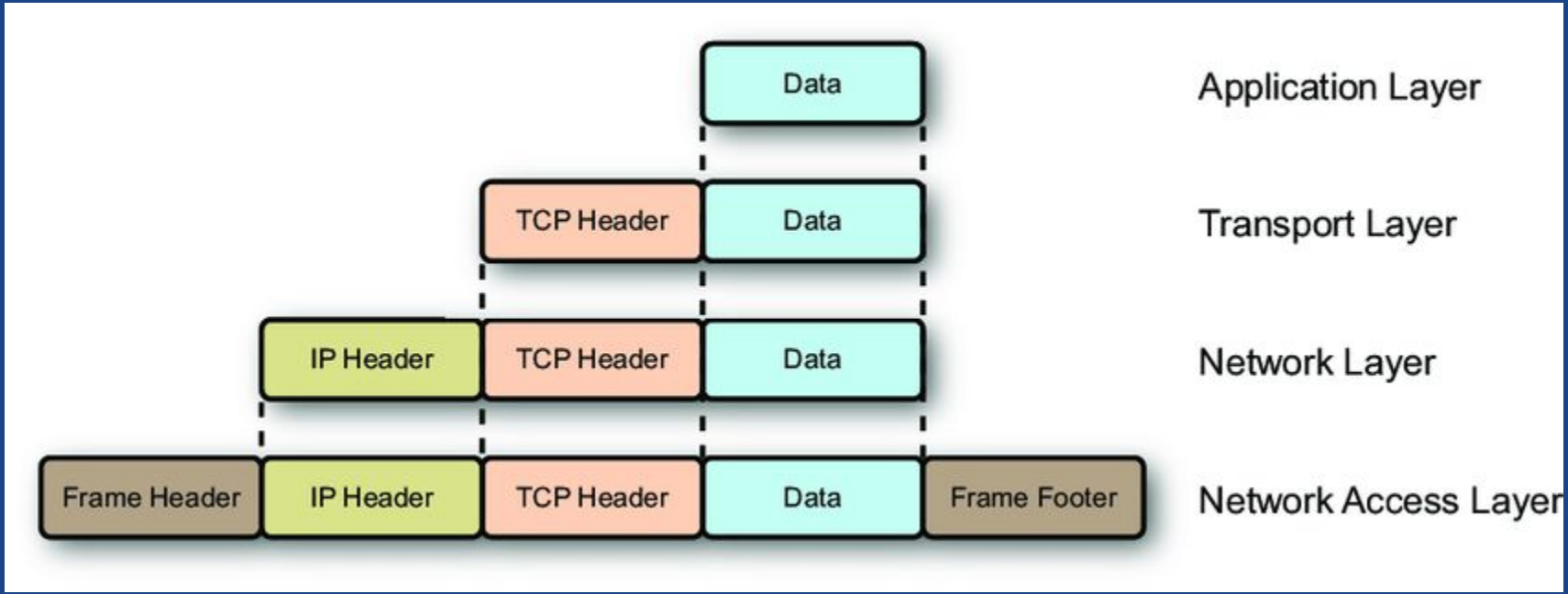


Data Layers

OSI Model begins to break down here…



Layer Encapsulation



Common Application Protocols

DHCP - The most introspective protocol

You might be asking yourself… Who am I?

Dynamic Host Configuration Protocol

- Assigns IP Addresses to devices on the local network
- Built on top of UDP

Ports: 67 (on Server) & 68 (on Client)

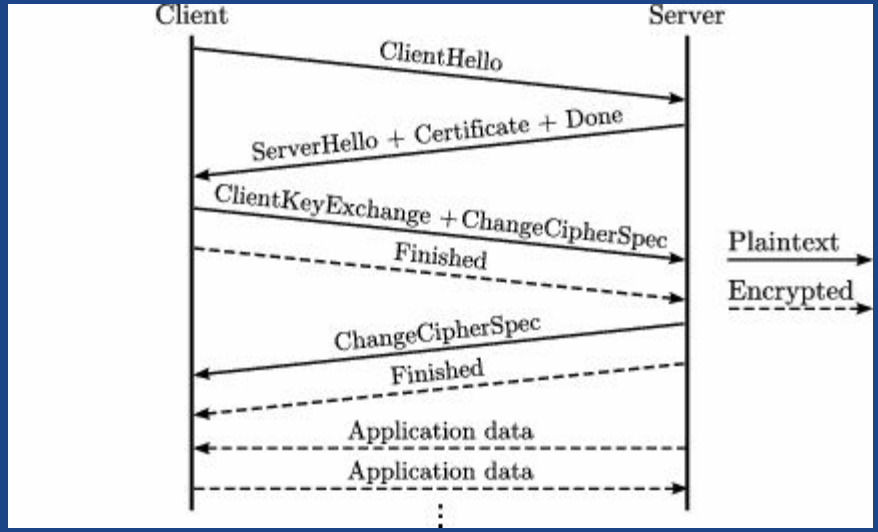
Exploiting DHCP

- Man in the middle Attack
  - Spoof DHCP Server and forward all traffic through malicious device

- Denial of Service
  - Request enough IP Addresses so that the actual devices can’t

TLS - formerly SSL

- Transport Layer Security
- Built on top of TCP
- Provides Confidentiality
  - Encrypt traffic between server client
- Provides Authenticity
  - Verify server's certificate



Allows us to secure other protocols. No specific relevant port.

Exploiting TLS

- Padding Oracle On Downgraded Legacy Encryption (POODLE) - 2014
  - Downgrade to SSL 3.0
  - Padding Oracle Attack
- Browser Exploit Against SSL/TLS (BEAST) - 2011
  - TLS 1.0 CBC Mode
- Compression Ratio Info-leak Made Easy (CRIME) - 2012
  - Compression in TLS leaks information about encrypted content
- Heartbleed - 2014
  - TLS Heartbeat w/ incorrect length leaks server memory as padding

HTTP/S - Hypertext Transfer Protocol

- You know, the internet one, for websites...

HTTP over TLS (HTTPS)

- Secure your browsing traffic
- Prevent man-in-the-middle attacks

Ports: 80 (HTTP) & 443 (HTTPS)

HTTP

- Everything is in the clear
  - A network attacker can see every single packet

- Don’t use HTTP for anything!

- Even using HTTPS will still leak your browsing history

DNS

- Mapping URLs to IP Addresses
- Built on top of UDP

DoT - DNS over TLS (Dedicated Port 853)

DoH - DNS over HTTPS (Port 443)

Exploits with DNS

- Control of a DNS server means you can forward any request anywhere
- Obvious DOS by giving invalid/no response
- DNS is in the clear, but even encrypted DNS is viewable by someone

Other Common Protocols

- S/FTP
- SMTP
- IMAP
- POP3
- Telnet
- SSH
- ICMP
- NTP
- NFS
- RIP
- BGP

Common Networking Tools

Wireshark

- Capture Network Traffic from…
  - Your device
  - The network

- Analyze Network Traffic from…
  - PCAP’s (Packet Captures)

- Follow _____ Stream is very useful

ping

- Check your connection to an IP Address
- Talks ICMP

nslookup/dig/host

- Resolve a URL to it’s IP Address
- Talks DNS

netcat/nc

- Connect to an IP:Port
- Listen on a port
- Write/Read to remote port
- Tons of other features (*man netcat)*
- Talks TCP/UDP

Notable Mentions:

- socat - More functionality/complexity
- websocat - Connect to WebSockets

curl

- Retrieve a website
- Talks HTTP/HTTPS

nmap

- A very powerful scanning tool
- Allows you to scan for...
  - Available IPs on a Subnet
  - Open Ports at an IP Address

BE CAREFUL! YOU WILL GET IN TROUBLE IF YOU USE THIS ON A NETWORK YOU DO NOT OWN!
IT'S EXTREMELY SKETCHY! AND POSSIBLY ILLEGAL!
YOU HAVE BEEN WARNED!