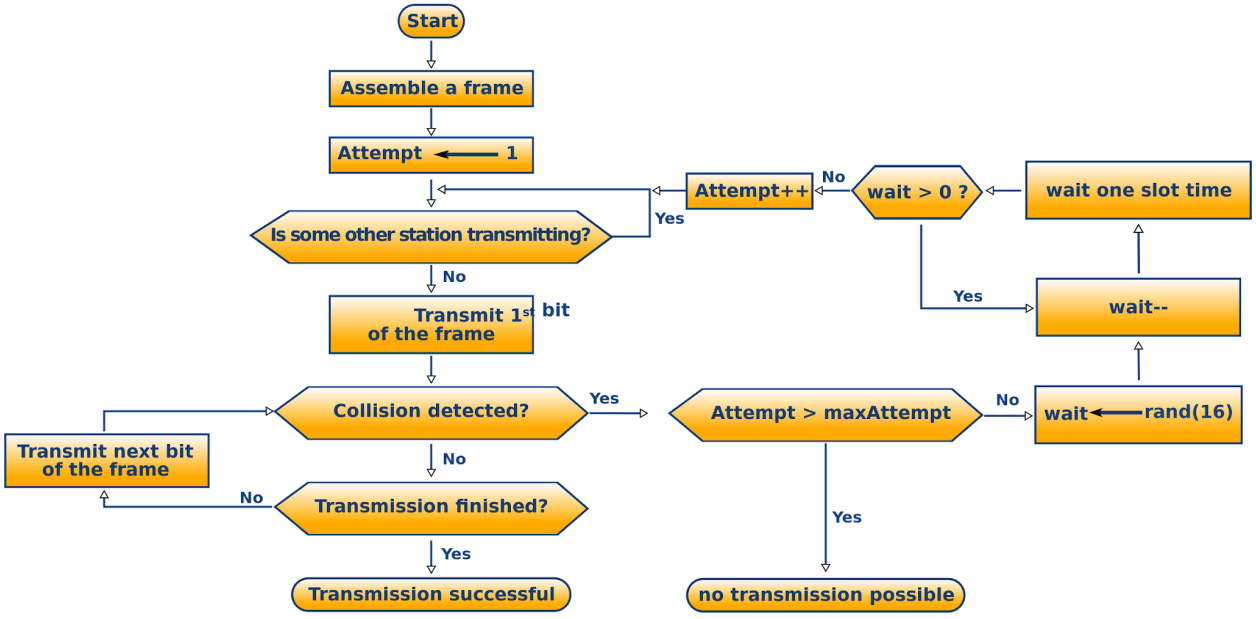
Network + Section 6 Ethernet Fundamentals

Ethernet Fundamentals

- OBJ 1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.
- OBJ 2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.
- OBJ 2.3 Given a scenario, configure and deploy common Ethernet switching features.
- OBJ 4.4 Compare and contrast remote access methods and security implications.
- OBJ 5.5 Given a scenario, troubleshoot general networking issues.

- Early ethernet connections were 10BASE2 (ThinNet) and 10BASE5 (ThickNet)
- 10BASE-T allows up to 10 Mbps of speed but only covers a distance of up to 100 meters.
- How should a network communicate?
    - Deterministic - Very organized and orderly and requires an electronic token to transit.
        - Token bus
        - Toke rings
        - Broken up into chunks of time which can waste a lot of resources.
    - Contention-Based - Very chaotic and can transmit whenever possible. Is susceptible to collisions.
        - Contention-based access is chaotic and can cause collisions.
- Ethernet uses contention-based network access.
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - Prevents collisions by using carrier-sensting to defer transmissions until no other stations are transmitting.



- CSMA
    - Carrier Sensing - determines if there's a signal already being transmitted.
    - Carrier - signal that carries information or data.

    - MA multiple devices that hold the ability to access, listen to, and transmit to that network at the same time.
- CD
    - In ethernet if a collision is detected both ethernet devices will stop transmitting, pick a random number and then wait to retransmit. This is known as a random back of timer. It allows two devices to attempt to retransmit again when the timer hits zero.
- Collision Domain - Each area of the network that shares a single segment.
    - Devices operate in half-duplex mode when connected to a hub.
    - Keep collision domains small inside your networks.
- Ethernet Switch - Increases scalability of a network by creating multiple collision domains.
    - Every single switch port is its own collision domain.
    - Operates in full-duplex mode.

CATEGORY	STANDARD	BANDWIDTH	DISTANCE
CAT 3	10BASE-T	10Mbps	100 meters
CAT 5	100BASE-TX	100 Mbps	100 meters
CAT 5e	1000BASE-T	1000 Mbps	100 meters
CAT 6	1000BASE-T/ 10-GBASE-T	1000/Mbps/10 Gbps	100 meters/ 55 meters
CAT 6a	10GBASE-T	10 Gbps	100 meters
CAT 7	10GBASE-T	10 Gbps	100 meters
CAT 8	40GBASE-T	40 Gbps	30 meters

- Bandwidth - Measures how many bits the network can transmit per second.
- MMF(Multi-mode Fiber)/SMF (Single Mode Fiber)

Standard	Mode	Bandwidth	Distance
100BASE-FX	MMF	100 Mbps	2 kilometers
100BASE-SX	MMF	100 Mbps	300 meters
1000BASE-SX	MMF	1000 Mbps	220-250 meters
1000BASE-LX	SMF/MMF	1000 Mbps	5 Kilometers/550 meters
10GBASE-SR	MMF	10 Gbps	400 meters
10GBASE-LR	SMF	10 Gbps	10 kilometers

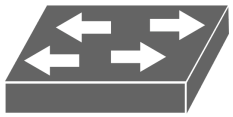
- When it comes to distances there are a few key things that need to be memorized.

1. Copper cables have a maximum distance of 100 meters.
2. Using CAT 6 at 100 meters will limit the speed from 10 Gbps to 1 Gbps.
3. Using CAT 6 at under 55 meters can reach 10 Gbps of speed.
4. Multimode fibers deal with shorter distances, something in the 200 to 500-meter range.
5. Use single mode fiber for long distances.

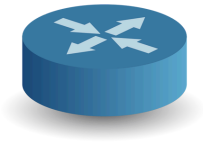
- For the exam…
    - For copper, expect to see questions about specific cable lengths or limitations.
    - For fiber, expect to see questions about multimode and single mode distances.
    - **S** is not Single. This will tell you whether or not that fiber is single mode or multimode fiber.

Network Infrastructure Devices

- Hub - Also known as a multiport repeater, it is a Layer 1 device that connects multiple network devices and workstations.
    - Multiport repeaters.
        - Passive - Repeats signal with no amplification.
        - Active - Repeats signal with amplification. Better for long distances. Multiple active hubs can be used for wide distances, it restarts the 100 meter signal.
        - Smart - Active hub with enhanced features like SNMP. Adds a bit of intelligence.



- Collision Domains - Multiple network segments connected together by hubs.
- Bridge - Analyzed source MAC addresses and makes intelligent forwarding decisions based on the destination MAC in the frames. Layer 2 device.
- Switch - Also known as a multiport bridge, it is a Layer 2 device that connects multiple network segments together. Similar to a multiport bridge
    - Switches make forwarding decisions, just like a bridge.
    - Each port has its own Collision domain.
    - When the switch wants to communicate for the first time it will send out an ARP packet and check its table. If that ARP packet is not in its table it broadcasts to all devices in its broadcast domain. Once the server responds identifying itself it sends a response message and the switch records the MAC address in its ARP table. A connection is established when the MAC address of the machine on the network is identified and they can begin to communicate.
- Router - Layer 3 device that connects multiple networks and makes forwarding decisions based on logical network information.
    - Layer 3 and IP addresses.
    - May have multiple different connectors used to connect to networks.



- Layer 3 Switch - Makes Layer 3 routing decisions and then interconnects enter networks, not just network segments.
    - Layer 3 devices that are used to connect multiple networks together, and can perform routing functions.
    - Each of their ports is going to act as its own broadcast domain and own collision domain.
    - Layer 3 switches are not efficient being used as a router in a large network.

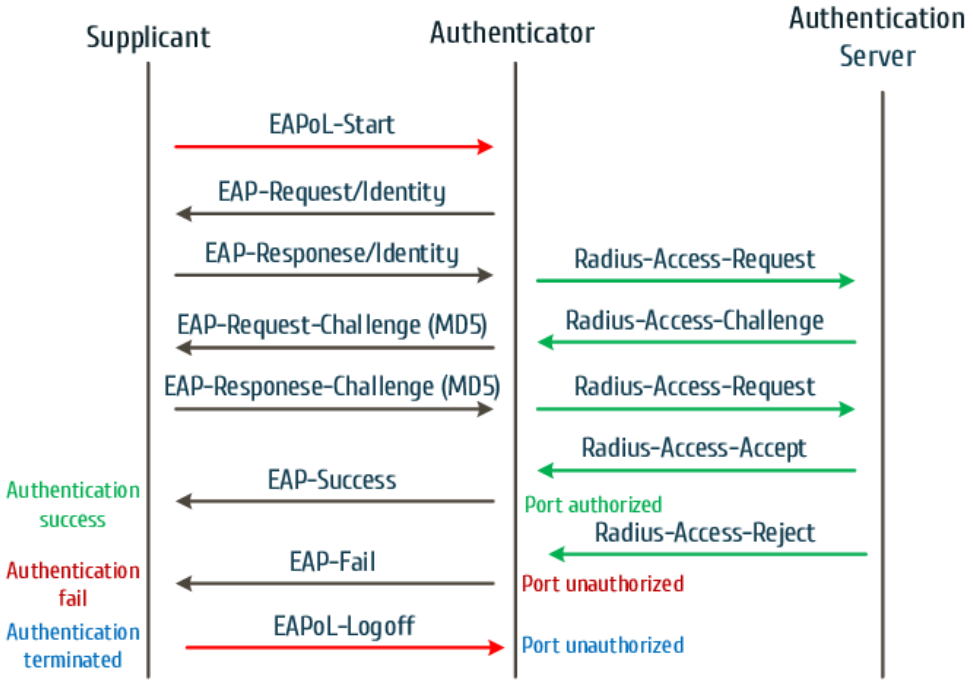
Device Type	Collision Domains	Broadcast Domains	OSI Layer
Hub	1	1	1
Bridge	1 per port	1	2
Switch	1 per port	1	2
Multilayer Switch	1 per port	1 per port	3+
Router	1 per port	1 per port	3+

- For the exam
    - Switch - Layer 2 device focused on MAC addresses.
    - Router - Router Layer 3 device focused on IP addresses.
    - Multilayer or Layer 3 switch.

Additional Ethernet Switch Features

- These additional ethernet switch features are there to enhance multiple things.
    - Network performance
    - Redundancy
    - Security
    - Management
    - Flexibility
    - Scalability
- Link Aggregation (IEEE 802.3ad) - Combines multiple physical connections into a single logical connection to minimize or prevent congestion. Exam tip…IEEE will be asked in the exam and you need to be able to identify what it is.
    - Congestion can occur when ports all operate at the same speed link aggregation can alleviate this .
- Power Over Ethernet (PoE 802.3af PoE+ 802.3at) - Supplies electrical power over ethernet and requires CAT 5 or higher copper cable.
    - PoE 802.3af - Up to 15.4 watts.
    - PoE 802.3at - Up to 25.5 watts.
    - There are two types of devices that use this PSE (Power sourcing equipment) and PD (Powered device).
        - PSE can be something like a Switch.
        - PD may be something like a Voip phone or Wireless Access Point.
    - Must be using a CAT 5 cable or higher.
- Port Monitoring or Mirroring - Makes a copy of all traffic destined for a port and sends it to another port.
    - Helpful to analyze packet flow over a network.
    - This can be done on a switch by setting up port monitoring or port mirroring to collect and analyze traffic.

    - If you have a 24 port switch and all the traffic is running on port one through 23 and you would have it mirrored out on port 24 and attach your sensor there, the network analyst machine, and collect the data and read it.
    - Port mirroring sends a copy of all the traffic on the network from multiple machines and devices.
- User Authentication (802.1x) - Requires users to authenticate themselves before gaining access to the network.



- Management Access and Authentication is used to configure or manage a switch, there are three different methods that can be used.
    - SSH - Remote administration program that allows connection to the switch over a network.
    - Console port - Allows for local administration of the switch using a separate laptop and a rollover cable (DB-9 to RJ-45).
        - Locally plug into it.
        - You can use an RS 232 serial cable, called a rollover cable, which has one end as RF-45 and the other as a DB-9.
    - Out-of-band (OOB) Management - Keeps all network configuration devices on a separate network.
        - Creates another network that sits on top of your network that's used for data.
        - This network is only used to connect to devices and configure them.
- First-Hop Redundancy - Uses Hot Standby Router Protocol (HSRP) to create virtual IP and MAC addresses to provide active and standby routers. Layer 3 switches.
    - There are 3 other redundancy protocols.
        - Gateway Load Balancing Protocol (GLBP)
        - Virtual Router Redundancy Protocol (VRRP)
        - Common Address Redundancy Protocol (CARP)

- MAC Filtering - Permits or denies traffic based on a device's MAC address. We're dealing with switches.
- Traffic Filtering - Permits or denies traffic based on IP addresses or application ports. Router or multilayer switch. Layer 3 IP address, Layer 4 ports.
- Quality of Service (QoS) - Forwards traffic based on priority markings.

Spanning Tree Protocol

- Spanning Tree Protocol (802.1d) - Permits redundant links between switches and prevents looping of network traffic.
    - Availability of networks should be in 5 nines, 99.999%.
- Shortest Path Bridging (SPB) - Used instead of STP for larger network environments.
- Broadcast Storm - Multiple copies of frames being forwarded back and forth which then consumes the network.
    - The network consumes the copies of these packets being sent out which creates more traffic which can crash the network under the weight of this.
- How STP functions.
    - Root bridge - Switch with the lowers bridge ID (BID)
        - Acts as a reference point for the entire spanning tree chooses the lowest BID and that is how the root bridge is elected.
        - BID is made up of a priority value and a MAC address.
    - Non-root bridge - All other switches in an STP topology.
    - Root Port - Every non-root bridge has a single root port which is the closest to the root bridge in terms of cost.
        - Faster cables have lower cost, while slower cables have higher cost.
    - Designated Port - Every network segment has a designated port which is the closest to the root bridge in terms of cost.
        - All the ports on the root bridge are designated ports. They are really fast.
    - Non-Designated Port - Ports that block traffic to create loop-free topology.
        - Blocks are put in place to prevent a broadcast storm from being created.
        - Non-designated ports receive bridge protocol data units (BPDUs).
        - To get to the forwarding state, it has to transition through four states.
            - Blocking - BPDUs are received but not forward.
            - Listening - Populates the MAC address table but does not forward frames.
            - Learning - Processes BPDUs and this is where the switch determines its role in the spanning tree.
            - Forwarding - Forwards frames for operations.
- Link Cost - Associated with the speed of the link - the lower the link's speed, the higher the cost.

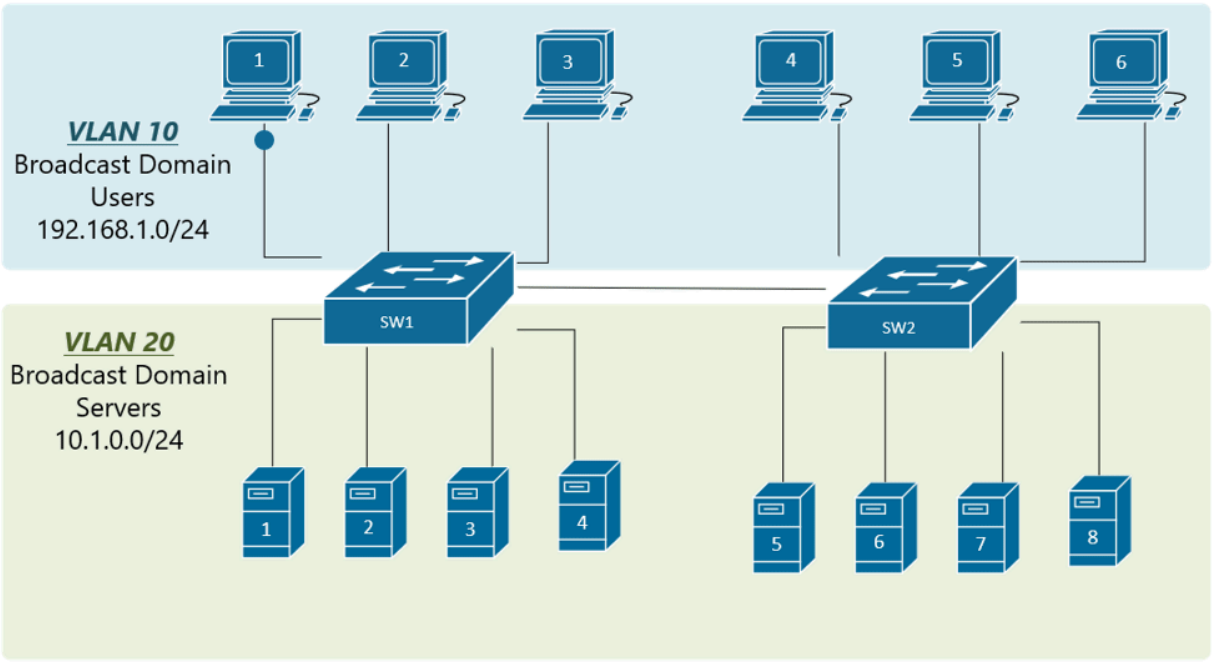
Speed	Ethernet Type	STP Port Cost
10 Mbps	Ethernet	100
100 Mbps	Fast ethernet	19
1 Gbps	Gigabit ethernet	4

10 Gbps	10 - Gigabit ethernet	2

- For the exam
    - Faster cables have lower cost, while slower cables have higher cost.

Virtual Local Area Network

- Virtual Local Area Network (VLAN) - Allows different logical networks to share the same physical hardware and provides added security and efficiency.
    - Before VLANs, different switches were required for each LAN for separation. Switches may have to be at different locations like different floors which made things more difficult.
    - With VLANs this can be consolidated into just two switches.
- VLAN Trunking (801.1q) - Multiple VLANs transmitted over the same physical cable.



- Identifying different VLANs going over this trunk is by using an electronic tag that is 4-bytes long called a 4-byte identifier. There are two parts to this.
    - Tag Protocol Identifier (TPI)
    - Tag Control Identifier (TCI)
- When you have one VLAN and it's left untagged that becomes your native VLAN, referred to as VLAN zero.
- VLANs are great for security and if you're using VLAN trunking, 802.1Q is your standard for VLANs.

Specialized Network Devices

- Virtual Private Network - Creates a secure VPN or virtual tunnel over an untrusted network like the Internet.

- VPN Concentrator - Terminates VPN tunnels and allows for multiple VPN connections in one location.
    - Can be part of a device like a UTM or a firewall.
- VPN Headend - A specific type of VPN concentrator used to terminate IPSec VPN tunnels within a router or other device.
- Firewall - A network security appliance placed at the boundary of a network.
    - Firewalls can be Software or Hardware
    - Stateful or Stateless
- Next-Generation Firewall (NGFW) - Conducts deep packet inspection at Layer 7 and can look through traffic to detect and prevent attacks.
- Intrusion Detection/Prevention System - Recognizes and responds to attacks through signatures and anomalies.
- Proxy Server - A specialized device that makes requests to an external network on behalf of a client.
    - Two functions as to why a proxy server would be implemented.
        - Security, it can perform content filtering and logging.
        - They can have a cache that can store a copy of information that was requested by the user.
- Content Engine/Caching Engine - Dedicated appliance that performs the caching functions of a proxy server.
    - Beneficial for large organizations with a large internet pipe.
- Content Switch/Load Balancer - Distributes incoming requests across various servers in a server farm.

Other Devices

- VoIP Phone - A hardware device that connects to your IP network to make a connection to a call manager within your network.
    - Unified Communications (or Call) Manager - Used to perform the call processing for hardware and software-based IP phones.
        - Configure call manager to route those calls to the public telephone network by connecting it with a telephone provider.
- Printers can be hardwired or connected to the network. They can be assigned a static IP or assigned an IP via DHCP.
- Physical access control devices - they are often connected to a network, usually not directly connected to the main network due to security purposes.
    - Security Gates
    - Turnstiles
    - Door Locks
    - Etc….
- Security cameras will be connected to your security network for larger organizations, they can be insecure devices.
- Heating Ventilation (HVAC) should be placed on there own network for security purposes and may require additional defenses.
- IoT devices should be on their own network due to these devices not being secure.
    - Smart tvs, watches, door bells, etc…
- Industrial Control System (ICS) - Describes the different types of control systems and associated instrumentation.

    - This includes devices, systems, networks, controls, used to operate and automate industrial processes.
    - This normally consists of electronic sensors in equipment built specifically to have an effect on the physical world.
- Supervisory Control and Data Acquisition (SCADA) - Acquires and transmits data from different systems to a central panel for monitoring and control.
- ICS and SCADA also run on networks. These systems are engineered in Segmented or separated manner due to security issues. Normally these systems are not connected to the internet.