Network + Section 2 - Network Basics

Network Components

- Client - A device used by an end-user to access the network.
    - Can be any device that connects to the network.
- Server - A device that provides resources to the rest of the network.
    - Different servers provide different functions
        - Dedicated Hardware
        - Specialized Software
- Hub - Older technology that connects network devices together / Layer 1 device
    - Hubs can lead to increased network errors
    - Receives information and broadcasts it
- Wireless Access Point (WAP) - A device that allows wireless devices to connect into wired network
    - A WAP acts like a wireless hub
- Switch - A device that connects network devices together (Like a next generations hub)
    - Provides more security and efficiency
- Router - Connects two different networks together and forwards traffic to and from a network
    - Modern routers use IP address (Can be Layer 3)
- Media - Connects two devices or a device to a switch port
    - Each type has its own strengths and limitations
- Wide Area Network (WAN) Link - Physically connects two geographically dispersed networks
    - Connects as internal network to an external one

Network Resources

- Client/Server Model - Uses dedicated server to provide access to files, scanners, printers, and other resources
    - Administration and back are easier
        - Client/Server Benefits
            - Centralized administration
            - Easier management
            - Better scalability
        - Client/Server Drawbacks
            - Higher cost
            - Requires specialized OS
            - Requires dedicated resources
- Peer-to-Peer Model - Peers share resources (files/printers) directly with others
    - Administration and backup is difficult
        - Benefits of Peer-to-Peer
            - Lower cost
            - No dedicated resources
            - No specialized OS
        - Peer-to-Peer Drawbacks

- Decentralized management
- Inefficient for large networks
- Poor Scalability

Network Geography

- Personal Area Network (PAN) - Smallest type of wired or wireless network and covers the least amount of area
- Local Area Network (LAN) - Connects components within a limited distance
    - Up to a few hundred feet
    - Ethernet (IEEE 802.3) or Wi-Fi (IEEE 802.11)
- Campus Area Network (CAN) - Connects LANs that are building-centric across a university, industrial park, or business park
    - Up to a few miles
- Metropolitan Area Network (MAN) - Connects scattered locations across a city or metro area
    - Up to about 25 miles
- Wide Area Network (WAN) - Connects geographically disparate internal networks and consists of leased lines or VPNs
    - Worldwide coverage

Wired Network Topology

- Physical - How devices are connected by media
- Logical - How the actual network traffic flows
- Bus Topology - Uses a single cable where each device taps into by using whether a vampire tap or a T-connector
- Ring Topology - Uses a cable running in a circular loop where each device connects to the ring but data travels in a singular direction/collisions can occur
- Token Ring - Ring topology that uses an electronic token to prevent collisions when communicating on the network
    - FDDI (Fiber Distributed Data Interface) - use two counter-rotating rings for redundancy
    - Modern ring networks are usually FDDI networks
    - If you see ring on the exam, think FDDI and redundancy
- Star Topology - Most popular physical LAN topology where devices connect to a single point
    - If the central device fails, the entire network fails
- Hub-and-Spoke Topology - Similar to Star but with WAN links instead of LAN connections and it is used for connecting multiple sites.
- Full-Mesh Topology - Optimal routing always available as every node connects to every other node
    - This can be quite expensive and may require many resources due to every machine or system being interconnected
- Partial-Mesh Topology - Hybrid of the full mesh and the hub-and-spoke topologies
    - Provides optimal routes between some sites
    - Must consider network traffic patterns

Wireless Network Topologies

- Infrastructure Mode - Uses a wireless access point as a centralized point and support wireless security controls
- Ad Hoc Mode - Decentralized wireless network which creates P2P connections and does not require a router or access point
- Wireless Mesh Topology - Interconnection of different types of nodes, devices, or radios
    - Created redundant and reliable connections

Internet of Things (IoT)

- 802.11 - Wireless networks that can operate in infrastructure or ad hoc models (802.11, a,b,g,n,or ac)
- Bluetooth - Low energy use variant of Bluetooth which allows for a mesh network
- Radio-frequency Identification (RFID) - Uses electromagnetic fields to read data stored in embedded tags
- Near-field Communication (NFC) - Enables two devices to communicate with a 4-cm range
- Infrared (IR) - Operates with line of sight
- Z-Wave - Provides short-range, low-latency data transfer with slower rates and less power consumption that Wi-Fi
    - If you see Z-wave, think automation (exam question)
    - Used primarily for home automation (turning lights on and off, turning sound on and off)
- ANT + - Collection and transfer of sensory data
    - If you see ANT+, think sensors (exam question)
- The S in IoT stands for security…but there is no S in IoT! This is referencing how IoT devices can be a security risk. Ensuring security is imperative.