**Directions:** For each bullet point, tell me what is it and how it works in your own words (from now on, “in your own words” = “working definition”). Copy-pasted definitions will not count even if it is more accurate. If you find yourself just not understanding a concept, that’s okay. Ask but try beforehand.

**Protocols**

* TCP - protocol that establishes a connection-oriented session to exchange data
* UDP – protocol that establishes a connectionless-oriented session to send data
* ARP – protocol used to map IP addresses based off MAC addresses through broadcasting
* DHCP – automates the process of assigning ip addresses within a defined range
* DNS – resolves FQDN’s to IP addresses
* Telnet – remote access service but transmits in clear text
* SSH – secure remote access service
* 1:1 NAT – translating one internal address to one external address and vice versa
* Port Forwarding – the gateway forwards traffic of a specific port to a specific node
* HTTP – protocol used by web servers to define format, transmission, and actions
* HTTPS – secure http using asymmetric PKI to encrypt and decrypt transmissions

**Networking Basics**

* OSI Model – 7 layers used to segment breakdown the process of network enablement and description for network protocol design that standardizes networking.
  + Physical – physical layer that controls signals. Devices include wiring, hubs and other repeats.
  + Data link – encoding and decoding electrical signals into bits. Consists of MAC addressing and switches.
  + Network – Creates a virtual circuit between nodes to route traffic. Consists of routers, IP addresses and TCP/IP suite.
  + Transport – end to end transportation process of data between systems. Consists of TCP and UDP.
  + Session – establishment, management, and termination of connections. Consists of file sharing protocols like NFS and netbios.
  + Presentation – Visible data on screen (ASCII). Includes decryption and encryption of data.
  + Application – managing application services like email, ftp, http, telnet, ssh, etc.
* Encapsulation – enclosing data within another set of data.
* Subnetting – segment a network into smaller networks

**Physical Devices/Layout**

* Physical network topology – psudeo view of how the network layout will visibly be designed.
  + Bus – single cable where all nodes are connected and everyone receives transmissions.
  + Star – single connection that is the source for all other connections
  + Tree – combination of star and bus
* Firewalls – allow and deny traffic to and from network through filtering
* Access points – enables wifi or Bluetooth for wireless devices to provide connectivity
* Router – level 3 networking device that routes traffic based off ip address
* Switch – layer 2 networking device that directs traffic based off destination address. They also segment collision domains. Full duplex = one channel for send and one for receive which gets rid of collision domains (when nodes send packets at the same time)
* Hub – layer 1 networking device that floods received packets to everyone on the network outside of the source. Half duplex which causes collision domains.
* **Device Addresses**
* MAC address – physical address that uniquely identifies the NIC
* IP address – logical address that uniquely identifies the system

**Brownie Points**

If two computers are connected to a single switch for the first time, describe the communication that takes place with a ping request

Typically takes a few pings in order to establish the MAC tables of who is who. Once it receives a ping from an unknown address, it floods all the ports to find who the destination address belongs to and once that specific system replies, the switch will store it and now it’s functioning.