Networking

Protocols

TCP vs UDP

- **TCP (Transmission Control Protocol)** and **UDP (User Datagram Protocol)** are basic standards that define the rules of the internet
  - Included within the standards defined by the Internet Engineering Task Force (IETF)
- TCP is more common than UDP and is meant for most websites, emails, file transfers, etc.
- UDP is faster so it is used for video conferencing, streaming videos, voice calls, etc…

Connection-Oriented vs Connectionless

- TCP is a **connection-oriented** protocol
- UDP is **connectionless** protocol
- A connection-oriented protocol means that a connection will be made between two hosts and then data will be sent back and forth between the two hosts
  - Sometimes referred to as the telephone system, where two phones will connect with each other and then start communicating back and forth
  - Constantly checking for errors
- A connectionless does not require a connection between the hosts to send data
  - Sometimes referred to as a postal system
  - Does not verify packets were received correctly

ICMP

- **ICMP (Internet Control Message Protocol)** is commonly used for a network to report problems with different services
- If a device is unable to reach another device, ICMP will send a message notifying the sender that the receiver is unreachable
- **`ping`** and **`traceroute`** use ICMP traffic
  - **`ping`** sends an echo request to another device on the network to check connectivity between the two devices
  - **`traceroute`** will trace the physical route between two hosts
- ICMP also reports if a router's memory is full and/or if the max number of hops is reached when a device is attempting to reach another device

GRE and IPSec

- **GRE (Generic Routing Encapsulation)** is a protocol that allows for tunneling where many different types of protocols can be used inside this tunnel
  - This protocol was developed by Cisco and can be used with point-to-point tunneling and/or point-to-multipoint tunnels
  - No additional security, GRE does not encrypt data
- **IPSec (IP Security)** creates tunnels and provides security between two devices
  - VPNs created with IPSec will have encrypted packets and would be safer to use over unsecure/untrusted networks
- IPSec uses two main security protocols to protect their packets: **AH (Authentication Header**) and **ESP (Encapsulating Security Payload)**
  - An AH is a hash sent with the data that the receiving device can hash the data to get the same hash
    - If the hashes match up, they know that the data was not altered in transmission
  - ESP has five parts to it:
    - Data is encrypted using different algorithms
    - Data uses checksums to make sure that the data was not tampered with
    - Authentication to make sure the data is being sent to the proper recipient
    - Check for replays, helping stop a replay attack where a malicious user will resend the same packets
    - Traffic flow that controls all the traffic and keeps outsiders from accessing it