CompTIA Network+ (N10-008)

Study Notes

Introduction

- **Introduction**
    - CompTIA Network+ certification is considered the first networking certification for anyone entering the IT or cybersecurity industry
        - It provides a solid foundation and baseline knowledge of networking, covering configuration, management, and troubleshooting of network infrastructure within a company or organization
    - This certification is designed for beginners with less than one year of IT operations or administration experience or for those who have completed the A+ examination
    - On the Network+ exam, knowledge of the CompTIA A+ exam is assumed, and the course builds upon the foundational knowledge of hardware, software, and computer networks
    - CompTIA Network+ (N10-008) certification exam consists of five domains or areas of knowledge
        - 24% of Networking Fundamentals
        - 19% of Network Implementations
        - 16% of Network Operations
        - 19% of Network Security
        - 22% of Network Troubleshooting

- While the course won't follow the order of the official exam objectives, each section will cover all objectives, and videos will specify the objectives covered
- Exam Format and Structure
  - The Network+ exam allows 90 minutes to answer up to 90 questions
  - Questions include multiple-choice and multiple-select, where you may need to choose 2 or 3 correct answers
  - Performance-Based Questions (PBQs) simulate job functions in a simulated environment
  - The exam requires a passing score of at least 720 points out of 900
  - Exam vouchers can be purchased from store.comptia.org or at diontraining.com/vouchers for a 10% discount
- Tips for Success in the Course
  - Closed Captioning
    - Enable closed captions for accurate understanding, especially for non-native English speakers
  - Playback Speed Control
    - Adjust the playback speed to suit your preference for efficient learning
  - Study Guide
    - Download the PDF study guide from Lesson 2 to take notes and highlight important information
  - Facebook Group
    - Join the Facebook group at facebook.com/groups/diontraining for community support, daily questions, and assistance from over 25,000 students

Networks Basics

Objectives:

- 1.2 - Explain the characteristics of network topologies and network types
- 2.1 - Compare and contrast various devices, their features, and heir appropriate placement on the network

- **Overview of Networks**
    - Computer Networks
        - What comes to mind?
        - Is it limited to computers?
        - Is it limited to Ethernet, WiFi, or fiber?
    - Purpose of Networks
        - To make connections between machines
        - Converged networks combine multiple types of traffic like data, video, and voice
        - We expect 99.999% availability (The 5 9's)
            - Only 5 minutes downtime per year
    - Network Traffic Examples
        - File sharing
        - Video chatting
        - Surfing the Web
        - Social Media
        - Streaming Video
        - E-mail
        - Messaging

        - VoIP

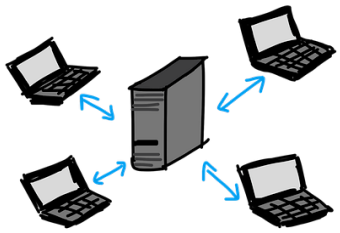
- **Network Components**
    - *Client*
        - Device end-user accesses the network with
        - Workstation, laptop, tablet, smartphone, television, server, or other terminal devices
        - Can be any device that connects to the network
    - *Server*
        - Provides resources to the rest of the network
        - Different servers provide different functions, such as an E-mail server, Web server, File server, Chat server, and Print server
        - Can be a dedicated server hardware/software or can be a device that is acting like a server for a particular function
    - *Hub*
        - Older technology to connect networked devices, such as clients and servers
        - Can be interconnected to provide more ports, but leads to increased network errors
        - Receives information in one port and rebroadcasts it out all the other ports
    - *Wireless Access Point (WAP)*
        - Device that allows wireless devices to connect into a wired network
        - Commonly used in home, small business, and even some large enterprise networks
        - Acts as a wireless hub

- *Switch*
  - Connects networked devices such as clients and servers (like a hub)
  - Switches learn what devices are on which switch ports
  - Switches only forward traffic received from a port to the destination port based on the device's MAC address
  - Provides more security and efficiently uses available bandwidth
- *Router*
  - Connect two different networks together
  - Intelligently forwards traffic to and from a network based on its logical address
  - Most modern routers use Internet Protocol (IP) address to determine routing of traffic
- *Media*
  - Connect two devices or a device to a port
  - Made from copper cable, fiber optic cable, or radio frequency waves (WiFi)
  - Each type has strengths and limitations, such as its available bandwidth, capacity, distance that can be covered, and cost to install and maintain
- *Wide Area Network (WAN) Link*
  - Physically connects networks together
  - Numerous WAN links are available
    - Leased lines
    - DSL
    - Cable
    - Fiber Optic
    - Satellite

- Cellular
- Microwave

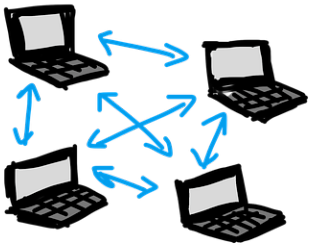
- Connects internal network to external networks, such as a SOHO network to Internet

- **Network Resources**
  - *Client/Server Model*



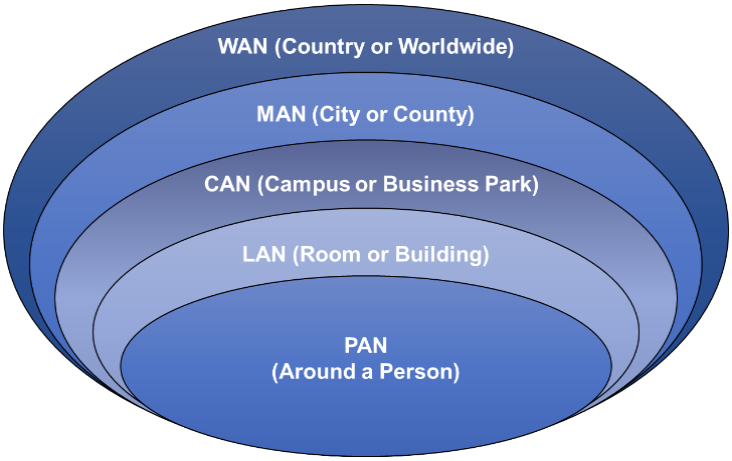
    - Uses dedicated server to provide access to files, scanners, printers, and other resources
    - Administration and backup are easier since resources are located on a few key servers
  - Benefits of Client/Server
    - Centralized administration
    - Easier management
    - Better scalability
  - Drawbacks of Client/Server
    - Higher cost
    - Requires dedicated resources
    - Requires network operating system

- *Peer-to-Peer Model*



  - Peers (PCs) share resources (files/printers) with each other directly
  - Administration and backup are more difficult since resources are located on a many PCs which adds to the administrative burden
- Benefits of Peer-to-Peer
  - Lower cost
  - No dedicated resources required
  - No specialized operating system required
- Drawbacks of Peer-to-Peer
  - Decentralized management
  - Inefficient for large networks
  - Poor scalability

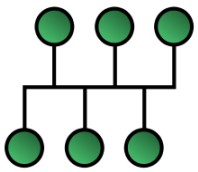
- **Network Geography**



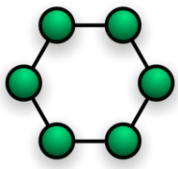
  - *Personal Area Network (PAN)*
    - Smallest type of wired or wireless network
    - Covers the least amount of area (few meters)
    - Some examples
      - Bluetooth cellphone to car
      - USB hard drive to laptop
      - Firewire video camera to computer
  - *Local Area Network (LAN)*
    - Connects components in a limited distance
    - Each segment is limited to short distances, such as 100 meters with CAT 5 cabling
    - Consists of Ethernet (IEEE 802.3) or WiFi networks (IEEE 802.11)
      - Internal wired or wireless networks

- *Campus Area Network (CAN)*
  - Connects building-centric LANs across a university, industrial park, or business park
  - Covers many square miles and buildings
  - Some examples
    - College campus
    - Business Parks
    - Military bases
- *Metropolitan Area Network (MAN)*
  - Connects scattered locations across a city
  - Larger than a CAN, but smaller than a WAN
  - Covers up to a 25-mile radius in larger cities
  - Some examples
    - City departments like the police department
    - Community college with campuses spread across a county
- *Wide Area Network (WAN)*
  - Connects geographically disparate internal networks
  - Consists of leased lines or Virtual Private Networks tunneled over the Internet
  - Covers distances around the country or around the world
  - Some examples
    - The Internet (largest WAN)
    - Connecting two private corporate networks from New York to Seattle

- **Wired Network Topology**
  - Defining Network Topology
    - *Physical Topology*
      - How devices are physically connected by media
    - *Logical Topology*
      - How the actual traffic flows in the network
  - *Bus Topology*

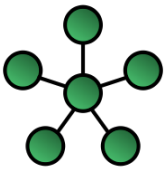


    - Uses a cable running through area that required network connectivity
    - Each device “taps” into the cable using either a T connector or vampire tap
    - Old technology, not commonly used anymore
    - Devices on cable form single collision domain
  - *Ring Topology*

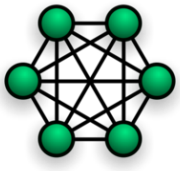


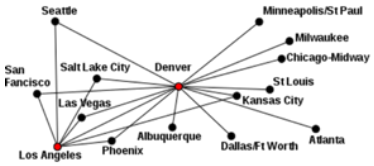
    - Uses a cable running in a circular loop
    - Each device connects to the ring, but data travels in a singular direction
    - FDDI (Fiber networks) used two counter-rotating rings for redundancy
    - On token ring networks, devices wait for a turn to communicate on ring by passing a token

- *Star Topology*



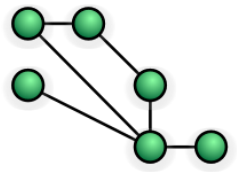
  - Most popular physical LAN topology
  - Devices connect to a single point
  - Commonly used with Ethernet cabling, but wireless or fiber is also used
  - If the central device fails, the entire network fails
- *Hub-and-Spoke Topology*
  - Used for connecting multiple sites
  - Similar to Star but with WAN links instead of LAN connections
  - Not redundant, if central office (hub) fails, the whole network can fail
- *Full-Mesh Topology*





  - Most redundant topology
  - Every node connects to every other node
  - Optimal routing is always available
  - Very expensive to maintain and operate
  - Number of Connections
  - x= n(n - 1) / 2

- *Partial-Mesh Topology*



  - Hybrid of the full-mesh and the hub-and-spoke topologies
  - Provides optimal routes between some sites, while avoiding the expense of connecting every site
  - Must consider network traffic patterns to design it effectively

- **Wireless Network Topology**
  - *Infrastructure Mode*
    - Most common type of wireless network
    - Requires centralized management
    - Uses a wireless access point as a centralized point like a star topology
    - Supports wireless security controls
  - *Ad Hoc Mode*
    - Decentralized wireless network
    - No routers or access points are required
    - Forwarding decisions for data on the network are made dynamically
    - Allows creation/joining of networks “on-the-fly”
    - Creates P2P connections
  - *Wireless Mesh Topology*
    - Interconnection of different types of nodes or devices
    - Consists of clients, routers, and gateways
    - Utilizes different radio frequencies to extend and expand access

        - Reliable and redundant connections

- **Internet of Things (IoT)**
    - Internet of Things (IoT) Technologies
        - *802.11*
            - Operates as infrastructure or ad hoc
        - *Bluetooth*
            - Low energy use variant of Bluetooth which allows for a mesh network
        - *RFID*
            - Uses electromagnetic fields to read data stored in embedded tags
        - *NFC*
            - Enables two electronic devices to communicate within a 4 cm range
        - *Infrared (IR)*
            - Operates with line of sight
        - *Z-Wave*
            - Provides short-range, low-latency data transfer at rates and power consumption lower than Wi-Fi
            - Used primarily for home automation
        - *Ant+*
            - Collection and transfer of sensor data
            - Used with remote control systems (tire pressure, TVs, lights)

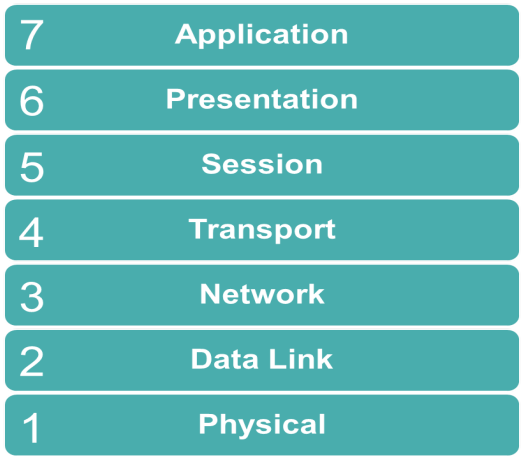
OSI Model

Objectives:

- 1.1 - Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts
- 5.3 - Given a scenario, use the appropriate network software tools and commands

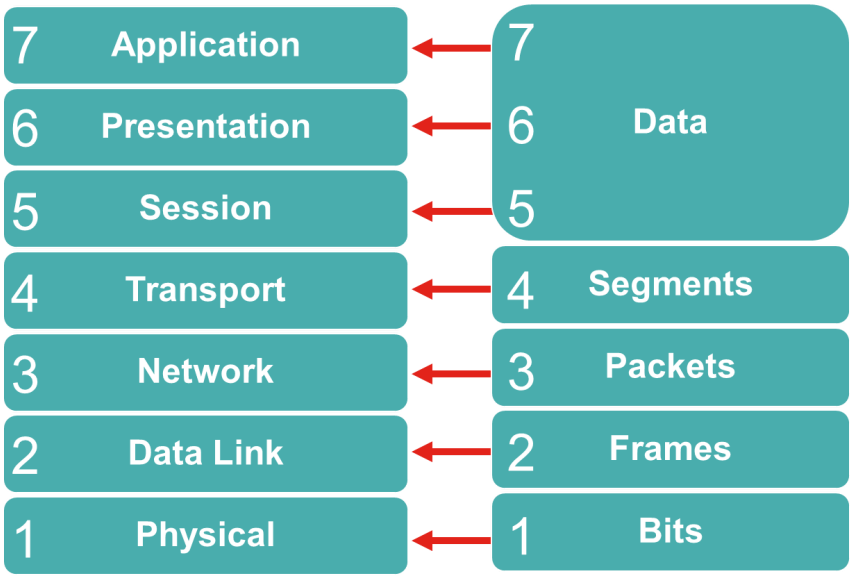
- **OSI Model Overview**
  - *OSI Model (Open Systems Interconnection)*
    - Developed in 1977 by International Organization for Standardization (ISO)
    - Called the OSI model or OSI stack
    - Consists of 7 layers
    - Useful in troubleshooting networks
    - Serves as a reference model in networks
  - Purpose of Reference Model
    - Categorize functions of the network into particular layer(s)
    - Compare technologies across different manufacturers
    - By understanding its functions, you can understand how best to communicate with that device

- OSI Model Layers



***P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way!*

- Data Types in the OSI Model



***D**on't **S**ome **P**eople **F**ear **B**irthdays?*

- **Layer 1 (Physical)**
    - *Physical Layer (Layer 1)*
        - Transmission of bits across the network
        - Physical and electrical characteristics
        - Characteristics
            - How bits are represented on the medium
            - Wiring standards for connectors and jacks
            - Physical topology
            - Synchronizing bits
            - Bandwidth usage
            - Multiplexing strategy
    - How are bits represented on the medium?
        - Electrical voltage (copper wiring) or light (fiber optics) represent 1's and 0's (bits)
        - Current State
            - If 0 volts, then 0 is represented
            - If +/- 5 volts, then 1 is represented
        - Transition Modulation
            - If it changed during the clock cycle, then a 1 is represented, otherwise, a 0
    - How are the cables wired?
        - TIA/EIA-568-B is standard wiring for RJ-45 cables and ports
        - Crossover cables use T-568A and T-568B
        - Straight-thru cables typically use T-568B on both ends, but could use T-568A on both

- How are the cables connected?
  - Layer 1 devices view networks from a physical topology perspective
  - Includes the following
    - Bus
    - Ring
    - Star
    - Hub-and-Spoke
    - Full Mesh
    - Partial Mesh
- How is communication synchronized?
  - *Asynchronous*
    - Uses start bits and stop bits to indicate when transmissions occur from sender to receiver
  - *Synchronous*
    - Uses a reference clock to coordinate the transmissions by both sender and receiver
- How is bandwidth utilized?
  - *Broadband*
    - Divides bandwidth into separate channels
    - Example
      - Cable TV
  - *Baseband*
    - Uses all available frequency on a medium (cable) to transmit data and uses a reference clock to coordinate the transmissions by both sender and receiver

- Example
  - Ethernet

- How can we get more out of a limited network?
  - *Time-Division Multiplexing (TDM)*
    - Each session takes turns, using time slots, to share the medium between all users
  - *Statistical Time-Division Multiplexing (StatTDM)*
    - More efficient version of TDM, it dynamically allocates time slots on an as-needed basis instead of statically assigning
  - *Frequency-Division Multiplexing (FDM)*
    - Medium is divided into various channels based on frequencies and each session is transmitted over a different channel
      - Broadband
- Examples at Layer 1
  - Cables
    - Ethernet
    - Fiber optic
  - Radio frequencies
    - Wi-Fi
    - Bluetooth
  - Infrastructure devices
    - Hubs
    - Wireless Access Points
    - Media Converters

- **Layer 2 (Data Link)**
    - *Data Link Layer (Layer 2)*
        - Packages data into frames and transmitting those frames on the network, performing error detection/correction, and uniquely identifying network devices with an address (MAC), and flow control
            - MAC
            - Physical addressing
            - Logical topology
            - Method of Transmission
            - Link Layer Control (LLC)
                - Connection services
                - Synchronizing transmissions
    - *Media Access Control (MAC)*
        - Physical addressing
            - Uses 48-bit address assigned to a network interface card (NIC) by manufacturer
            - First 24-bits is the vendor code
            - Second 24-bits is a unique value
        - Logical topology
            - Layer 2 devices view networks logically
            - Ring, bus, star, mesh, hub-and-spoke, ...
        - Method of transmission
            - Many devices are interconnected
            - Determines whose turn it is to transmit to prevent interference with other devices

- *Logical Link Control (LLC)*
  - Provides connection services
  - Acknowledgement of receipt of a message
  - *Flow Control*
    - Limits amount of data sender can send at one time to keep receiver from becoming overwhelmed
  - *Error Control*
    - Allows receiver to let sender know when an expected data frame wasn't received or was corrupted by using a checksum
- How is communication synchronized?
  - *Isochronous*
    - Network devices use a common reference clock source and create time slots for transmission
    - Less overhead than synchronous or asynchronous
  - *Synchronous*
    - Network devices agree on clocking method to indicate beginning and end of frames
    - Uses control characters or separate timing channel
  - *Asynchronous*
    - Network devices reference their own internal clocks and use start/stop bits
- Examples at Layer 2
  - Network Interface Cards (NIC)
  - Bridges
  - Switches

- **Layer 3 (Network)**
    - *Network Layer (Layer 3)*
        - Forwards traffic (routing) with logical address
            - Example
                - IP Address (IPv4 or IPv6)
        - Logical addressing
        - Switching
        - Route discovery and selection
        - Connection services
        - Bandwidth usage
        - Multiplexing strategy
    - *Logical Address*
        - Numerous routed protocols were used for logical addressing over the years
            - AppleTalk
            - Internetwork Packet Exchange (IPX)
            - Internet Protocol (IP)
        - Only Internet Protocol (IP) remains dominant
            - IPv4
            - IPv6
    - How should data be forwarded or routed?
        - *Packet Switching*
            - Known as “Routing”
            - Data is divided into packets and forwarded
        - *Circuit Switching*
            - Dedicated communication link is established between two devices

        - *Message Switching*
            - Data is divided into messages, similar to packet switching, except these messages may be stored then forwarded
    - Route Discovery and Selection
        - Routers maintain a routing table to understand how to forward a packet based on destination IP address
        - Manually configured as a static route or dynamically through a routing protocol
            - RIP
            - OSPF
            - EIGRP
    - Connection Services
        - Layer 3 augment Layer 2 to improve reliability
        - *Flow Control*
            - Prevents sender from sending data faster than receiver can get it
        - *Packet Reordering*
            - Allows packets to be sent over multiple links and across multiple routes for faster service
    - *Internet Control Message Protocol (ICMP)*
        - Used to send error messages and operational information about an IP destination
        - Not regularly used by end-user applications
        - Used in troubleshooting (ping and traceroute)
    - Examples at Layer 3
        - Routers
        - Multilayer switches

        - IPv4 protocol
        - IPv6 protocol
        - Internet Control Message Protocol (ICMP)

- **Layer 4 (Transport)**
    - *Transport Layer (Layer 4)*
        - Dividing line between upper and lower layers of the OSI model
        - Data is sent as segments
        - TCP/UDP
        - Windowing
        - Buffering
    - *TCP (Transmission Control Protocol)*
        - Connection-oriented protocol
        - Reliable transport of segments
            - If segment is dropped, protocol detects it and resends segment
        - Acknowledgements received for successful communications
        - Used for all network data that needs to be assured to get to its destination
    - *UDP (User Datagram Protocol)*
        - Connectionless protocol
        - Unreliable transport of segments
            - If dropped, sender is unaware
        - No retransmission
        - Good for audio/video streaming
        - Lower overhead for increased performance

- TCP vs UDP

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

- *Windowing*
  - Allows the clients to adjust the amount of data sent in each segment
  - Continually adjusts to send more or less data per segment transmitted
    - Adjusts lower as number of retransmissions occur
    - Adjusts upwards as retransmissions are eliminated
- *Buffering*
  - Devices, such as routers, allocate memory to store segments if bandwidth isn't readily available
  - When available, it transmits the contents of the buffer
  - If the buffer overflows, segments will be dropped
- Examples at Layer 4
  - TCP
  - UDP
  - WAN Accelerators
  - Load Balancers

        - Firewalls

- **Layer 5 (Session)**
    - *Session Layer (Layer 5)*
        - Think of a session as a conversation that must be kept separate from others to prevent intermingling of the data
        - Setting up sessions
        - Maintaining sessions
        - Tearing down sessions
    - Setting up a Session
        - Check user credentials
        - Assign numbers to session to identify them
        - Negotiate services needed for session
        - Negotiate who begins sending data
    - Maintaining a Session
        - Transfer the data
        - Reestablish a disconnected session
        - Acknowledging receipt of data
    - Tearing Down a Session
        - Due to mutual agreement
            - After the transfer is done
        - Due to other party disconnecting
    - Examples at Layer 5
        - *H.323*
            - Used to set up, maintain, and tear down a voice/video connection

        - *NetBIOS*
            - Used by computers to share files over a network

- **Layer 6 (Presentation)**
    - *Presentation Layer (Layer 6)*
        - Responsible for formatting the data exchanged and securing that data with proper encryption
        - Functions
        - Data formatting
        - Encryption
    - *Data Formatting*
        - Formats data for proper compatibility between devices
            - ASCII
            - GIF
            - JPG
        - Ensures data is readable by receiving system
        - Provides proper data structures
        - Negotiates data transfer syntax for the Application Layer (Layer 7)
    - *Encryption*
        - Used to scramble the data in transit to keep it secure from prying eyes
        - Provides confidentiality of data
        - Example
            - TLS to secure data between your PC and website
    - Examples at Layer 6
        - HTML, XML, PHP, JavaScript, …
        - ASCII, EBCDIC, UNICODE, …

        - GIF, JPG, TIF, SVG, PNG, …
        - MPG, MOV, …
        - TLS, SSL, …

- **Layer 7 (Application)**
    - *Application Layer (Layer 7)*
        - Provides application-level services
            - Not Microsoft Word or Notepad
        - Layer where the users communicate with the computer
        - Functions
            - Application services
            - Service advertisement
    - *Application Services*
        - Application services unite communicating components from more than one network application
        - Examples
            - File transfers and file sharing
            - E-mail
            - Remote access
            - Network management activities
            - Client/server processes
    - *Service Advertisement*
        - Some applications send out announcements
        - States the services they offer on the network
        - Some centrally register with the Active Directory server instead

        - Examples
            - Printers
            - File servers
    - Examples at Layer 7
        - E-mail (POP3, IMAP, SMTP)
        - Web Browsing (HTTP, HTTPS)
        - Domain Name Service (DNS)
        - File Transfer Protocol (FTP, FTPS)
        - Remote Access (TELNET, SSH)
        - Simple Network Management Protocol (SNMP)

- **Encapsulation**
    - The process of putting headers (and sometimes trailers) around some data

- **Decapsulation**
    - Action of removing the encapsulation that was applied
    - If we move down the OSI layers from 7 to 1, we encapsulate data
    - If we move upward from layers 1 to 7, we decapsulate data
    - *Protocol Data Unit*
        - Single unit of information transmitted within a computer network
            - Layer 1 - bits
            - Layer 2 - frames
            - Layer 3 - packets
            - Layer 4 - segments if TCP or datagrams if UDP

- *SYN (or synchronization) Flag*
  - The most well-known flag in TCP communications because it is used to synchronize the connection during the three-way handshake
- *ACK (or acknowledgement) Flag*
  - Used during the three-way handshake, but it is also used to acknowledge the successful receipt of packets
- *FIN (or finished) Packet*
  - Used to tear down the virtual connections created using the three-way handshake and the SYN flag
  - The FIN flag always appears when the last packets are exchanged between a client and server and the host is ready to shutdown the connection
- *RST (or reset) Flag*
  - Used when a client or server receives a packet that it was not expecting during the current connection
- *PSH (or PUSH) Flag*
  - Used to ensure that the data is given priority and is processed at the sending or receiving ends
- *URG (or urgent) Flag*
  - It is like the PUSH flag and identifies incoming data as “urgent”
  - The main difference is PSH is used by a sender to indicate data with a higher priority level where URG is sent to tell the recipient to process it immediately and ignore anything else in queue
    - Source and Destination Ports
      - Just like the ones used in UDP, they dictate where the data is coming from and where it is going to

- Length
  - Used to indicate how many bytes the UDP packet is, including its header and its data
- Checksum
  - Not a mandatory field, but it can be used to provide some validation that the UDP data being sent was received with some level of integrity

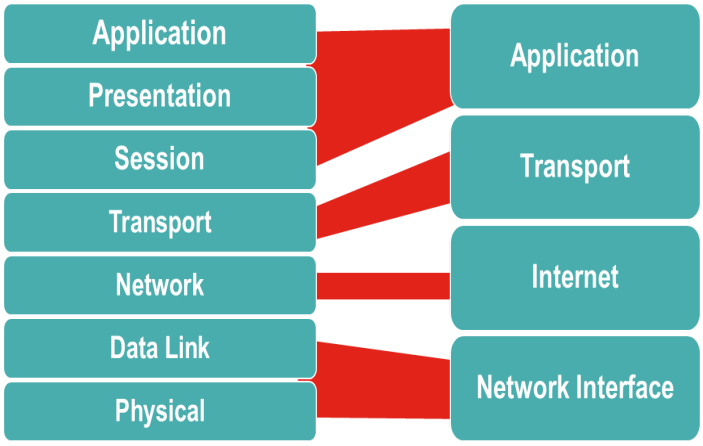
- *MAC Address*
  - A physical address that is used to identify a network card on the local area network
  - Allows the source to find the destination by using this type of addressing
- *EtherType Field*
  - Used to indicate which protocol is encapsulated in the payload of the frame
  - As data moves from layer 7 to layer 1, that data is encapsulated
    - At layer 4, we add our source and destination ports
    - At layer 3, we add our source and destination IP addresses
    - At layer 2, we add our source and destination MAC addresses
  - Once we get to layer 1, we are simply transmitting our layer 2 frames as a series of 1's and 0's over the medium
  - Once that host is found, it will keep decapsulating the information all the way up to layer 7, where its application can read and understand the underlying data

TCP/IP Model

Objectives:

- 1.1 - Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts
- 1.5 - Explain common ports and protocols, their application, and encrypted alternatives
- 5.3 - Given a scenario, use the appropriate network software tools and commands

- **TCP/IP Model**
  - *TCP/IP Model*
    - Also known as TCP/IP stack or the DoD Model
    - Alternative to the OSI Model
    - More relevant model for network designers since it's based on TCP/IP
    - Only a 4-layer model
  - OSI Model to TCP/IP Model



  - *Network Interface (Layer 1)*
    - Physical and electrical characteristics
    - Describes how to transmit bits across the network (1's and 0's)
    - Determines how interface uses network medium

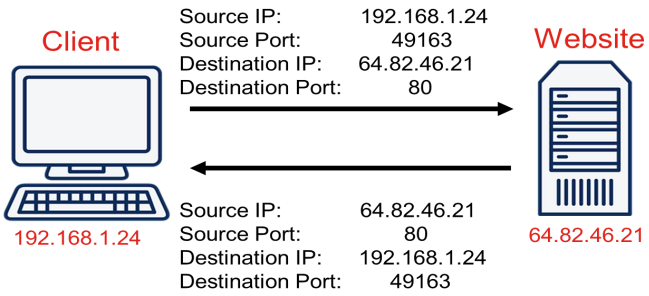
- Coaxial, Optical fiber, or Twisted-pair copper cabling
- Examples
  - Ethernet
  - Token Ring
  - FDDI
  - RS-232

- *Internet (Layer 2)*
  - Packages data into IP datagrams
    - Contains source and destination IPs
    - Forwards datagrams between hosts across the networks
  - Routes IP datagrams across networks
  - Connectivity occurs externally
  - Examples
    - IP
    - ICMP
    - ARP
    - RARP
- *Transport (Layer 3)*
  - Provides communication session management between hosts
  - Defines level of service and status of connection used for transport
  - Examples
    - TCP
    - UDP
    - RTP

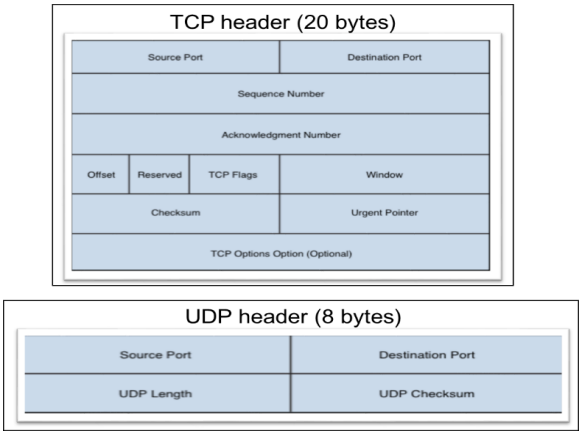
- *Application (Layer 4)*
  - Defines TCP/IP application protocols
  - Defines how programs interface with the transport layer service
  - Layer with which the user interacts
  - Examples
    - HTTP
    - TELNET
    - FTP
    - SNMP
    - DNS
    - SMTP
    - SSL
    - TLS

- **Data Transfer Over Networks**
  - *Ports*
    - Port numbers can be 0 to 65,535
    - "Well-known" & Reserved Ports
      - Ports 0 to 1023
    - Ephemeral Ports
      - Short-lived transport port that is automatically selected from a predefined range
      - Ports 1024 to 65,535

- Data Transfer



- IPv4 Packets
  - Source Address
    - IP of sender
  - Destination Address
    - IP of receiver
  - IP Flags
    - Allows packet fragmentation
  - Protocol
    - Is this packet using TCP or UDP?
- Overhead of TCP and UDP



- **Ports and Protocols**
  - *File Transfer Protocol FTP (Port 20, 21)*
    - Transfers computer files between a client and server on a computer network
    - Unsecure method
    - Data transferred in the clear
  - *Secure Shell SSH (Port 22)*
    - Cryptographic network protocol for operating network services securely over an unsecured network
    - Best known for remote login to computer systems by users
  - *SSH File Transfer Protocol SFTP (Port 22)*
    - Provides file access, file transfer, and file management over any reliable data stream
  - *Telnet (Port 23)*
    - Provides bidirectional interactive text-oriented communication facility using a virtual terminal connection
    - Like SSH, but insecure
  - *Simple Mail Transfer Protocol SMTP (Port 25)*
    - Internet standard for sending electronic mail
    - RFC 821 was defined originally in 1982
    - RFC 5321 developed in 2008 (current version)
  - *Domain Name Service DNS (Port 53)*
    - Hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network
    - Converts domain names to IP addresses

- *Dynamic Host Control DHCP (Port 67, 68)*
  - DHCP server dynamically assigns an IP address and other network configuration parameters to a client
  - Enables computers to request IP addresses and networking parameters automatically
  - Reduces burden on network administrators
- *Trivial File Transfer TFTP (Port 69)*
  - Transmits files in both directions of a client-server application
  - Used for booting an operating system from a local area network file server
  - Doesn't provide user authentication or directory visibility
  - Essentially a stripped-down version of FTP
- *HyperText Transfer HTTP (Port 80)*
  - Foundation of data communication for WWW
  - Designed for distributed, collaborative, and hypermedia presentation across many devices
- *Post Office Protocol v3 POP3 (Port 110)*
  - Used by local email clients to retrieve email from a remote server over TCP/IP connection
- *Network Time Protocol NTP (Port 123)*
  - Provides clock synchronization between computer systems over packet-switched, variable-latency data networks
  - Created in 1985, one of the oldest Internet protocols in current use
- *NetBIOS (Port 139)*
  - Network Basic Input/Output System

        - Provides services allowing applications on separate computers to communicate over a local area network for file and printer sharing
    - *Internet Message Access Protocol IMAP (Port 143)*
        - Provides e-mail clients to retrieve e-mail messages from a mail server over a TCP/IP connection
        - Allows the end user to view and manipulate the messages as if they're stored locally
    - *Simple Network Management SNMP (Port 161)*
        - Provides collection and organization of information about managed devices on IP networks
        - Can modify that information to change device behavior, commonly used in network devices
    - *Lightweight Directory Access LDAP (Port 389)*
        - Open, vendor-neutral, industry standard for accessing and maintaining distributed directory information services
        - LDAP and Active Directory use this port
    - *HTTP Secure HTTPS (Port 443)*
        - Foundation of ecommerce on WWW
        - Designed for adding security to the insecure HTTP protocol
    - *Server Message Block SMB (Port 445)*
        - Provides shared access to files, printers, and miscellaneous communications between devices on a network
    - *System Logging Protocol Syslog (Port 514)*
        - Used to send logging data back to a centralized server
    - *Simple Mail Transfer Protocol Transport Layer Security SMTP TLS (Port 587)*
        - Secure and encrypted way to send emails

- *LDAP Secure LDAPS (Port 636)*
  - Open, vendor-neutral, industry standard for accessing and maintaining distributed directory information services
  - Provides secure directory services
- *Internet Message Access Protocol over SSL IMAP over SSL (Port 993)*
  - Secure and encrypted way to receive emails
- *Post Office Protocol Version 3 over SSL POP3 over SSL (Port 995)*
  - Secure and encrypted way to receive emails
- *Structured Query Language Server Protocol SQL (Port 1433)*
  - Used for communication from a client to the database engine
- *SQLnet Protocol (Port 1521)*
  - Used for communication from a client to an Oracle database
- *MySQL (Port 3306)*
  - Used for communication from a client to the MySQL database engine
- *Remote Desktop Protocol RDP (Port 3389)*
  - Proprietary protocol developed by Microsoft
  - Provides a user with a graphical interface to connect to another computer over a network connection
  - User employs RDP client software for this purpose and the other computer must run RDP server software
- *Session Initiation Protocol SIP (Port 5060, 5061)*
  - Provides signaling and controlling multimedia communication sessions in applications
  - Used for Internet telephony for voice and video calls, VOIP, and instant messaging

- Ports to remember

Service	Description	Port Number	Service	Description	Port Number
FTP	File Transfer	20, 21	LDAP	Directory Services	389
SSH	Secure Remote Access	22	HTTPS	Secure Web Browsing	443
SFTP	Secure File Transfer	22	SMB	Windows File Sharing	445
Telnet	Unsecure Remote Access	23	Syslog	System Logging	514
SMTP	Sending Emails	25	SMTP TLS	Secure Sending of Emails	587
DNS	Domain Name Service	53	LDAPS	Secure Directory Services	636
DHCP	Dynamic Host Control	67, 68	IMAP SSL	Secure Receiving of Emails	993
TFTP	Trivial File Transfer	69	POP3 SSL	Secure Receiving of Emails	995
HTTP	Web Browsing	80	SQL	Database Communication	1433
POP3	Receiving Emails	110	SQLnet	Oracle DB Communication	1521
NTP	Network Time	123	MySQL	MySQL DB Communication	3306
NetBIOS	Windows File Sharing	139	RDP	Remote Desktop	3389
IMAP	Receiving Emails	143	SIP	VoIP and Video Calls	5060, 5061
SNMP	Network Management	161, 162			

- **IP Protocol Types**
  - *Transmission Control Protocol (TCP)*
    - A transport protocol that operates at layer 4 of the OSI model
    - Used on top of the Internet Protocol for the reliable packet transmission
    - Operates by conducting a three-way handshake between a client and a server, and then establishing the connection
    - TCP is considered a connection-oriented method of communication
  - *User Datagram Protocol (UDP)*
    - A lightweight data transport protocol that also works on top of IP
    - Can detect if its packets are corrupted when they are received by a client using a checksum, but there is no connection and no sequencing to the UDP segments

- Great for some applications, like streaming audio and video, but it definitely does NOT provide reliable delivery of the data

- *Internet Control Message Protocol (ICMP)*
  - A network level protocol that is used to communicate information about network connectivity issues back to the sender
  - ICMP is used a lot by network technicians during troubleshooting, but it is also used by attackers to conduct ping scans and network mapping
- *Generic Routing Encapsulation (GRE) Protocol*
  - A tunneling protocol that was developed by Cisco to encapsulate a wide variety of network layer protocols inside a virtual point-to-point or point-to-multipoint link over an Internet Protocol network
  - Important to set a smaller maximum transmission unit or MTU size on the tunnel
  - It does not provide any encryption
- *Internet Protocol Security (IPsec) Protocol*
  - Set of secure communication protocols at the network or packet processing layer that is used to protect data flows between peers
    - *Authentication Header (AH)*
      - A protocol within IPSec that provides integrity and authentication
    - *Encapsulating Security Payload (ESP)*
      - Provides encryption and integrity for the data packets sent over IPsec
      - Backwards-compatible with most IP routers including those that were not designed to work with IPsec initially

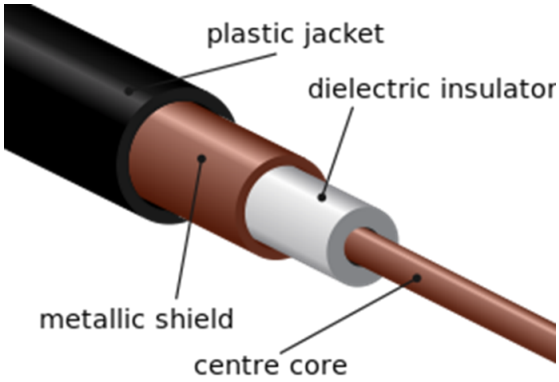
Media and Cabling Distribution

Objectives:

- 1.3 - Summarize the types of cables and connectors and explain which is the appropriate type for a solution
- 5.2 - Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools

- **Media**
    - Material used to transmit data over the network

- **Copper Media**
    - Types of Media
        - Three categories
            - Copper
            - Fiber optic
            - Wireless
        - Each category is divided into subcategories
        - Each has different specifications and uses
    - Coaxial Cable (Coax)
        - Inner
            - Insulated conductor or center wire passes data
        - Outer
            - Braided metal shield used to help shield and protect the data transmission
            - Provides EMI resistance due to shielding



- Coaxial Cables
  - *RG-6*
    - Commonly used by local cable companies to connect individual homes
  - *RG-59*
    - Typically used to carry composite video between two nearby devices, such as from a cable box to the television
- Coaxial Connectors
  - *F-connector*
    - Typically used for cable TV and cable modem connections
  - *BNC*
    - Termed Bayonet Neill-Concelman or British Naval Connector
    - Was used for 10BASE2 Ethernet networks
- *Twinaxial Cable*
  - Similar to coaxial cable but uses two inner conductors to carry the data instead of just one
- *Serial Cable*
  - Usually have a series of straight copper wires inside a single cable or plastic jacket

- *DB-9 or DB-25 (RS-232)*
  - 9-pin or 25-pin D-subminiature
  - Used for asynchronous serial communications and connecting to an external modem

- Twisted Pair Cables
  - Most popular physical LAN media type
  - Eight individually insulated strands of copper wire inside each cable
  - Each pair twisted together to reduce EMI
    - Tighter twists = Less EMI
  - Types
    - *Unshielded Twisted Pair (UTP)*
      - Number of twists determines how much EMI can be blocked
        - CAT 6 has more twists per inch than CAT 5
      - UTP is cheaper than STP
      - Media of choice in most LANs
    - *Shielded Twisted Pair (STP)*
      - Wires are twisted in pairs and surrounded in a metallic shielding to minimize EMI
      - Outer shielding minimizes EMI, but makes STP cost more than UTP

- Twisted Pair Connectors
  - *RJ-45*
    - 8-pin connector in Ethernet networks
    - Most Ethernet use only 4-pins

- *RJ-11*
  - 6-pin connector
  - Commonly only 2 or 4 pins are used
  - Commonly found in telephone systems

- *Registered Jack (RJ)*
  - Used to carry voice or data which specifies the standards a device needs to meet to connect to the phone or data network
- *Bandwidth*
  - Theoretical measure of how much data could be transferred from a source to its destination
- *Throughput*
  - Actual measure of how much data transferred from a source to its destination

CATEGORY	STANDARD	BANDWIDTH	DISTANCE
CAT 3	10BASE-T	10 Mbps	100 meters
CAT 5	100BASE-TX	100 Mbps	100 meters
CAT 5e	1000BASE-T	1000 Mbps	100 meters
CAT 6	1000BASE-T/ 10GBASE-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

- Cable Lengths
  - Keep cable runs under 70 meters from the IDF to the office

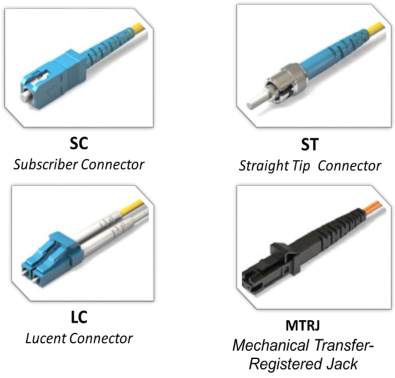
- *Straight-Through Patch Cables*
  - Contains the exact same pinout on both ends of the cable
  - T-568B is the preferred standard for wiring a building if no pre-existing pattern is used
    - *Data Terminating Equipment (DTE)*
      - "Endpoint" devices that connect to a piece of data communications equipment or DCE (e.g. laptops, desktops, servers, and routers)
    - *Data Communications Equipment (DCE)*
      - Includes things like switches, modems, hubs, and bridges
    - Connecting DTE and DCE devices
      - Straight-through
        - DTE to DCE
        - DCE to DTE
      - Crossover
        - DTE to DTE
        - DCE to DCE
- *Crossover Cables*
  - Swaps the send and receive pins on the other end of the cable when the connector and its pinout are created
- *Pinouts (568A/568B)*
  - TIA/EIA-568A and TIA/EIA-568B are standard
  - Orange and Green pairs swap
- *Medium Dependent Interface Crossover (MDIX)*
  - An automated way to electronically simulate a crossover cable connector even if using a straight-through patch cable

        - If a switch doesn't support MDIX, use a crossover cable to make them talk
    - Plenum and Non-Plenum Cable
        - *Plenum Cable*
            - A special coating put on a UTP or an STP cable that provides a fire-retardant chemical layer to the outer insulating jacket
            - Minimizes dangerous fumes if cable on fire
            - Safe for use in ceilings, walls, and raised floors
        - *Non-plenum Cable*
            - Also known as PVC
            - Normal UTP/STP rated cable
            - Cannot be used in raised floors, ceilings, or walls

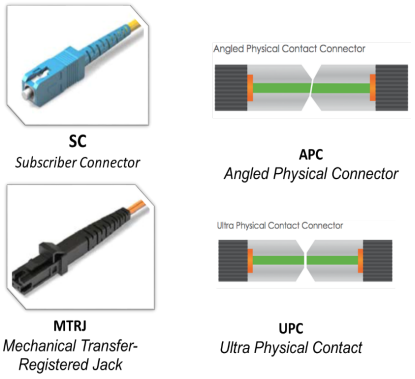
- **Fiber Media**
    - *Fiber Optic Cables*
        - Uses light from an LED or laser to transmit information through a glass fiber
            - Immune to EMI
            - Uses light instead of electricity
        - Benefits
            - Greater range (many miles)
            - Greater data-carrying capacity (measured in Tbps)
        - Types
            - Multimode Fiber (MMF)
            - Single-Mode Fiber (SMF)

- *Single-Mode Fiber (SMF)*
  - Used for longer distances and has smaller core size which allows for only a single mode of travel for the light signal
  - SMF's core size is 8.3-10µ in diameter
- *Multimode Fiber (MMF)*
  - Used for shorter distances and has larger core size which allows for multiple modes of travel for the light signal
  - MMF's core size is 50-100µ in diameter
  - Up to 2 kms or less

Fiber Optic Connectors



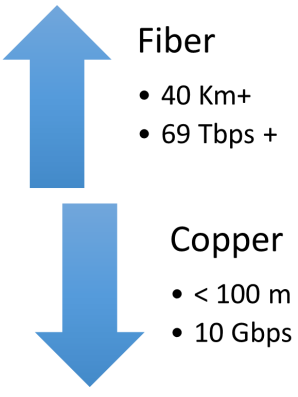
Specialized SC Connectors



- *Wavelength Division Multiplexing (WDM)*
  - Combines multiple signals into one signal and sends over a single fiber optic strand using different wavelengths of the laser light source

	Coarse WDM (CWDM)	Dense WDM (DWDM)
Wavelength channels	Up to 18 channels	Up to 80 channels
Channel distance	20nm	0.8nm
Speed	Up to 10 Gbps (Ethernet) Up to 16 Gbps (Fiber)	Up to 8 Tbps (100 Gbps/channel)

- **Transceivers**
  - Copper vs Fiber Optic Cables



    - Fiber-Optic Advantages
      - Higher bandwidth

- Longer distances
- Immune to EMI
- Better security

- Copper Advantages
- Less expensive
- Easy to install
- Inexpensive tools

- *Media Converters*
- Convert media from one format to another
- Layer 1 device
- Physical conversion of signal only
- Examples
- Ethernet to Fiber Optic
- Fiber Optic to Ethernet
- Coaxial to Fiber
- Fiber to Coaxial

- *Transceivers*
- Device that sends (transmits) and receives data
- *Bidirectional*
- Devices take turns communicating
- Known as half-duplex
- Duplex
- *Full Duplex*
- Occurs when devices can both communicate at the same time

- *Half Duplex*
  - Occurs when devices can either transmit or receive, but cannot do both at the same time

- Types of transceivers used in switches and routers

Transceiver	Speed
Small form-factor pluggable (SFP)	Up to 4.2 Gbps
SFP+	Up to 16 Gbps
Quad small form-factor pluggable (QSFP)	Up to 40 Gbps
QSFP+	Up to 41.2 Gbps
QSFP28	Up to 100 Gbps
QSFP56	Up to 200 Gbps

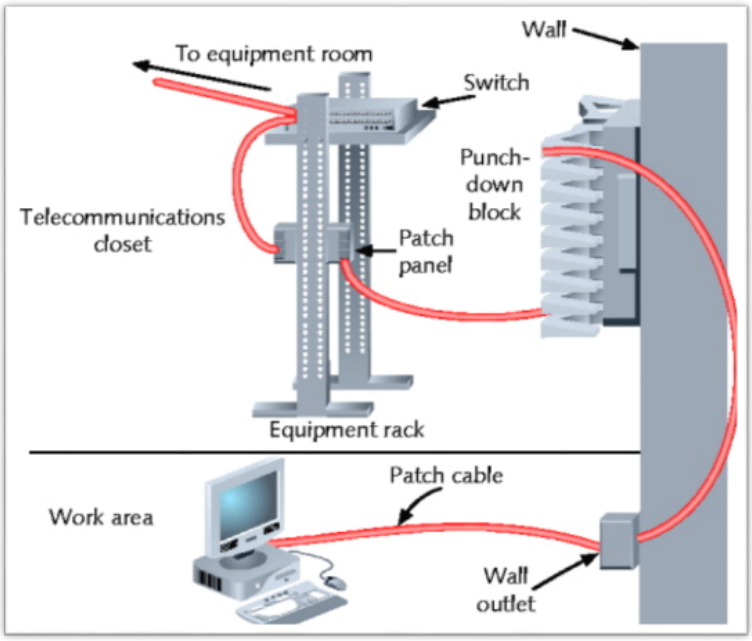
  - *GBIC*
    - Standard, hot-pluggable gigabit Ethernet transceiver (copper or fiber)
  - *Small Form-factor Pluggable (SFP)*
    - Compact, hot-pluggable optical module transceiver
    - Support up to 4.25 Gbps
    - Known as Mini-GBIC
  - *SFP+*
    - Enhanced SFP
    - Support up to 16 Gbps
  - *Quad Small Form-factor Pluggable (QSFP)*
    - Compact, hot-pluggable optical module transceiver
    - Supports up to 100 Gbps

- **Cable Distribution**
    - An organized system to connect the network's backbone in the main distribution frame to the intermediate distribution frames and finally to the end user's wall jacks
    - *Cable Distribution System*
        - Use an organized system that is hierarchical
            - *Demarcation Point*
                - The entrance facilities where you WAN connection will enter your building
        - Components
            - Entrance facilities
            - MDF
            - Cross-connect facilities
            - IDF
            - Backbone wiring
            - Telecommunications closet
            - Horizontal wiring
            - Patch Panels
            - Work area
    - Punch Down Blocks
        - *66 Block*
            - Used for phones and older LAN wiring
            - Causes crosstalk due to proximity of cables
            - Bad choice for higher-speed LAN wiring
                - Do not use for CAT 5 or above

- *110 Block*
  - Used for higher-speed network wiring
    - Required for CAT 5 or above cabling
- *Krone Block*
  - A proprietary European alternative to a 110 block
- *BIX Block*
  - Another proprietary punch down block that comes in various sizes
  - If you are going to work on a BIX block, you will need a BIX-specific punch down tool

- *Patch Panels (Copper)*
  - Device with jacks to connect wiring from the jack to a network switch in a flexible manner
  - Has punch downs (like a 110 block) on the back side that is used to connect wiring to wall jacks in building
  - Front has RJ-45 jacks
- *Patch Panels (Fiber)*
  - Connect fiber jacks throughout building to a single patch panel in network closet
  - Front uses patch cables to connect different wall jacks and switch ports

- Example of Cable Distribution



Typical Copper Cable Installation

Ethernet Fundamentals

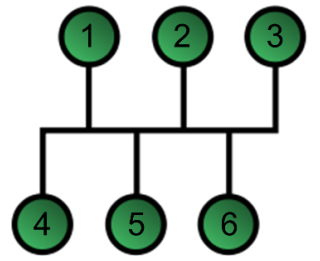
Objectives:

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

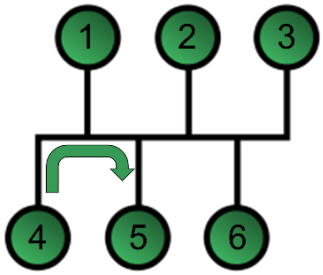
- **Ethernet Fundamentals**
    - Ethernet Fundamentals
        - In early computer networks, there were many different network technologies competing for a portion of the market share
        - Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), and others fought for dominance
        - Currently, Ethernet is dominant for Layer 1
        - Due to Ethernet's popularity, it is important to understand the fundamentals of Ethernet
    - Origins of Ethernet
        - Was first run over coax cables (10Base5, 10Base2)
        - Ethernet has changed to using twisted pair cables
        - 10BASE-T is Unshielded Twisted Pair
            - Maximum speed: 10 Mbps
            - Maximum distance: 100 meters

- How should devices access the network?
  - *Deterministic*
    - Very organized and orderly
    - Need an electronic token to transmit
    - For example, Token Ring networks
  - *Contention-based*
    - Very chaotic
    - Transmit (almost) whenever you want
    - For example, Ethernet networks
- Carrier Sense Multiple Access/Collision Detect (CSMA/CD)
  - Ethernet devices transmit based on a principle called Carrier Sense Multiple Access/Collision Detect (CSMA/CD)
  - *Carrier Sense*
    - Listen to the wire, verify it is not busy
  - *Multiple Access*
    - All devices have access at any time
  - *Collision Detect*
    - If two devices transmit at the same time, a collision occurs
    - Back off, wait a random time, and try again

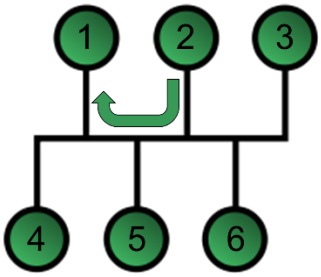
- Example of CSMA/CD



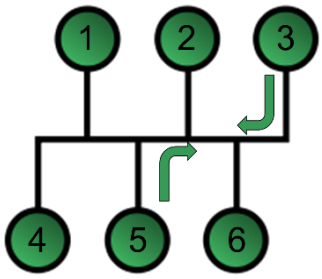
Ethernet devices on a shared network segment



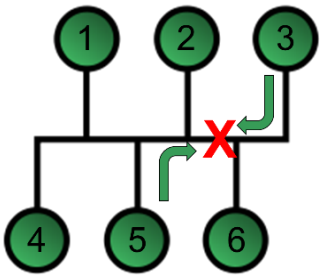
Communication on an Ethernet segment



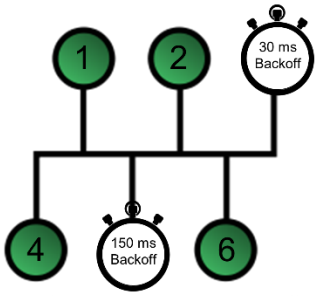
Communication on an Ethernet segment



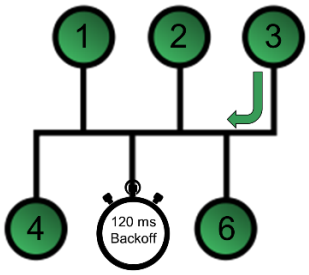
Collision on an Ethernet segment



Collision on an Ethernet segment



Recovering from a collision with random backoff timers



Traffic flowing again while other device waits for timer

- *Collision Domains*
  - Comprised of all devices on a shared Ethernet segment (everything on same cable or hub)
  - Devices operate at half-duplex when connected to a hub (Layer 1 device)
  - Devices must listen before they transmit to avoid collisions when operating as CSMA/CD

- Collision Domains with Switches
  - Ethernet switches increase scalability of the network by creating multiple collision domains
  - Each port on a switch is a collision domain, no chance of collisions, and increases speed
  - Switches can operate in full-duplex mode
- Speed Limitations

Ethernet Type	Bandwidth Capacity	Description
Ethernet	10 Mbps	10 million bits per second
Fast Ethernet	100 Mbps	100 million bits per second
Gigabit Ethernet	1000 Mbps (1 Gbps)	1 billion bits per second
10-Gigabit Ethernet	10 Gbps	10 billion bits per second
100-Gigabit Ethernet	100 Gbps	100 billion bits per second

  - Bandwidth is the measure of how many bits the network can transmit in 1-second (bps)
  - Type of cable determines the bandwidth capacity of the network
- Distance Limitations

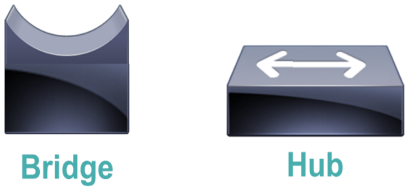
Ethernet Standard	Media Type	Bandwidth Capacity	Distance Limitation
10BASE-T	Cat 3 or higher	10 Mbps	100 m
100BASE-TX	Cat 5 or higher	100 Mbps	100 m
1000BASE-TX	Cat 6 or higher	1 Gbps	100 m
1000BASE-SX	MMF	1 Gbps	220 m
1000BASE-LX	MMF	1 Gbps	550 m
1000BASE-LX	SMF	1 Gbps	5 km
1000BASE-ZX	SMF	1 Gbps	70 km

*** Not an exhaustive list of cable types ***

- Type of cable determines the distance limitation of the network

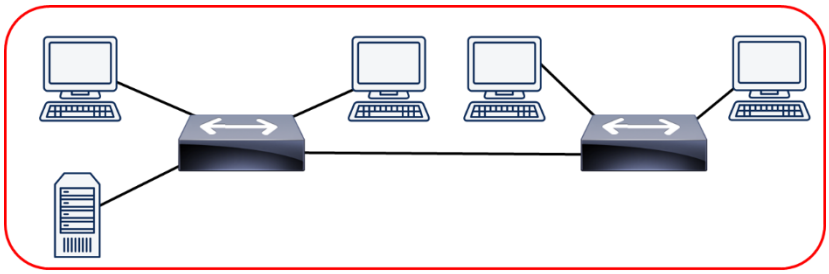
- **Network Infrastructure Devices**
  - Network Infrastructure
    - Primary devices used in our networks

    - Devices they evolved from

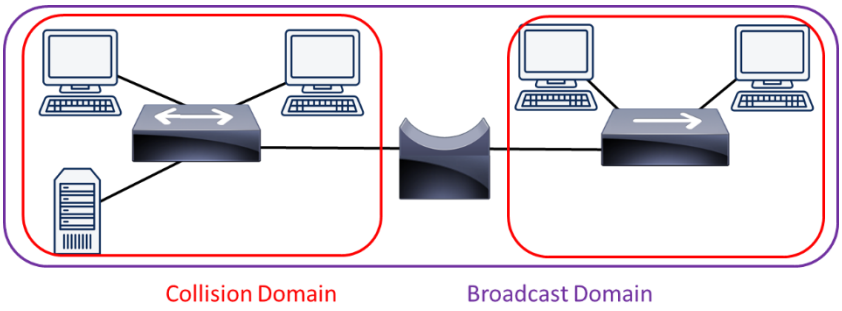


  - *Hub*
    - Layer 1 device used to connect multiple network devices/workstations
    - Known as Multiport Repeaters
    - Three basic types of ethernet hubs
      - *Passive Hub*
        - Repeats signal with no amplification
      - *Active Hub*
        - Repeats signal with amplification
      - *Smart Hub*
        - Active hub with enhanced features like SNMP

- *Collision Domains*
  - Multiple network segments connected together by hubs
  - Hubs (layer 1) were used to connect multiple network segments together
  - Each LAN segment becomes a separate collision domain



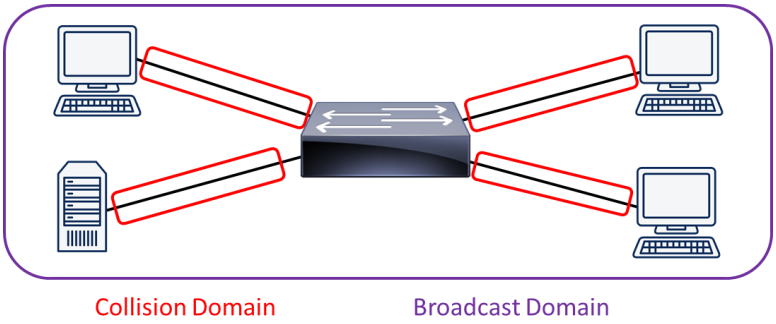
- *Bridges*
  - Bridges analyze source MAC addresses in frames entering the bridge and populate an internal MAC address table
  - Makes intelligent forwarding decisions based on destination MAC address in the frames



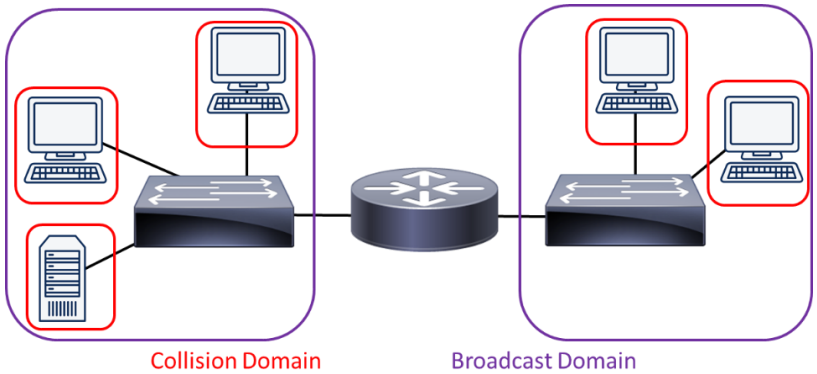
- *Switch*
  - Layer 2 device used to connect multiple network segments together
  - Essentially a multiport bridge
  - Switches learn MAC addresses and make forwarding decisions based on them

- Switches analyze source MAC addresses in frames entering the switch and populate an internal MAC address table based on them

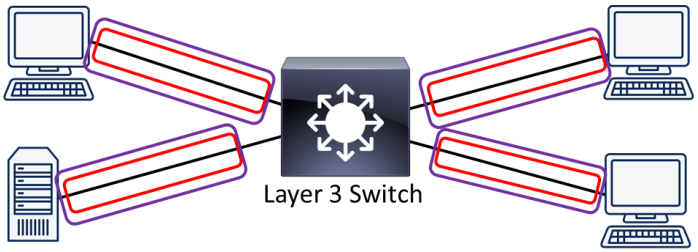
- *Layer 2 Switch*
  - Each port on a switch represents an individual collision domain
  - All ports belong to the same broadcast domain



- *Router*
  - Layer 3 device used to connect multiple networks together
  - Make forwarding decisions based on logical network address information
    - Such as using IP addresses (IPv4 or IPv6)
  - Routers are typically more feature rich and support a broader range of interface types than multilayer switches
  - Each port is a separate collision domain
  - Each port is a separate broadcast domain



- *Layer 3 Switch*
  - Layer 3 device used to connect multiple network segments together
  - Can make Layer 3 routing decisions and interconnect entire networks (like a router), not just network segments (like a switch)



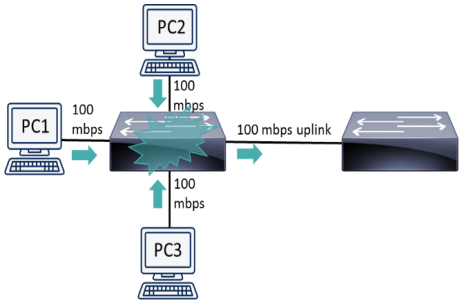
- Summary of Network Infrastructure

Device Type	Collision Domains Possible	Broadcast Domains Possible	OSI Layer of Operation
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+

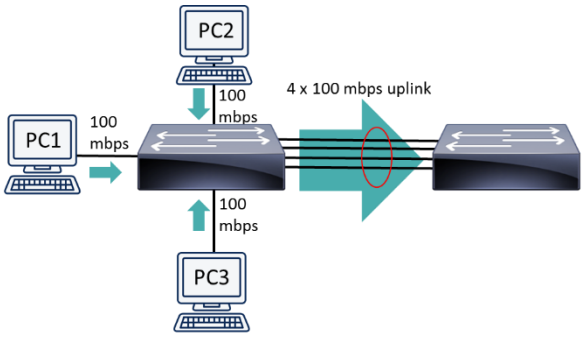
- **Additional Ethernet Features**
  - Features to enhance network performance, redundancy, security, management, flexibility, and scalability
    - Common switch features
      - Virtual LANs (VLANs)

- Trunking
- Spanning Tree Protocol (STP)
- Link aggregation
- Power over Ethernet
- Port monitoring
- User authentication

- *Link Aggregation (802.3ad)*
  - Congestion can occur when ports all operate at the same speed



  - Allows for combination of multiple physical connections into a single logical connection
  - Bandwidth available is increased and the congestion is minimized or prevented

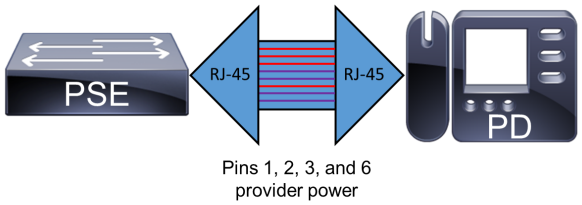


- *Power Over Ethernet (PoE 802.3af, PoE+ 802.3at)*
  - Supplies electrical power over Ethernet
    - Requires CAT 5 or higher copper cable

- Provides up to 15.4 watts of power to device
- PoE+ provides up to 25.5 W of power to device

■ Two Device Types

- Power Sourcing Equipment (PSE)
- Powered Device (PD)

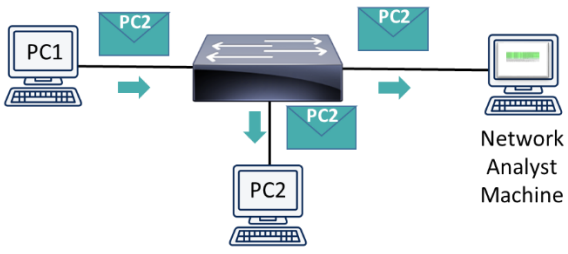


○ *Port Monitoring or Mirroring*

■ Helpful to analyze packet flow over network

- Connect a network sniffer to a hub and it sees all
- But, switches require port monitoring for network analyzer to see all the traffic

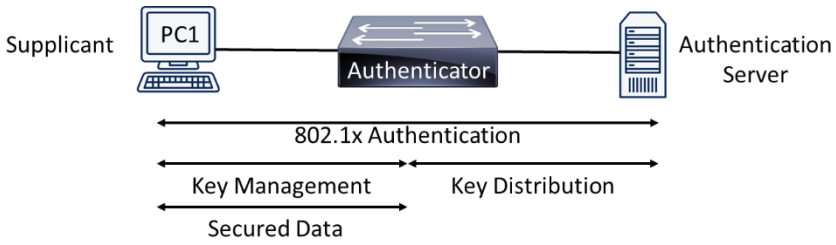
■ Port mirroring makes a copy of all traffic destined for a port and sends it to another port



○ *User Authentication (802.1x)*

■ For security purposes, switches can require users to authenticate themselves before gaining access to the network

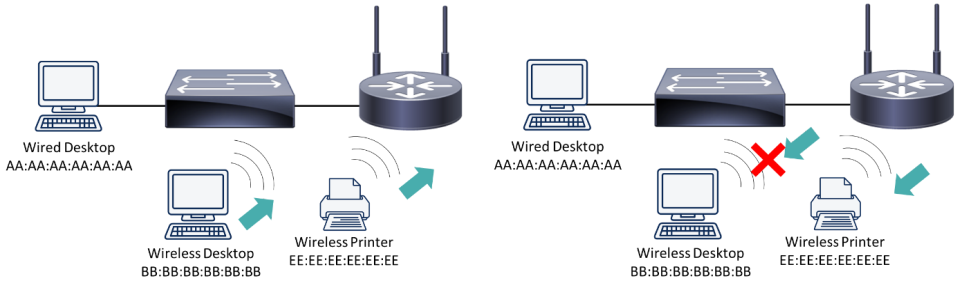
■ Once authenticated, a key is generated and shared between the supplicant (device wanting access) and the switch (authenticator)



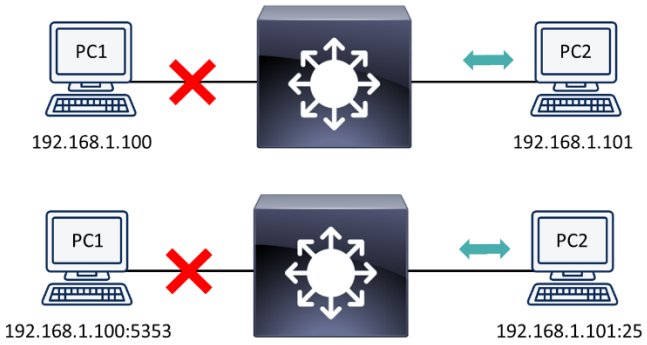
- Authentication server checks the supplicant's credentials and creates the key
- Key is used to encrypt the traffic coming from and being sent to the client

- Management Access and Authentication
  - To configure and manage switches, you can use two options
    - *SSH*
      - Remote administration program that allows you to connect to the switch over the network
    - *Console Port*
      - Allows for local administration of the switch using a separate laptop and a rollover cable (DB-9 to RJ-45)
- *Out-of-band (OOB)*
  - Management involves keeping all network configuration devices on a separate network
- *First-Hop Redundancy*
  - Hot Standby Router Protocol (HSRP) uses virtual IP and MAC addresses to provide a "active router" and a "standby router"
    - HSRP is a Cisco-proprietary protocol
    - If Active is offline, then standby answers

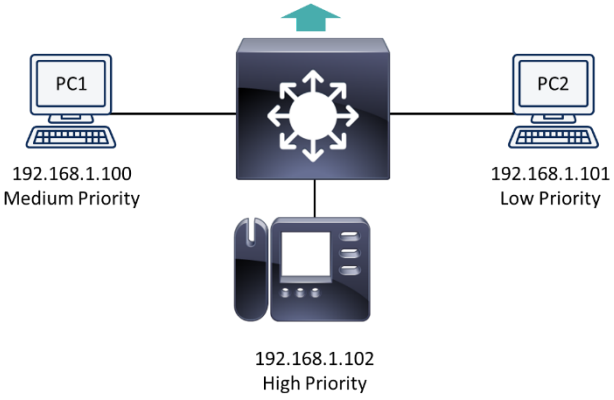
- Other First-Hop Redundancy Protocols
  - Gateway Load Balancing Protocol (GLBP)
    - Cisco-proprietary protocol
  - Virtual Router Redundancy Protocol (VRRP)
    - Open-source protocol
  - Common Address Redundancy Protocol (CARP)
    - Open-source protocol
- *MAC Filtering*
  - Permits or denies traffic based on a device's MAC address to improve security



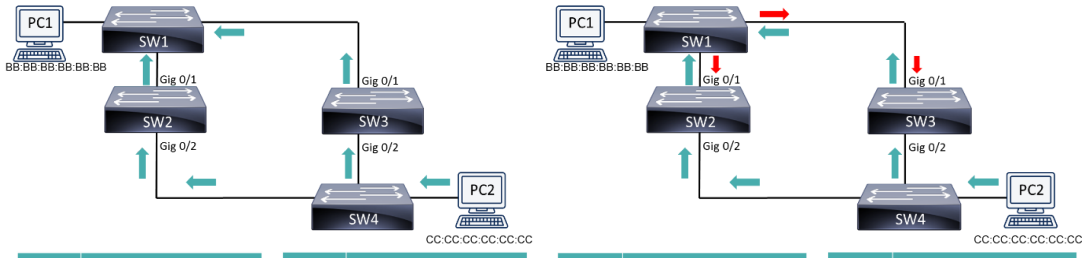
- *Traffic Filtering*
  - Multilayer switches may permit or deny traffic based on IP addresses or application ports



- *Quality of Service (QoS)*
  - Forwards traffic based on priority markings



- **Spanning Tree Protocol (STP) (802.1D)**
  - Permits redundant links between switches and prevents traffic loops
  - Availability is measured in 9's
    - Five 9's is 99.999% uptime and allows only 5 minutes down per year
  - Shortest Path Bridging (SPB) is used for larger network environments instead
  - Without STP, MAC Address table corruption can occur



Port	MAC Address
Gig 0/1	CC:CC:CC:CC:CC:CC
Gig 0/2	CC:CC:CC:CC:CC:CC

Switch 2
MAC Address Table

Port	MAC Address
Gig 0/1	
Gig 0/2	CC:CC:CC:CC:CC:CC

Switch 3
MAC Address Table

Port	MAC Address
Gig 0/1	CC:CC:CC:CC:CC:CC
Gig 0/2	CC:CC:CC:CC:CC:CC

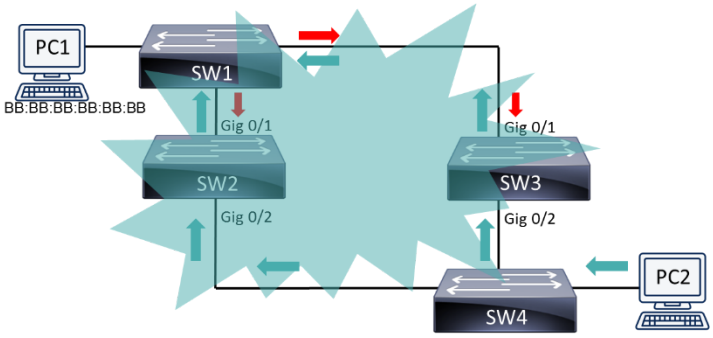
Switch 2
MAC Address Table

Port	MAC Address
Gig 0/1	CC:CC:CC:CC:CC:CC
Gig 0/2	CC:CC:CC:CC:CC:CC

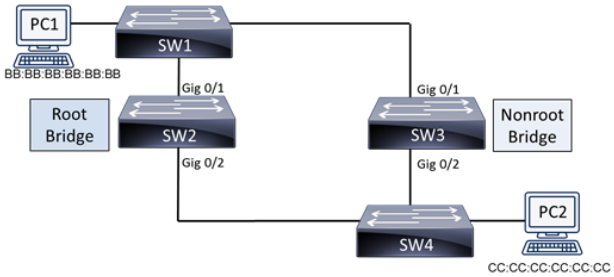
Switch 3
MAC Address Table

  - Broadcast Storms
    - If broadcast frame received by both switches, they can forward frames to each other

- Multiple copies of frame are forwarded, replicated, and forwarded again until the network is consumed with forwarding many copies of the same initial frame

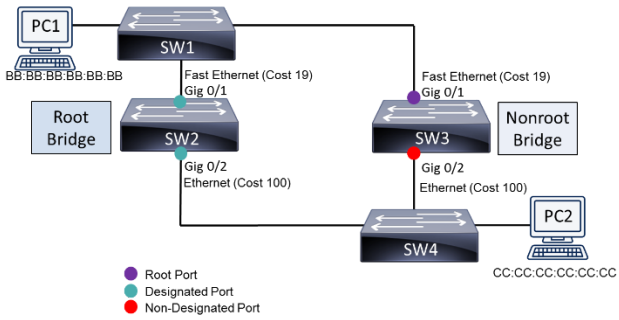


- Root and Nonroot Bridges
  - *Root Bridge*
    - Switch elected to act as a reference point for a spanning tree
    - Switch with the lowest bridge ID (BID) is elected as the root bridge
    - BID is made up of a priority value and a MAC address (with the lowest value considered root)
  - *Nonroot Bridge*
    - All other switches in an STP topology
  - MAC Address table corruption can occur



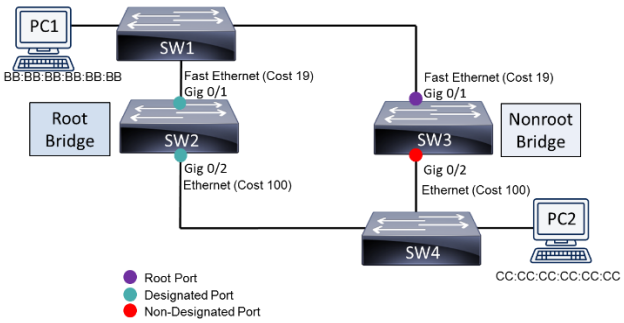
Switch	MAC Address	Priority
SW2	22:22:22:22:22:22	31423
SW3	33:33:33:33:33:33	31423

- Root, Designated, and Non-Designated Ports
  - *Root Port*
    - Every non-root bridge has a single root port
    - Port closest to the root bridge in terms of cost
    - If costs are equal, lowest port number is chosen
  - *Designated Port*
    - Every network segment has a designated port
    - Port closest to the root bridge in terms of cost
    - All ports on root bridge are designated ports
  - *Non-Designated Port*
    - Ports that block traffic to create loop-free topology
- Root and Nonroot Bridges
  - Single root port on non-root bridge
  - All other ports on non-root bridge are non-designated
  - All ports on root bridge are designated

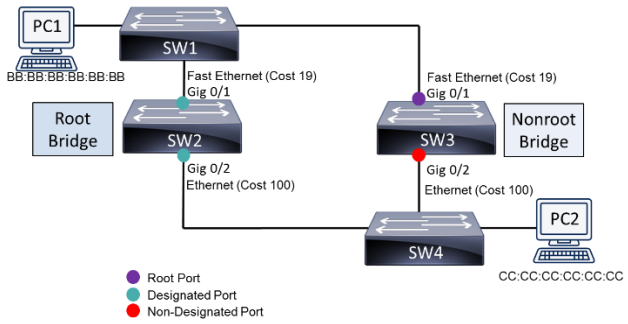


- Port States
  - Non-designated ports do not forward traffic during normal operation; however, they do receive bridge protocol data units (BPDUs)

- If a link in the topology goes down, the non-designated port detects the failure and determines whether it needs to transition to a forwarding state
- To get to the forwarding state, though, it has to transition through four states
    - Blocking
        - BPDUs are received but they are not forwarded
        - Used at beginning and on redundant links
    - Listening
        - Populates MAC address table
        - Does not forward frames
    - Learning
        - Processes BPDUs
        - Switch determines its role in the spanning tree
    - Forwarding
        - Forwards frames for operations
- Root and Non-designated port are blocking
- Designated ports are forwarding



- Link Costs
  - Associated with the speed of a link
  - 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

  - Long STP is being adopted due to higher link speeds over 10 Gbps
  - Values range from 2,000,000 for 10-Mbps Ethernet to as little as 2 for 10 Tbps

- **Virtual Local Area Network (VLAN)**
  - VLANs
    - Switch ports are in a single broadcast domain
    - Allow you to break out certain ports to be in different broadcast domains
    - Before VLANs, you had to use routers to separate departments, functions, or subnets
    - Allow different *logical* networks to share the same *physical* hardware
    - Provides added security and efficiency

- Before VLANs
  - Different switches were required for each LAN for separation
- Using VLANs
  - Same switches but switch ports can be in different VLANs
- *VLAN Trunking (802.1q)*
  - Multiple VLANs transmitted over the same physical cable
  - VLANs are each tagged with 4-byte identifier
    - Tag Protocol Identifier (TPI)
    - Tag Control Identifier (TCI)
  - One VLAN is left untagged
    - Called the Native VLAN

- **Specialized Network Devices**
  - *Virtual Private Network (VPN)*
    - Creates a secure VPN or virtual tunnel over an untrusted network like the Internet
  - *VPN Concentrator*
    - Dedicated network device that provides secure connections between remote users and a company network
  - *VPN Headend*
    - A specific type of VPN concentrator used to terminate IPSec VPN tunnels within a router or other device
  - *Firewalls*
    - Network security appliance at your boundary
    - Firewalls can be software or hardware

- *Stateful Firewalls*
  - Allows traffic that originates from inside the network and go out to the Internet
  - Blocks traffic originated from the Internet from getting into the network
- *Next-Generation Firewall (NGFW)*
  - Conducts deep packet inspection at Layer 7
  - Detects and prevents attacks
  - Much more powerful than basic stateless or stateful firewalls
  - Continually connects to cloud resources for latest information on threats
- Intrusion Detection or Prevention System (IDS/IPS)
  - *Intrusion Detection System (IDS)*
    - Recognizes attacks through signatures and anomalies
  - *Intrusion Prevention System (IPS)*
    - Recognizes and responds
- *Proxy Server*
  - A specialized device that makes requests to an external network on behalf of a client
- *Content Engine/Caching Engine*
  - Dedicated appliance that performs the caching functions of a proxy server
- *Content Switch/Load Balancer*
  - Distributes incoming requests across various servers in a server farm

- **Other devices you may find on your network**
    - *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
    - *Industrial Control System (ICS)*
        - Describes the different types of control systems and associated instrumentation
    - *Supervisory Control and Data Acquisition (SCADA)*
        - Acquires and transmits data from different systems to a central panel for monitoring and control
    - *Virtual Network Devices*
        - Major shift in the way data centers are designed, fielded, and operated

IP Addressing

Objectives:

- 1.4 - Given a scenario, configure a subnet and use appropriate IP addressing schemes
- 1.6 - Explain the use and purpose of network services

- **Internet Protocol (IP) Address**
    - An assigned numerical label that is used to identify Internet communicating devices on a computer network
        - Layer 2
            - Between two devices that are internal to own network or LAN
        - Layer 3
            - Between two different networks or even two different subnets

- **IPv4 Addressing**
    - Internet Protocol Version 4 (IPv4) Addressing
        - Written in dotted-decimal notation
            - 10.1.2.3
            - 172.21.243.67
        - Each IPv4 address is divided into 4 separate numbers and divided by dots
        - Each of these divisions are called octets due to having 8 bits assigned
        - 32-bits in length

	1st Octet	2nd Octet	3rd Octet	4th Octet
Dotted-Decimal	192	168	1	4
Binary Digits	11000000	10101000	00000001	00000100

        - IPv4 address is divided into network and host portions
        - Subnet mask defines the network portion
            - Network portion if a binary 1

- Host portion if binary 0

IP Address (In Decimal)	192	168	1	4
IP address	11000000	10101000	00000001	00000100
Subnet mask	255	255	255	0
Subnet mask	11111111	11111111	11111111	00000000
	Network bits	*Network bits*	*Network bits*	*Host bits*

- Classes of IP Addresses
  - Default subnet mask assigned by first octet
    - Classful Masks if using default subnet mask
  - Defines the Class of IP Address

Address Class	Value in First Octet	Classful Mask (Dotted Decimal)	Classful Mask (Prefix Notation)
Class A	1 – 126	255.0.0.0	/8
Class B	128 – 191	255.255.0.0	/16
Class C	192 – 223	255.255.255.0	/24
Class D	224 – 239	n/a	n/a

Notice that 127 is skipped between Class A and Class B since it is a reserved block for the loopback address (127.0.0.1)

- Routable IPs
  - Publicly routable IP addresses are globally managed by ICANN
    - Internet Corporation for Assigned Names and Numbers
      - ARIN, LACNIC, AFNIC, APNIC, and RIPE NCC
  - Public IP's must be purchased before use through your Internet Service Provider (ISP)
- Private IPs
  - Private IP's can be used by anyone
  - Not routable outside your local area network
  - Network Address Translation (NAT) allows for routing of private IPs through a public IP

Address Class	Address Range	Default Subnet Mask
Class A	10.0.0.0 – 10.255.255.255	255.0.0.0
Class B	172.16.0.0 – 172.31.255.255	255.255.0.0
Class C	192.168.0.0 – 192.168.255.255	255.255.255.0

- Specialized IPs
  - *Loopback Addresses (127.x.x.x range)*
    - Refers to the device itself and used for testing
    - Most commonly used as 127.0.0.1
  - *Automatic Private IP Addresses (APIPA)*
    - Dynamically assigned by OS when DHCP server is unavailable and address not assigned manually
    - Range of 169.254.x.x

Description	Address Class	Address Range	Default Subnet Mask
Loopback	Class A	127.0.0.1 – 127.255.255.255	255.0.0.0
APIPA	Class B	169.254.0.0 – 169.254.255.255	255.255.0.0

Special address ranges never assigned by an administrator or DHCP server

- Identifying Network and Hosts in IPv4

• Class A network address example:
  • IP Address: 114.56.20.33
    Subnet Mask: 255.0.0.0

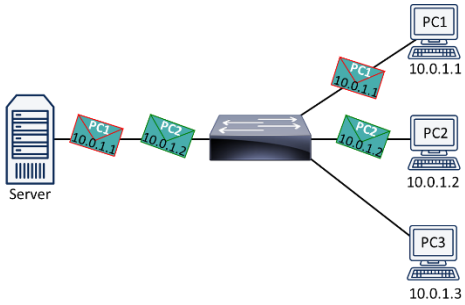
• Class B network address example:
  • IP Address: 147.12.38.81
  • Subnet Mask: 255.255.0.0

• Class C network address example:
  • IP Address: 214.51.42.7
  • Subnet: 255.255.255.0

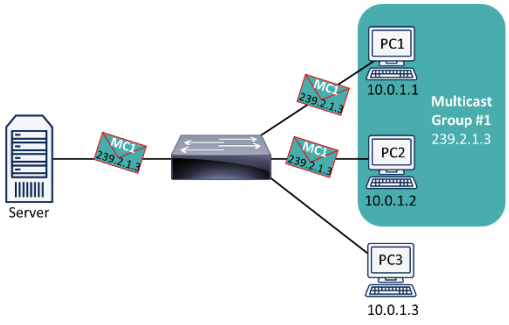
Network Host

- *Virtual IP Addresses (VIP or VIPA)*
  - An IP address that does not correlate to an actual physical network interface
  - respond to numerous IP addresses and have them resolve to your physical network interface to establish connectivity
- *Subinterfaces*
  - A virtual interface that is created by dividing up one physical interface into multiple logical interfaces

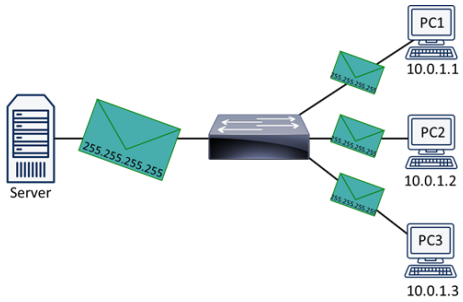
- **IPv4 Data Flows**
  - *Unicast*
    - Data travels from a single source device to a single destination device



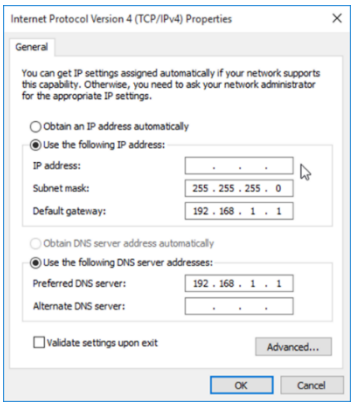
  - *Multicast*
    - Data travels from a single source device to multiple (but specific) destination devices



- *Broadcast*
  - Data travels from a single source device to all devices on a destination network



- **Assigning IP Addresses**
  - Static

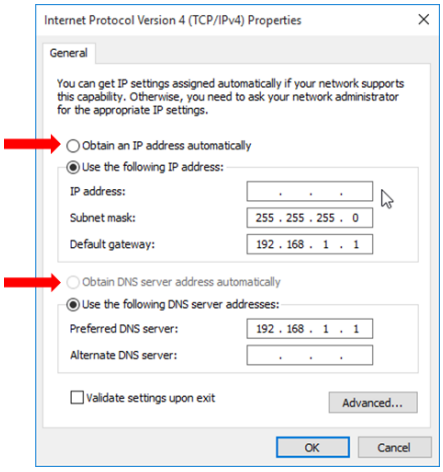


    - Simple
    - Time-consuming
    - Prone to human errors
    - Impractical for large networks
  - Dynamic
    - Quicker
    - Easier
    - Less confusing

- Simplistic for large networks

- Components of an IP Address
  - Information assigned from static or dynamic
    - IP Address
    - Subnet Mask
    - Default Gateway
    - Server addresses
      - *Domain Name System (DNS)*
        - Converts domain names to IP address
      - *Windows Internet Name Service (WINS)*
        - Converts NetBIOS computer name into an IP address

- Dynamic Host Control Protocol (DHCP) Configuration



  - Based on the older Bootstrap Protocol (BOOTP for short)
    - Required static database of IP and MAC to assign
  - *Dynamic Host Control Protocol (DHCP)*
    - Service assigns an IP from an assignable pool (scope)

- *IP Address Management*
  - Software used to manage the IP's being assigned

- *Dynamic Host Control Protocol (DHCP)*
  - Provides clients with
    - IP
    - Subnet mask
    - Default gateway
    - DNS server
    - WINS server
    - Other variables needed for VoIP
  - Each IP is leased for a given amount of time and given back to the pool when lease expires (TTL)

- *Automatic Private IP Address (APIPA)*

  - Used when device does not have a static IP address and cannot reach a DHCP server
  - Allows a network device to self-assign an IP address from the 169.254.0.0/16 network
  - Designed to allow quick configuration of a LAN without need for DHCP

        - Non-routable but allows for network connectivity inside the local subnet
    - *Zero Configuration (Zeroconf)*
        - Newer technology based on APIPA providing
            - Assigning link-local IP addresses
                - Non-routable IP usable only on local subnet
            - Resolving computer names to IP addresses without the need for DNS server on local network
                - mDNS - Multicast Domain Name Server
            - Locating network services
                - Provides service discovery protocols
                    - Service Location Protocol (SLP)
                    - Microsoft's Simple Service Discovery Protocol (SSDP)
                    - Apple's DNS-based Service Discovery (DNS-SD)

- **Computer Mathematics**
    - Humans count using Base-10 numbers
        - Decimals
        - 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, …
    - Computers and networks do not understand decimal numbers natively
    - Process numbers using Base-2 numbers
        - Binary
        - 0, 1, 10, 11, …

- **Converting Binary to Decimal**
  - Use table to convert from binary to decimal
  - Each number is a factor of 2
  - Starting from the right and go to the left

128 (2^7)	64 (2^6)	32 (2^5)	16 (2^4)	8 (2^3)	4 (2^2)	2 (2^1)	1 (2^0)

  - Populate the table with the binary digits
  - Add up any columns that contain a 1

128 (2^7)	64 (2^6)	32 (2^5)	16 (2^4)	8 (2^3)	4 (2^2)	2 (2^1)	1 (2^0)
1	0	0	1	0	1	1	0

10010110

➡128 + 16 + 4 + 2

➡150

- **Converting Decimal to Binary**
  - Use subtraction to convert decimal to binary

128 (2^7)	64 (2^6)	32 (2^5)	16 (2^4)	8 (2^3)	4 (2^2)	2 (2^1)	1 (2^0)
1	0	1	0	0	1	1	1

167	39	7	3	1
-128	-32	-4	-2	-1
39	7	3	1	0

(Check Your Answer by Adding It Back Up)

128 + 32 + 4 + 2 + 1 = 167

- **Computer Mathematics Practice**
  - You must be able to convert
  - Binary ➡ Decimal
    Decimal ➡ Binary

- **Converting Binary to Decimal**

Convert 01101011
to decimal

128 (2^7)	64 (2^6)	32 (2^5)	16 (2^4)	8 (2^3)	4 (2^2)	2 (2^1)	1 (2^0)

128 (2^7)	64 (2^6)	32 (2^5)	16 (2^4)	8 (2^3)	4 (2^2)	2 (2^1)	1 (2^0)
0	1	1	0	1	0	1	1

➡64 + 32 + 8 + 2 + 1
➡107

Convert 10010100
to decimal

128 (2^7)	64 (2^6)	32 (2^5)	16 (2^4)	8 (2^3)	4 (2^2)	2 (2^1)	1 (2^0)

128 (2^7)	64 (2^6)	32 (2^5)	16 (2^4)	8 (2^3)	4 (2^2)	2 (2^1)	1 (2^0)
1	0	0	1	0	1	0	0

➡128 + 16 + 4
➡148

- **Converting Decimal to Binary**

Convert 49
to binary

128 (2^7)	64 (2^6)	32 (2^5)	16 (2^4)	8 (2^3)	4 (2^2)	2 (2^1)	1 (2^0)

128 (2^7)	64 (2^6)	32 (2^5)	16 (2^4)	8 (2^3)	4 (2^2)	2 (2^1)	1 (2^0)
0	0	1	1	0	0	0	1

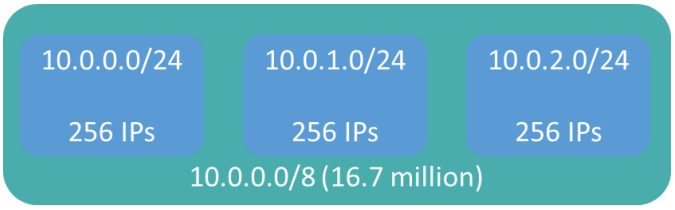
```
 49     17     1
-32    -16    -1
 17      1     0
```

49 ➡ 00110001

Check Your Answer:

49 = 32 + 16 + 1

- **Subnetting**
  - Default classful subnet masks are rarely the optimal choice for a subnet size
  - Subnets can be modified using subnet masks to create networks that are better scoped
  - Creating a subnet involves borrowing bits from the original host portion and adding them to the network portion



- Purpose of Subnets
  - More efficient use of IP addresses than classful default
  - Enables separation of networks for security
  - Enables bandwidth control

Address Class	Default Subnet Mask	Assignable IP Calculation	Assignable IP Addresses
Class A	255.0.0.0	$2^{24} - 2 =$	16,777,214
Class B	255.255.0.0	$2^{16} - 2 =$	65,534
Class C	255.255.255.0	$2^{8} - 2 =$	254

- Subnet Masks

Dotted-Decimal Notation	CIDR	Binary Notation
255.0.0.0	**/8**	11111111.00000000.00000000.00000000
255.255.0.0	**/16**	11111111.11111111.00000000.00000000
255.255.255.0	**/24**	11111111.11111111.11111111.00000000
255.255.255.128	/25	11111111.11111111.11111111.10000000
255.255.255.192	/26	11111111.11111111.11111111.11000000
255.255.255.224	/27	11111111.11111111.11111111.11100000
255.255.255.240	/28	11111111.11111111.11111111.11110000
255.255.255.248	/29	11111111.11111111.11111111.11111000
255.255.255.252	/30	11111111.11111111.11111111.11111100

Classful subnets for Class A, B, and C in red

- Subnetting Formulas

• Number of Created Subnets = 2^s,
where *s* is the number of borrowed bits

• Number of Assignable IP Addresses = $2^h - 2$,
where *h* is the number of host bits

- Classful vs Subnetted Networks

  - Classful subnet (192.168.1.0/24)
    - 1 network (2^0), where *s* is the number of borrowed bits
    - 256 IPs (2^8), where *h* is the number of host bits

192	168	1	0
255	255	255	0
11111111	11111111	11111111	00000000
Network Bits			Host Bits

  - Classless subnet (192.168.1.64/26)
    - 4 networks (2^2), where *s* is the number of borrowed bits
    - 64 IPs (2^6), where *h* is the number of host bits

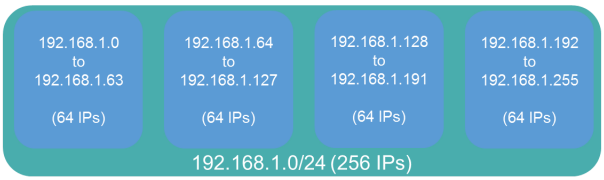
192	168	1	64	0
255	255	255	192	0
11111111	11111111	11111111	11	000000
Network Bits			Sub	Host Bits

- Calculating Number of Subnets

192.168.1.0/26

- Default mask is /24, so we *borrowed* 2 bits from the host space

$2^s = 2^2 = 4$,
which means there are four created subnets

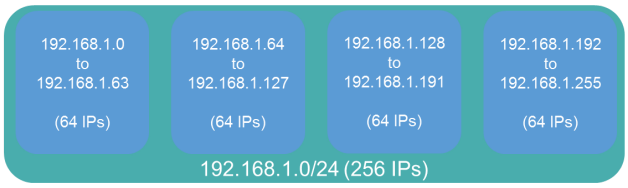


- Calculating Number of IPs
  - Total bits are 32 and the mask is /26

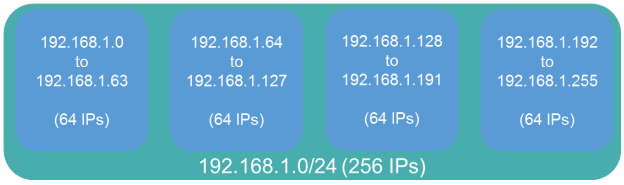
$$32 - 26 = 6 \text{ host bits } (h)$$

$$2^h - 2 = 2^6 - 2 = 64 - 2 = 62$$

62 assignable IPs in each subnet



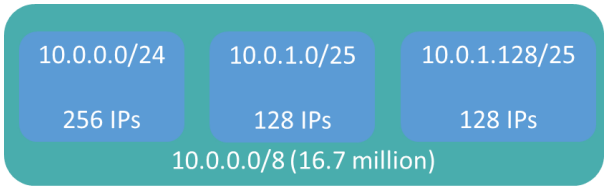
- Listing Subnets
  - *Created 4 subnets of 62 usable IPs each*
  - *Where does each network begin and end?*
  - *Network ID (First IP)*
    0, 64, 128, 192
  - *Broadcast (Last IP)*
    63, 127, 191, 255



- *Classless Interdomain Routing (CIDR)*
  - Instead of advertising multiple individual routes, the routes can be summarized and advertised as a single route
  - Used to summarize contiguous networks
    - Called "Route Aggregation"

Network Address	1st Octet	2nd Octet	3rd Octet	4th Octet
192.168.32.0	11000000	10101000	00000001	11000000
192.168.33.0	11000000	10101000	00000001	11000000
192.168.34.0	11000000	10101000	00000001	11000000
192.168.35.0	11000000	10101000	00000001	11000000

- *Variable-Length Subnet Masking (VLSM)*
  - Allows subnets of various sizes to be used
  - Requires a routing protocol that supports it
    - RIPv2, OSPF, IS-IS, EIGRP, and BGP
  - Basically, it is subnetting subnets
  - Without VLSM, all subnets would have to be the same size



- Subnetting Exam Tip

CIDR	# Subnets	# IPs
/30	64	4
/29	32	8
/28	16	16
/27	8	32
/26	4	64
/25	2	128
/24	1	256

- **Subnetting Practice**

Subnetting Practice #1

CIDR	# Subnets	# IPs
/30	64	4
/29	32	8
/28	16	16
/27	8	32
/26	4	64
/25	2	128

You are the network administrator for DionTraining.com. We decided to locate a small branch office in another city. To support the new location, you will need to subnet the private IP address range given to you into several smaller networks to service each department.

The new office location has been assigned the range of 10.10.10.0/24.

When you set up the new network, you need to configure separate subnets for each department in the new office. You should allocate the addresses using CIDR notation and provide each department the minimum number of IP addresses that will meet their needs.

Subnetting Practice #1

CIDR	# Subnets	# IPs
/30	64	4
/29	32	8
/28	16	16
/27	8	32
/26	4	64
/25	2	128

The departments at the new location will require these number of computers in their subnets:

54 – IT
32 – Instructors
5 – Sales
3 – Administrative
X – Unused

- When complete, summarize the remaining available IPs in their own subnet using CIDR notation.

Subnetting Practice #1

CIDR	# Subnets	# IPs
/30	64	4
/29	32	8
/28	16	16
/27	8	32
/26	4	64
/25	2	128

54 – IT
32 – Instructors
5 – Sales
3 – Administrative
X – Unused

- If you have memorized the table, this problem becomes quite simple.

- First, we round up our department numbers to the next highest multiple of 2. Remember, the numbers provided are for the computers, we still need to add 2 IPs to account for the network and broadcast IPs:

  - IT: 54 + 2 = 56 => 64 IPs will be assigned
  - Instructors: 32 + 2 = 34 => 64 IPs will be assigned
  - Sales: 5 + 2 = 7 => 8 IPs will be assigned
  - Administrative: 3 + 2 = 5 => 8 IPs will be assigned
  - Unused: 256 - 64 - 64 - 8 - 8 = 112 => 64 Unused IPs

Subnetting Practice #2

CIDR	# Subnets	# IPs
/30	64	4
/29	32	8
/28	16	16
/27	8	32
/26	4	64
/25	2	128

How many assignable IP addresses exist in this network?
172.16.1.0/27

- 30
- 32
- 14
- 64

Subnetting Practice #2

CIDR	# Subnets	# IPs
/30	64	4
/29	32	8
/28	16	16
/27	8	32
/26	4	64
/25	2	128

How many assignable IP addresses exist in this network?
172.16.1.0/27

- 30
- 32
- 14
- 64

Subnetting Practice #3

CIDR	# Subnets	# IPs
/30	64	4
/29	32	8
/28	16	16
/27	8	32
/26	4	64
/25	2	128

How many assignable IP addresses exist in this network?
192.168.1.0/28

- 30
- 16
- 14
- 64

Subnetting Practice #3

CIDR	# Subnets	# IPs
/30	64	4
/29	32	8
/28	16	16
/27	8	32
/26	4	64
/25	2	128

How many assignable IP addresses exist in this network?
192.168.1.0/28

- 30
- 16
- 14
- 64

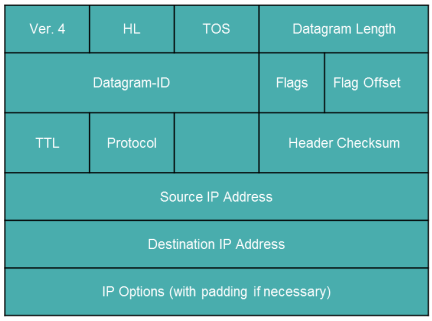
16 usable IPs – Network IP – Broadcast IP
= 16 – 1 – 1
= 16 – 2
= 14

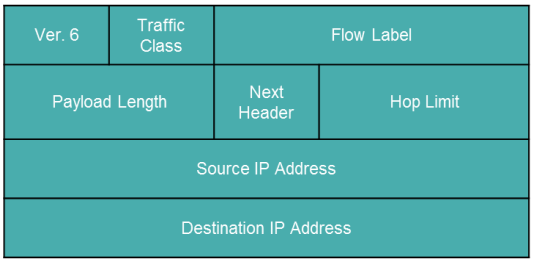
- **Internet Protocol Version 6 (IPv6) Addressing**
  - IPv6
    - IPv4 essentially ran out of addresses due to proliferation of devices
    - IPv6 addressing provides enough IP addresses for generations to come
    - Enough IPv6 addresses for every person on the planet (5×10^{28})

$$\text{IPv4} = 2^{32} = 4.2 \text{ billion addresses}$$
$$\text{IPv6} = 2^{128} = 340 \text{ undecillion addresses}$$

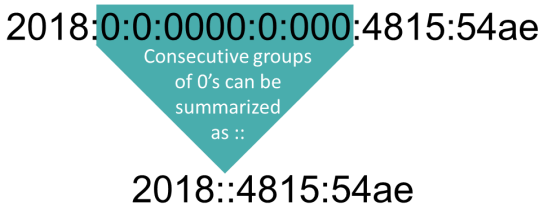
    - IPv5 was an experimental protocol that was abandoned, although some of its concepts have been incorporated into other protocols
  - IPv6 Benefits
    - No broadcasts
    - No fragmentation
      - Performs MTU (maximum transmission units) discovery for each session
    - Can coexist with IPv4 during transition
      - Dual stack (run IPv4 and IPv6 simultaneously)
      - IPv6 over IPv4 (tunneling over IPv4)
        - Allows an existing IPv4 router to carry IPv6 traffic
        - Encapsulates IPv6 packets within IPv4 headers to carry this IPv6 data over IPv4 routers and other infrastructure
    - Simplified header
      - 5 fields instead of 12 fields

- Headers (IPv4 and IPv6)





- IPv6 Address Structure
  - Each hexadecimal digit is 4-bits
  - 128-bits in an IPv6 address
  - No more than 32 hexadecimal digits



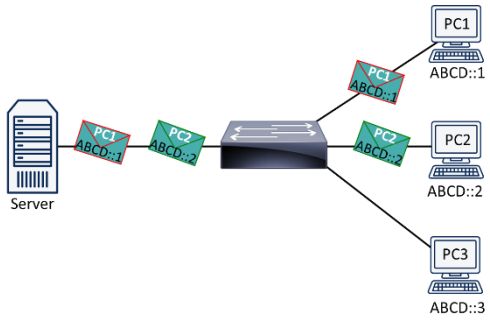
- IPv6 Address Types
  - *Unicast Addresses*
    - Used to identify a single interface
      - Globally routable unicast addresses
        - Begins with 2000 to 3999
      - Link-local address
        - Begins with FE80
        - It uses stateless address autoconfiguration, or SLAAC

- *Multicast Addresses*
  - Used to identify a group of interfaces so that a packet can be sent to a multicast address and then be delivered to all of the interfaces in the group
    - Begins with FF
- *Anycast Addresses*
  - Used to identify a set of interfaces so that a packet can be sent to any member of a set

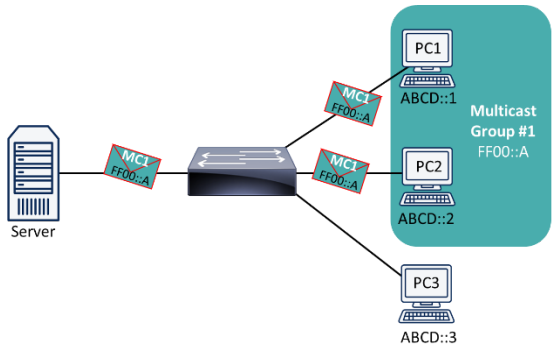
- Do you need DHCP for IPv6?
  - IPv6 uses auto configuration to discover the current network and selects its own host ID based on its MAC using the EUI64 process
  - If you want to still use DHCP, there is a DHCPv6 protocol
  - IPv6 uses Neighbor Discovery Protocol (NDP) to learn the Layer 2 addresses on the network
- *Stateless Address Autoconfiguration (SLAAC)*
  - Discovers the current network that an interface is located on and then select its own host ID based on its MAC address using the EUI64 process
    - Extended Unique Identifier (EUI)
- *Neighbor Discovery Protocol (NDP)*
  - Used to learn Layer 2 addresses on network
  - *Router Solicitation*
    - Hosts send message to locate routers on link
  - *Router Advertisement*
    - Router advertise their presence periodically and in response to solicitation

        - *Neighbor Solicitation*
            - Used by nodes to determine link layer addresses
        - *Neighbor Advertisement*
            - Used by nodes to respond to solicitation messages
        - *Redirect*
            - Routers informing host of better first-hop routers

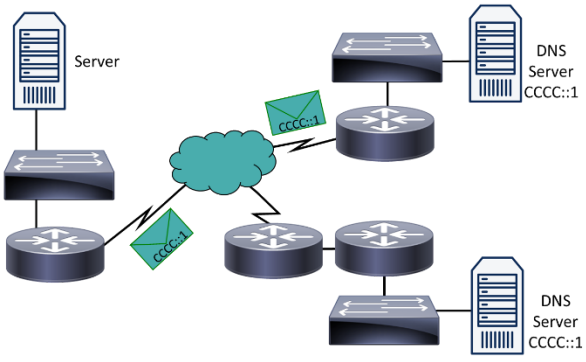
- **IPv6 Data Flows**
    - IPv6 Data Flows
        - Three data flow methods, like IPv4
            - Unicast
            - Multicast
            - Anycast (new to IPv6)
    - *Unicast*
        - Data travels from a single source device to a single destination device



- *Multicast*
  - Data travels from a single source device to multiple (but specific) destination devices



- *Anycast*
  - Designed to let one host initiate the efficient updating of router tables for a group of hosts
  - IPv6 can determine which gateway host is closest and sends the packets to that host as though it were a unicast communication
  - That host can anycast to another host in the group until all routing tables are updated
  - Data travels from a single source device to the device nearest to multiple (but specific) destination devices



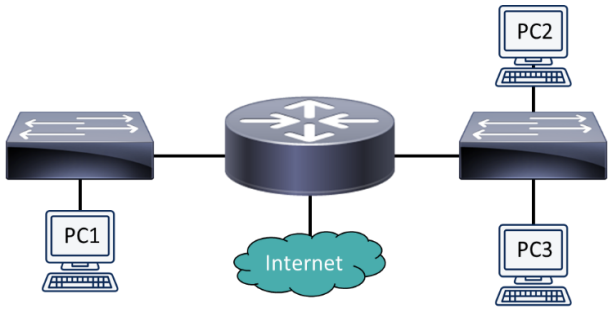
Routing

Objectives:

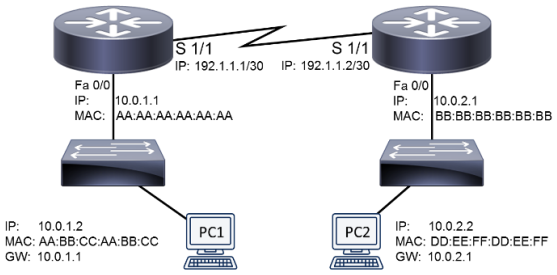
- 1.4 - Given a scenario, configure a subnet and use appropriate IP addressing schemes
- 2.2 - Compare and contrast routing technologies and bandwidth management concepts
- 5.5 - Given a scenario, troubleshoot general networking issues

- **Routers**
  - Used to forward traffic between subnets, between an internal and external network, or between two external networks
  - Each subnet or external network is going to be its own broadcast domain
  - Multilayer switches also perform routing functions
    - Switch
      - Layer 2 Switch
    - Multilayer Switch
      - Router

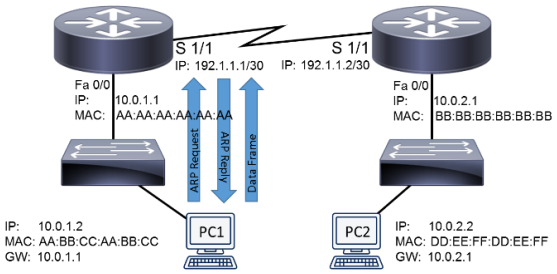
- **Routing Fundamentals**
  - Traffic is routed to flow between subnets
  - Each subnet is its own broadcast domain
  - Routers are the layer 3 devices that separate broadcast domains, but multilayer switches can also separate broadcast domains



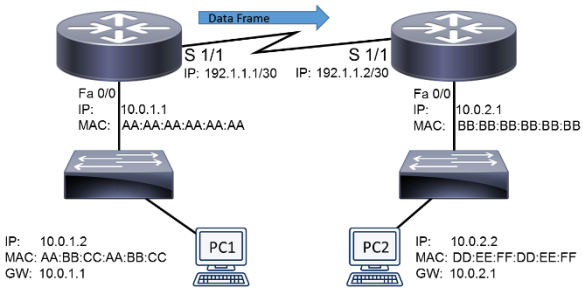
- Basic Routing Process



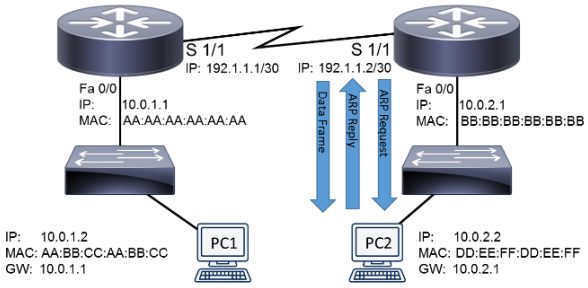
How does a packet from a source IP address of 10.0.1.2 (PC1) route to a destination IP address of 10.0.2.2 (PC2)?



PC1 needs to determine MAC address of router, sends an ARP request, receives ARP reply, then forwards data frame to router's MAC address

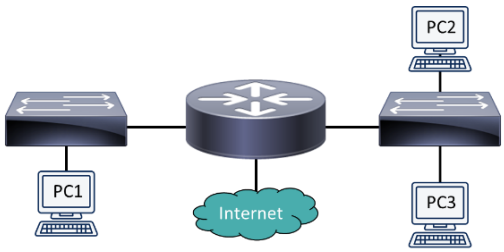


Router 1 receives data frame from PC1 and looks at the IP header. Determines best path by looking at routing table, decreases TTL by 1, and forwards data frame via Serial 1/1 (best route).



Router 2 receives the data frame, it decreases TTL by 1. If TTL isn't 0, looks at IP header to determine destination network. If on Router 2's network, Router 2 sends ARP request to find destination (Server 1), receives reply, forwards data frame to Server 1's MAC address. If not, Router 2 forwards it to next Router.

- **Routing Tables**
  - Routing Decisions
    - Layer 3 to Layer 2 Mapping
      - Routers use ARP caches to map an IP address to a given MAC address
    - Make packet-forwarding decisions based on its internal routing tables



  - *Routing Tables*
    - Table kept by the router to help determine which route entry is the best fit for the network
    - A route entry with the longest prefix is the most specific network
    - 10.1.1.0/24 more specific than 10.0.0.0/8

Destination Network	Next Router	Port	Route Cost
125.0.0.0	137.3.14.2	1	12
161.5.0.0	137.3.6.6	1	4
134.7.0.0	164.17.3.12	2	10

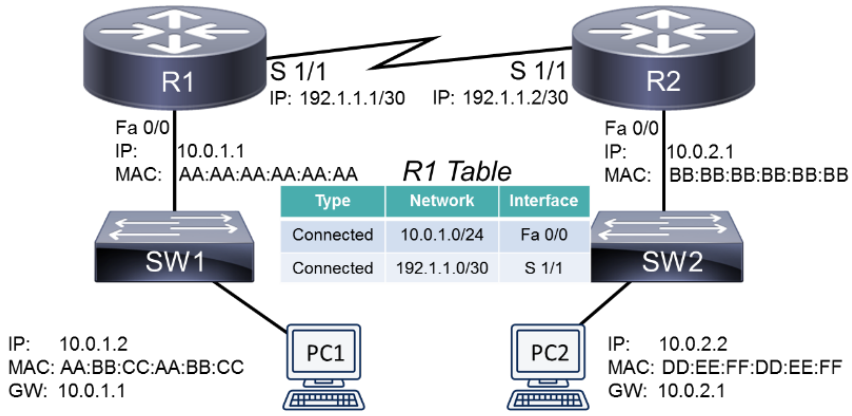
  - Sources of Routing Information
    - Directly Connected Routes
      - Learned by physical connection between routers
    - Static Routes
      - Manually configured by an administrator

- Default static route (0.0.0.0/0) is a special case
    - "If I don't know where, then send out the default static route"

■ Dynamic Routing Protocols

- Learned by exchanging information between routers

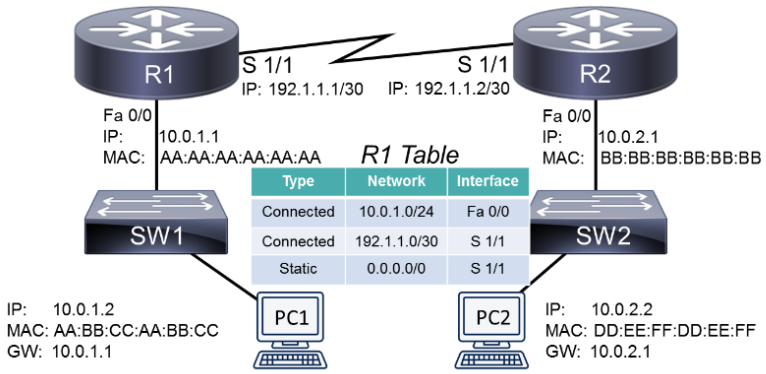
○ Directly Connected Routes



A router knows how to reach a destination because it has an interface directly participating in a network.

R1 knows how to connect to 10.0.1.0/24 network, since FastEthernet 0/0 is directly connected.

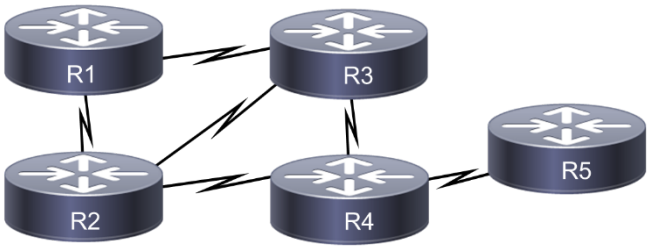
- Static Routes



A router knows how to reach a destination because the route has been statically (manually) configured by an administrator.

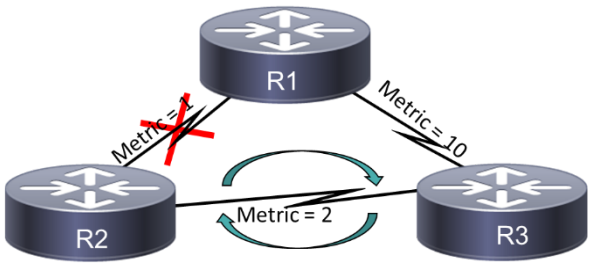
A *default static route* is a special route that states, "If traffic is not destined for a network currently in the routing table, send that traffic out this interface (like Serial 1/1 of Router 1).

- Dynamic Routing Protocols
  - More than one route can exist for a network
  - Different protocols consider different criteria when deciding which route to give preference
  - Based on number of hops (hop count in RIP), link bandwidths (OSPF), or other criteria

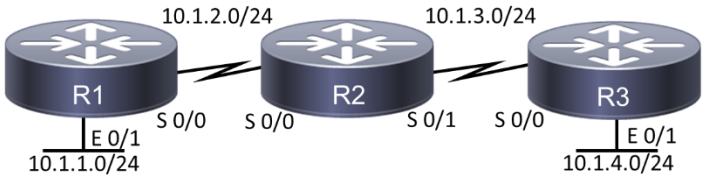


- Preventing Routing Loops
  - *Split Horizon*
    - Prevents a route learned on one interface from being advertised back out of that same interface

- *Poison Reverse*
  - Causes a route received on one interface to be advertised back out of that same interface with a metric considered to be infinite



- Routing Loops



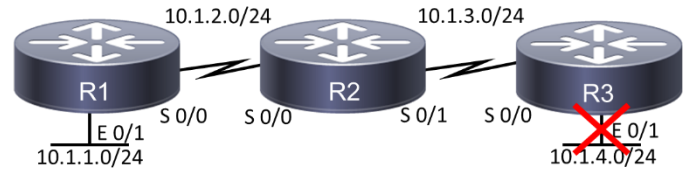
R2 Routing Table

Network	Interface	Metric
10.1.1.0/24	S 0/0	1
10.1.2.0/24	S 0/0	0
10.1.3.0/24	S 0/1	0
10.1.4.0/24	S 0/1	1

R3 Routing Table

Network	Interface	Metric
10.1.1.0/24	S 0/0	2
10.1.2.0/24	S 0/0	1
10.1.3.0/24	S 0/1	0
10.1.4.0/24	E 0/1	0

Network with no issues



R2 Routing Table

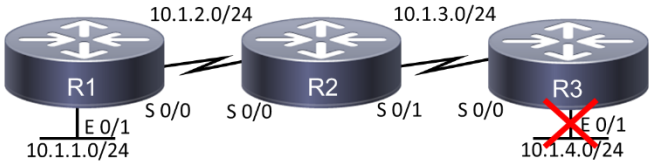
Network	Interface	Metric
10.1.1.0/24	S 0/0	1
10.1.2.0/24	S 0/0	0
10.1.3.0/24	S 0/1	0
10.1.4.0/24	S 0/1	1

R3 Routing Table

Network	Interface	Metric
10.1.1.0/24	S 0/0	2
10.1.2.0/24	S 0/0	1
10.1.3.0/24	S 0/1	0
10.1.4.0/24	E 0/1	0
10.1.4.0/24	S 0/0	2

10.1.4.0/24 Hop Count 1

Link goes down, so R3 gets information on how to connect to 10.1.4.0/24 from R2. Begins chain reaction of a routing loop.



R2 Routing Table

Network	Interface	Metric
10.1.1.0/24	S 0/0	1
10.1.2.0/24	S 0/0	0
10.1.3.0/24	S 0/1	0
10.1.4.0/24	S 0/1	1
10.1.4.0/24	S 0/1	3

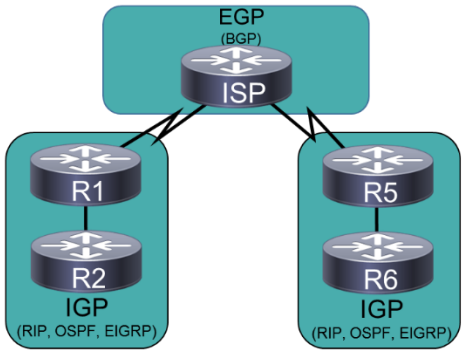
R3 Routing Table

Network	Interface	Metric
10.1.1.0/24	S 0/0	2
10.1.2.0/24	S 0/0	1
10.1.3.0/24	S 0/1	0
10.1.4.0/24	E 0/1	0
10.1.4.0/24	S 0/0	2

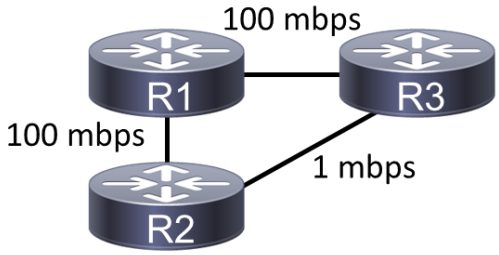
…and the cycle continues, causing a routing loop until the metric gets so big that no one will use that route.

10.1.4.0/24 Hop Count 2

- **Routing Protocols**
  - Internal and Exterior Routing Protocols
    - *Interior Gateway Protocols (IGP)*
      - Operate <u>within</u> an autonomous system
    - *Exterior Gateway Protocols (EGP)*
      - Operated <u>between</u> autonomous systems



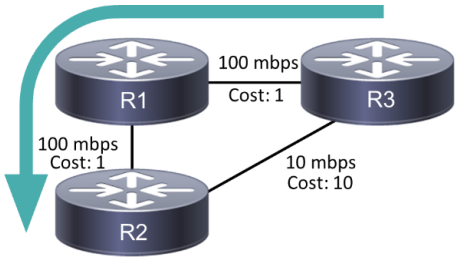
- *Router Advertisement Method*
  - Characteristic of a routing protocol
  - How does it receive, advertise, and store routing information?
    - Distance vector
    - Link state
  - Not every routing protocol fits neatly into one of these two categories (hybrids exist)
- *Distance Vector*



  - Sends full copy of routing table to its directly connected neighbors at regular intervals
  - Slow convergence time
    - Time it takes for all routers to update their routing tables in response to a topology change
  - Holding-down timers speeds up convergence
    - Prevents updates for a specific period of time

- Uses hop count as a metric

- *Link State*
  - Requires all routers to know about the paths that all other routers can reach in the network
  - Information is flooded throughout the link-state domain (OSPF or IS-IS) to ensure routers have synchronized information
  - Faster convergence time and uses cost or other factors as a metric
  - Each router constructs its own relative shortest-path tree with itself as the root for all known routes in the network
- *Routing Information Protocol (RIP)*
  - Interior Gateway Protocol
  - Distance-vector protocol using *hop count*
  - Maximum hops of 15, 16 is infinite
  - Oldest dynamic routing protocol, provides updates every 30 seconds
  - Easy to configure and runs over UDP
- *Open Shortest Path First (OSPF)*
  - Interior Gateway Protocol
  - Link-state protocol using *cost*
  - Cost is based on link speed between routers



- *Intermediate System to Intermediate System (IS-IS)*
  - Interior Gateway Protocol
  - Link-state protocol using *cost*
  - Cost is based on link speed between two routers
  - Functions like OSPF protocol, but not as popular or widely utilized
- *Enhanced Interior Gateway Routing Protocol (EIGRP)*
  - Interior Gateway Protocol
  - Advanced distance-vector protocol using bandwidth and delay making it a hybrid of distance-vector and link-state
  - Proprietary Cisco protocol that is popular in Cisco-only networks
- *Border Gateway Protocol (BGP)*
  - External Gateway Protocol
  - Path vector using the number of autonomous system hops instead of router hops
  - Widespread utilization, this protocol runs the backbone of the Internet
  - Does not converge quickly, though, when the topology changes
- Route Believability
  - If a network is using more than one routing protocol, how does it choose which routing protocol to make decisions from?
  - Some routing protocols are considered more believable than others, so routers use an index of believability called *administrative distance* (AD)
  - If a route has a lower the administrative distance (AD), the route is more believable

Routing Information Source	Administrative Distance
Directly connected network	0
Statically configured network	1
EIGRP	90
OSPF	110
RIP	120
External EIGRP	170
Unknown or Unbelievable	255 (unreachable)

- Metrics
  - If a routing protocol knows multiple paths to reach a network, how does it choose its path?
    - Metrics are the values assigned to a route
    - Lower metrics are preferred over higher metrics
  - Metrics calculated differently for each protocol (RIP, OSPF, IS-IS, EIGRP, and BGP)
    - Hop count
    - Bandwidth
    - Reliability
    - Delay
    - Other metrics

- Routing Protocol Summary

Routing Protocol	Abbreviation	Type	Interior/ Exterior
Routing Information Protocol	RIP	Distance vector	Interior
Open Shortest Path First	OSPF	Link state	Interior
Enhanced Interior Gateway Routing Protocol	EIGRP	Advanced distance vector	Interior
Intermediate System-to-Intermediate System	IS-IS	Link state	Interior
Border Gateway Protocol	BGP	Path vector	Exterior

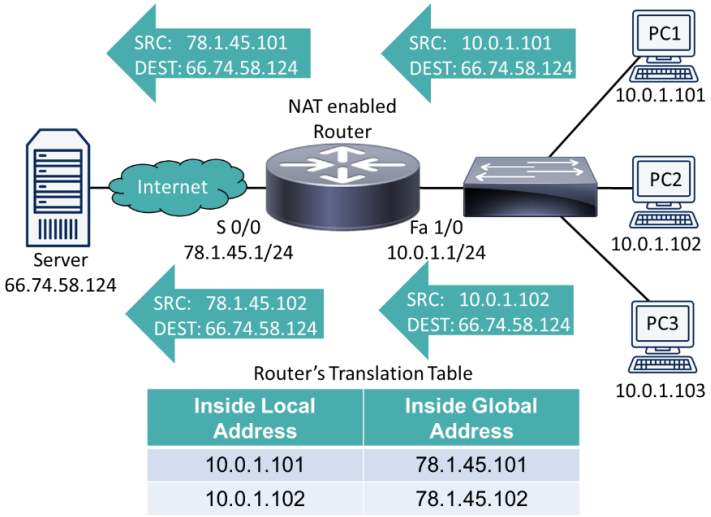
A network can simultaneously support more than one routing protocol through *route redistribution*. This allows a router to participate in OSPF on one interface and EIGRP on another interface. The router can than translate from one protocol for redistribution as the other protocol.

- **Address Translation (NAT & PAT)**
  - Address Translation
    - *Network Address Translation (NAT)*
      - Used to conserve the limited supply of IPv4 addresses
      - NAT translates private IP addresses to public IP addresses for routing over public networks
    - *Port Address Translation (PAT)*
      - Variation of address translation that utilizes port numbers instead of IP addresses for translation
  - Types of Address Translation
    - *Dynamic NAT (DNAT)*
      - IP addresses automatically assigned from a pool
      - One-to-one translations

- *Static NAT (SNAT)*
  - IP addresses manually assigned
  - One-to-one translations
- *Port Address Translation (PAT)*
  - Multiple private IP addresses share one public IP
  - Many-to-one translation
  - Common in small networks

- Names of NAT IP Addresses
  - Inside local
    - Private IP address referencing an inside device
  - Inside global
    - Public IP address referencing an inside device
  - Outside local
    - Private IP address referencing an outside device
  - Outside global
    - Public IP address referencing an outside device

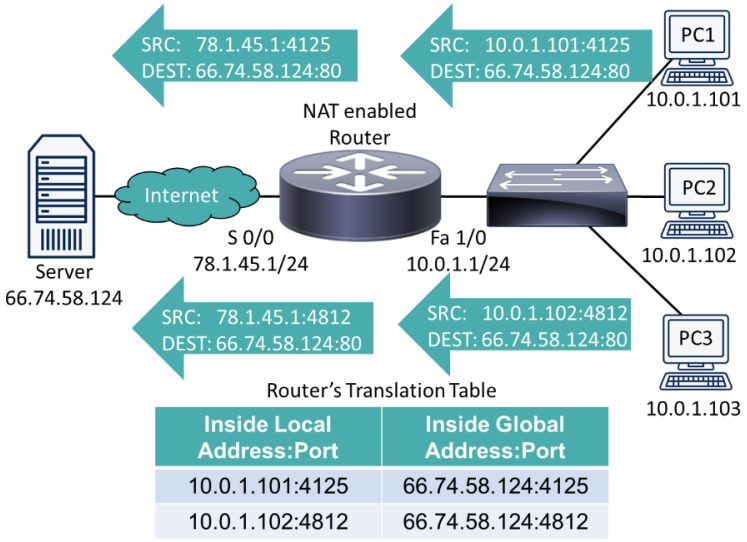
- How NAT Works



Router's Translation Table

Inside Local Address	Inside Global Address
10.0.1.101	78.1.45.101
10.0.1.102	78.1.45.102

- How PAT Works

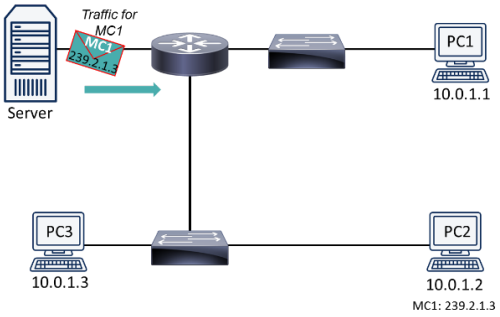


Router's Translation Table

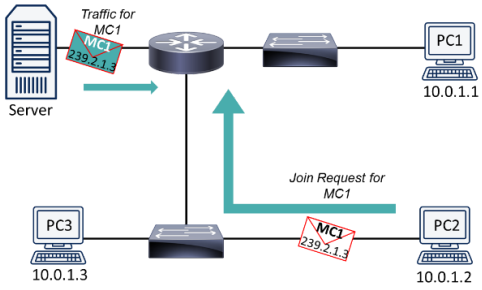
Inside Local Address:Port	Inside Global Address:Port
10.0.1.101:4125	66.74.58.124:4125
10.0.1.102:4812	66.74.58.124:4812

- **Multicast Routing**
  - What is multicast touring?
    - Multicast sender sends traffic to a Class D IP Address, known as a multicast group
    - Goal
      - Send the traffic only to the devices that want it
    - Two primary protocols
      - Internet Group Management Protocol (IGMP)
      - Protocol Independent Multicast (PIM)
  - *Internet Group Management Protocol (IGMP)*
    - Used by clients and routers to let routers known which interfaces have multicast receivers
    - Used by clients to join a multicast group

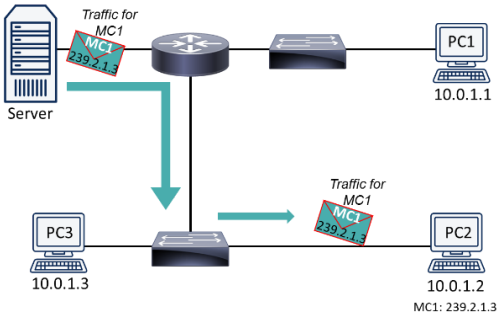
- Versions
  - IGMPv1
    - Client requests to join the group and is asked every 60 seconds if it wants to remain in the group
  - IGMPv2
    - Client can send a *leave* message to exit multicast group
  - IGMPv3
    - Client can request multicast from only specific server
    - Called source-specific multicast (SSM)
    - Allows multiple video streams to single multicast



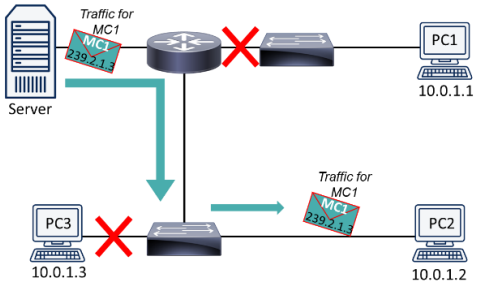
Router doesn't' forward the traffic because no clients are in the Multicast Group 1



PC2 joins the multicast traffic by sending the "join message" to its default gateway



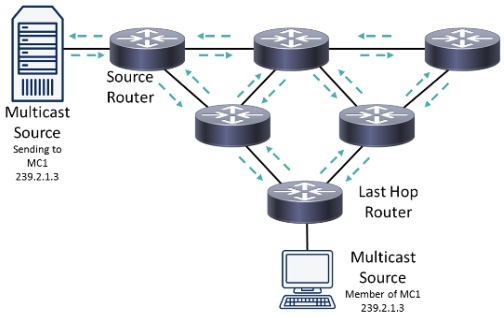
Router remembers that PC2 is now part of Multicast Group 1



Router forward traffic for 239.1.2.3 to PC2 and blocks it from going to other clients

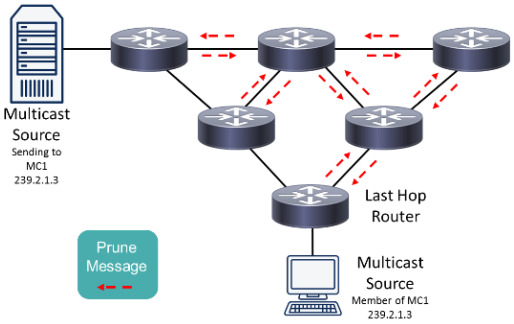
- *Protocol Independent Multicast (PIM)*
  - Routes multicast traffic between multicast-enabled routers
  - Multicast routing protocol forms a *multicast distribution tree*
    - *PIM Dense Mode (PIM-DM)*
      - Uses periodic flood and prune behavior to form optimal distribution tree
      - Causes a negative performance impact on the network
      - Rarely used in modern networks
    - *PIM Sparse Mode (PIM-SM)*
      - Initially uses a shared distribution tree, which may be suboptimal, but…
      - Eventually creates an optimal distribution tree through shortest path tree (SPT) switchover

- **PIM Dense Mode: Flooding**



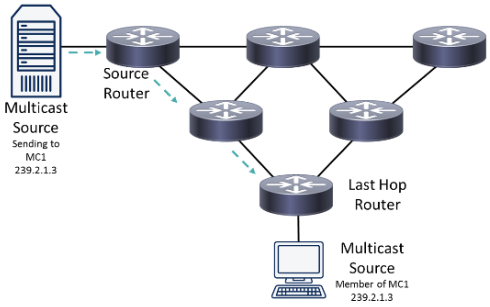
  - Uses source distribution tree (SDT) to form an optimal path between source router and last-hop router
  - Before the optimal path is formed, entire network is initially flooded and consumes unnecessary bandwidth

- **PIM Dense Mode: Pruning**



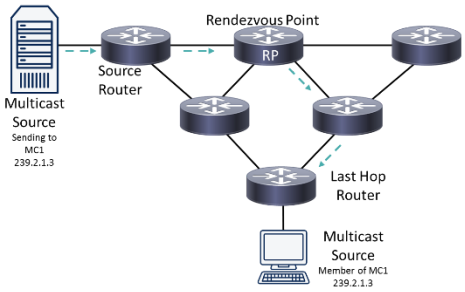
  - If a router receives multicast traffic in the initial flood and the traffic is not needed, then the router sends a prune message asking to be removed from the source distribution tree

- **PIM Dense Mode: After Pruning**

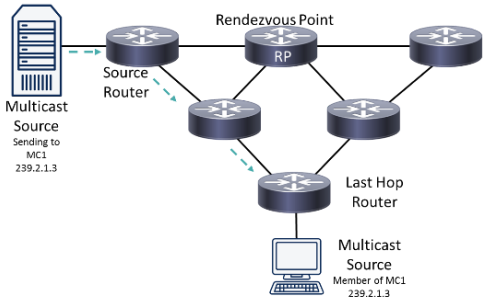


  - After sending prune messages, the resulting source distribution tree has an optimal path between source router and last-hop router
  - Flood and prune repeat every 3 minutes which can cause excessive performance impacts on the network

- **PIM Sparse Mode: Shared Distribution Tree**



  - An optimal path between the source and last-hop routers is not initially created
  - Instead, a multicast source sends traffic directly to a rendezvous point (RP)
  - All last-hop routers send join messages to the RP



  - Originally provides a suboptimal distribution tree, but when first multicast packet is received by last-hop router, then optimal distribution tree is created based on unicast routing table
  - Unneeded branches are pruned during Shortest Path Tree (SPT) switchover

Networks Services

Objective 1.6: Explain the use and purpose of network services

- **Dynamic Host Configuration Protocol (DHCP)**
  - Assigns devices with IP addresses and also provides them a subnet mask, default gateway, and DNS server
  - Operates over ports 67 and 68 using UDP

- **Domain Name System (DNS)**
  - Converts domain names to IP addresses using a hierarchical and decentralized system of naming
  - Operates over UDP and TCP using port 53

- **Zone Transfer**
  - Sharing of information between DNS servers about which domain names they have and their associated IP addresses

- **Network Time Protocol (NTP)**
  - Synchronizes clocks between systems communicating over a packet-switched, variable-latency data network
  - Sent over UDP using port 123

- **Dynamic Host Configuration Protocol (DHCP)**
    - DHCP also help eliminate configuration errors
        - Each device will automatically get assigned an IP from a scope
            - *Scope*
                - A list of valid IP addresses that are available for assignment or lease to a client computer or endpoint device on a given subnet
        - Use a DHCP reservation
        - DHCP server will acknowledge the IP that is being used
    - D-O-R-A process
        - Discover, Offer, Request and Acknowledge
    - If a device attempts to use DHCP and fails to receive its configuration, what should it do?
        - It is set to use an APIPA address, or automatic private IP address
    - *DHCP Relay*
        - Any host that forwards DHCP packets between clients and servers
    - DHCP is that it operates using the User Datagram Protocol or UDP
    - If the DHCP client and server are on different network segments, the router on the client's network segment must be configured with an IP helper address for DHCP to work properly

- **Domain Name System (DNS)**
    - Used to help your network clients find a website using human-readable hostnames instead of numeric IP addresses
    - Converts names to numbers and numbers to names
        - *Fully Qualified Domain Name (FQDN)*
            - This is when a domain name is under a top-level provider
            - The most common top-level provider
                - .com
                - .mil
                - .edu
                - .org
                - .net
    - Root Level
        - The highest level in the DNS hierarchy tree and the root name server answers requests in the root zone
        - These servers contain the global list of all the top-level domains, such as .com, .net, .org, .mil, and others
    - Top-level Domains
        - Organizational hierarchy
            - .com
            - .net
            - .org
        - Geographic hierarchy
            - .uk for the United Kingdom
            - .fr for France
            - .it for Italy

- Second-level Domains
  - These domains site directly below the top-level domain
    - For example
      - diontraining.com is a second level domain, and it sits underneath the top-level domain of .com
- Sub-domain
  - A new server underneath a second-level domain
- Host Level
  - This is the lowest and most detailed level inside of the DNS hierarchy and refers to a specific machine

- **DNS Records**
  - *A Records*
    - Address Record
    - Used to link a hostname to an IPv4 address
    - A records work for IPv4 addresses
    - AAAA records work for IPv6 addresses
  - *CNAME Record*
    - Canonical Name Record
    - Used instead of a A record or AAAA record if you want to point a domain to another domain name or subdomain
  - *MX Record*
    - Mail Exchange Record
    - Used to direct emails to a mail server
    - Used to indicate how email messages should be routed using the Simple Mail Transfer Protocol, or SMTP, over port 25

        - Can only be used to point to another domain, not an IP address
    - *SOA Record*
        - Start of Authority Record
        - Used to store important information about a domain or zone
    - *DNS Zone Transfer*
        - The process of sending DNS records data from the primary nameserver to a secondary name server
        - Uses the TCP protocol to transfer the data to ensure data is successfully sent by the primary server and received by the second server
    - *PTR Records*
        - Pointer Records
        - Used to correlate an IP address with a domain name
        - The opposite of an A record
        - Always stored under the .arpa (top-level domain)
    - *TXT Record*
        - Text records
        - Used by domain administrators to add text into the domain name system or DNS
        - A place to store machine-readable data
    - *SRV Records*
        - Service Record
        - Used to specify a host and port for a specific service
        - Can specify a port along with our IP address

- *NS Record*
  - Name Server Record
  - Used to indicate which DNS name server is the authoritative one for a domain
- *External DNS*
  - Records created around the domain names we purchase from a central authority and use on the public internet
- *DNS Resolver*
  - Also known as a DNS cache located on an individual host
  - This temporary database remembers the answers it received from the DNS server
    - *Recursive Lookup*
      - DNS server will hunt it down and report back to your resolver
    - *Interactive Lookup*
      - DNS resolve will continually query DNS servers until it finds the one with the IP for the domain

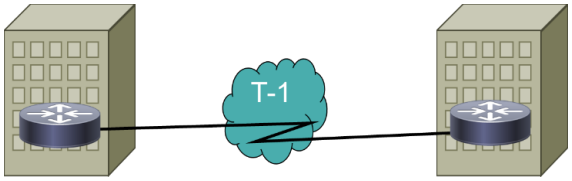
- **Network Time Protocol (NTP)**
  - Synchronizes clocks between systems communicating over a packet-switched, variable-latency data network
  - Sent over UDP using port 123
    - Stratum
    - Clients
    - Servers
  - NTP can handle a maximum of 15 stratum levels

Wide Area Networks

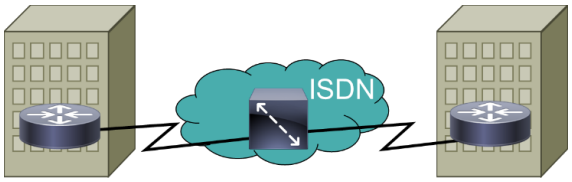
Objectives:

- 1.2 - Explain the characteristics of network topologies and network types
- 2.4 - Given a scenario, install and configure the appropriate wireless standards and technologies

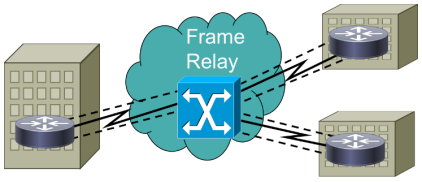
- **Wide Area Networks (WANs)**
  - WANs
    - In the early 1990s, computer-networking design guides commonly invoked the Pareto principle (80-20 rule)
    - Concept is that 80% of traffic stays on the LAN, while only 20% of traffic goes to WAN
    - Today, most network traffic leaves the LAN and travels across the WAN
  - WAN Connection Types
    - Dedicated leased line
    - Circuit-switched connection
    - Packet-switched connection
  - *Dedicated Leased Line*
    - Logical connection that connects two sites through a service provider's facility or telephone company's central office
    - More expensive than other WAN technologies because a customer doesn't share bandwidth with other customers



- *Circuit-Switched Connection*
  - Connection is brought up only when needed, like making a phone call
  - On-demand bandwidth can provide cost savings for customers who only need periodic connectivity to a remote site



- *Packet-Switched Connection*
  - Always on like a dedicated leased line, but multiple customers share the bandwidth
  - SLAs used to guarantee a certain quality (5mbps at least 80% of the time)
  - Virtual circuits are represented as dashed lines



- WAN Physical Media
  - Copper wires
    - Unshielded twisted-pair (UTP)
    - Shielded twisted pair (STP)
    - Coaxial cable
      - Support both analog and digital connections
  - Fiber-optic cable
    - High bandwidth, long distance, and no EMI

- Electric power lines
  - Broadband over Power Lines (BPL)
  - Supports up to 2.7 Mbps
  - Utilizes extensive infrastructure already in place (Power lines)

- WAN Wireless Media
  - Cellular (Phones and Hot Spots)
    - 1G
      - Communicated using a frequency of 30 KHz and had a bandwidth of about 2 kbps
    - 2G
      - Communicated over a GSM network using the 1800 Mhz frequency band
      - Used multiplexing
      - First to have SMS and text messages and international roaming
    - 3G
      - Support 144 Kbps
      - Use a wider frequency band with frequencies from 1.6 Ghz to 2 Ghz
        - *WCDMA*
          - Wideband Code Division Multiple Access
          - Could reach data speeds of up to 2 Mbps
          - The slowest of the 3G technologies
        - *HSPA*
          - High Speed Packet Access standard
          - Could reach speeds of up to 14.4 mbps

        - Referred to as 3.5G
    - *HSPA+*
        - High Speed Packet Access Evolution
        - Brought speed up to around 50 mbps
        - Referred to as 3.75G
- 4G
    - Introduction of multiple input multiple output, or MIMO
    - Uses an even wider frequency band, covering frequencies from 2 to 8 Ghz
    - Often called 4G LTE, or 4G Long Term Evolution
    - It was improved and became LTE Advanced or LTE-A
- 5G
    - Reach speeds up to 10 Gbps using high-band 5G frequencies
    - 5G is split into 3 frequency bands
        - *Low-band Frequencies*
            - Operates between 600-850 MHz and provide us with speeds of 30-250 Mbps
        - *Mid-band Frequencies*
            - Operate between 2.5 to 3.7 Ghz and supports higher data rates of 100-900 Mbps
        - *High-band Frequencies*
            - Operate between 25-39 Ghz
- *Global System for Mobile Communications (GSM)*
    - A cellular technology that takes your voice during a call and converts it to digital data

- A SIM card is used to identify yourself to the network
- *Code-Division Multiple Access (CDMA)*
  - A cellular technology that uses, code division, to split up the channel
  - For every call that is made, the data is encoded with a unique key and then all the data streams can be transmitted at once in a single channel

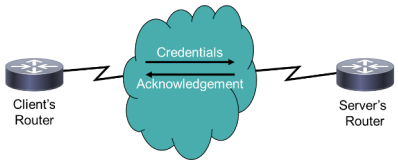
- *Microware*
  - A microwave link is a communication system that use a beam of radio waves in the microwave frequency range to transmit information between two fixed locations
  - Frequencies ranges from 300 Mhz to 300 Ghz
    - WiMax
      - Worldwide Interoperability for Microwave Access
      - Requires an antenna be installed on the roof of your home or office
      - WiMAX is faster than GSM (2G), UMTS (3G), HSPA (3.5G)
    - Satellite
      - Used for remote areas
      - Flying and Shipboard use
      - Expensive in comparison to cellular, cable, or fiber connections
    - Radio
      - Implementation varies country to country based on frequencies

- **Wide Area Network (WAN) Technologies**
  - *Dedicated Leased Line*
    - Point-to-point connection between two sites
      - All bandwidth on line is available all the time
    - Digital circuits are measured in 64-kbps channels called Digital Signal 0 (DS0)
      - *Channel Service Unit / Data Service Unit (CSU/DSU)*
        - Used to terminate the digital signals at customer's demarcation point
    - Common digital circuits include T1, E1, T3, and E3 circuits
    - Examples of Digital Signal Levels

Carrier	Signal Level	Number of T1 Signals	Number of Voice Channels	Speed
T1	DS1	1	24	1.544 Mbps
T1c	DS1c	2	48	3.152 Mbps
T2	DS2	4	96	6.312 Mbps
T3	DS3	28	672	44.736 Mbps
T4	DS4	168	4032	274.760 Mbps
E1	n/a	n/a	30	2.0 Mbps
E3	n/a	n/a	n/a	34.4 Mbps

  - *Metro Ethernet*
    - Service providers are beginning to offer Ethernet interfaces to their customers
    - Less expensive and more common than specialized serial ports used in a CSU/DSU
    - Technology used by service provider is hidden from customer and they only need to connect their network's router to a Smart Jack
  - *Point-to-Point Protocol (PPP)*
    - Commonly used Layer 2 protocol on dedicated leased lines to simultaneously transmit multiple Layer 3 protocols (IP, IPX)

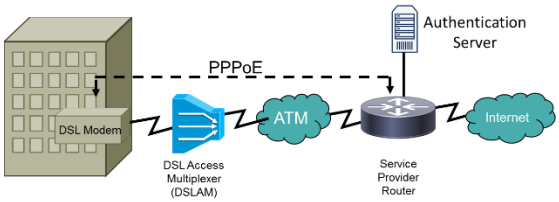
- Each Layer 3 control protocol runs an instance of PPP's Link Control Protocol (LCP)
  - Multilink interface
    - Allows multiple physical connections to be bonded together into a logical interface
  - Looped link detection
    - Layer 2 loop can be detected and prevented
  - Error detection
    - Frames containing errors can be detected and discarded
  - Authentication
    - Device on another end can authenticate the link
- PPP Authentication Methods
  - *Password Authentication Protocol (PAP)*
    - Performs one-way authentication between client & server
    - Credentials sent in clear-text



  - *Challenge-Handshake Authentication Protocol (CHAP)*
    - Challenge-Handshake Authentication Protocol
    - Performs one-way authentication using a three-way handshake
    - Credentials are hashed before transmission

- *Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP)*
  - Microsoft Challenge-Handshake Authentication Protocol
  - Microsoft-enhanced version of CHAP, includes two-way authentication

- *PPP over Ethernet (PPPoE)*
  - Commonly used with DSL modems
  - PPPoE encapsulates PPP frames within Ethernet frames
  - Allows for authentication over Ethernet



- Digital Subscriber Line (DSL)
  - *Asymmetric DSL (ADSL)*
    - Maximum distance to DSLAM: 18,000 feet
    - Voice and Data on same line
    - Downstream: Up to 8 Mbps
    - Upstream: Up to 1.544 Mbps
  - *Symmetric DSL (SDSL)*
    - Maximum distance to DSLAM: 12,000 feet
    - No simultaneous voice and data on same line
    - Downstream: 1.168 Mbps
    - Upstream: 1.168 Mbps

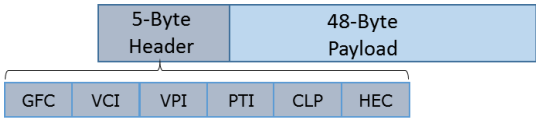
- *Very High Bit-Rate DSL (VDSL)*
  - Maximum distance to DSLAM: 4,000 feet
  - Downstream: Up to 52 Mbps
  - Upstream: Up to 12 Mbps

- Cable Modems
  - *Hybrid Fiber-Coax (HFC) Distribution Network*
    - Cable television infrastructure containing both coaxial and fiber-optic cabling
  - Specific frequency ranges are used for upstream and downstream data transmission as determined by Data-Over-Cable Service Interface Specification (DOCSIS)
    - Upstream (5 MHz to 42 MHz)
    - Downstream (50 MHz to 860 MHz)
  - Transmits and receives over cable television infrastructure
- Satellite Modems
  - Used in remote, rural, or disconnected locations where other connections are not available
  - Provides relatively fast speeds like a DSL modem, but contain low bandwidth usage limits and charge high costs for over limit usage
  - Potential issues with Satellite communications:
    - Delays - Time to satellite and back ($> \frac{1}{4}$ second)
    - Weather conditions
      - Thunderstorms and snow can cause loss of connectivity between satellite and receiver

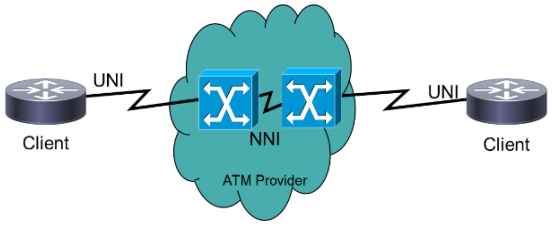
- *Plain Old Telephone Service (POTS)*
  - Public switched telephone network (PSTN) consists of telephone carriers from around the world
  - Analog connections (voice and/or data) using the PSTN
  - Dial-up modems have a maximum bandwidth of 53.3-kbps because they can only access one 64-kbps channel at a time
- *Integrated Services Digital Network (ISDN)*
  - Supports multiple 64-kbps B (Bearer) channels
  - Older technology designed to carry voice, video, or data over B channels
  - D channel (data or delta channel) existed for 64-kbps signaling data
  - Circuits classified as a basic rate interface (BRI) or primary rate interface (PRI)
    - Basic Rate Interface (BRI)
      - Offers a two 64-kbps B-channels with a 16kbps D-channel
    - Primary Rate Interface (PRI)
      - Offers a 1.472-Mbps data path over 23 B-channels and a 64-kbps D-channel
- *Frame Relay*
  - Losing market share due to cable and DSL
    - Frame relay sites connected to virtual circuits (VC)
    - VCs are point-to-point or point-to-multipoint
    - Low cost and widely available
    - Always-on or on-demand
    - Layer 2 technology
- *Synchronous Optical Network (SONET)*
  - Layer 1 technology using fiber as media

- Transports Layer 2 encapsulation (like ATM)
- High data rates (155 Mbps to 10 Gbps)
- Covers large distances (20 km to 250 km)
- Physical topology can be a bus or ring

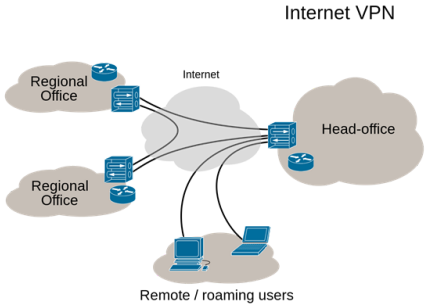
- *Asynchronous Transfer Mode (ATM)*
  - Layer 2 WAN technology operating using Permanent Virtual Circuits (PVCs) and Switched Virtual Circuits (SVCs)
  - Similar to Frame Relay, except all frames are transferred as fixed-length (cells) as its protocol data unit (PDU)
  - Fixed-length cells of 53-bytes used to increase speed of transmissions
    - Contains 48-byte payload and 5-byte header
      - Generic Flow Control (GFC)
      - Virtual Circuit Identifier (VCI)
      - Virtual Path Indicator (VPI)
      - Payload Type Indicator (PTI)
      - Cell Loss Priority (CLP)
      - Header Error Control (HEC)



- ATM Virtual Circuits
  - *User-Network Interface (UNI)*
    - Used to connect ATM switches and endpoints
  - *Network-Node Interface (NNI)*
    - Used to connect ATM switches together



- *Multiprotocol Label Switching (MPLS)*
  - Supports multiple protocols on the same network (used by service providers)
  - Support both Frame Relay and ATM on the same MPLS backbone
  - Allows traffic to be dynamically routed based on load conditions and path availability
  - Label switching is more efficient than Layer 3 IP address routing
  - Used by service providers for forwarding data in the backend, the customer remains unaware of the details
- *Dynamic Multipoint Virtual Private Network (DMVPN)*



  - Allow Internet to be used as WAN connection for secure site-to-site communication
  - VPN tunnel has authentication and encryption so users on the unsecure network cannot read or decrypt the traffic without proper keys
  - Can connect remote locations with low cost, instead of dedicated or leased-line access

- WAN Data Rates
  - Bandwidth measured in Kbps, Mbps, & Gbps
  - ATM and SONET measured by *optical carrier*
    - OC levels are based off of OC-1 (51.84 Mbps)
    - All others are multiples (OC-3 is 155.52 Mbps)

WAN Technology	Typical Available Bandwidth
Frame Relay	56 kbps – 1.544 Mbps
T1	1.544 Mbps
T3	44.736 Mbps
E1	2.048 Mbps
E3	34.4 Mbps
ATM	155 Mbps – 622 Mbps
SONET	51.84 Mbps (OC-1) – 159.25 Gbps (OC-3072)

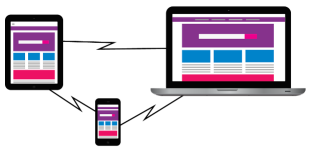
- *Software-Defined Wide Area Network (SDWAN)*
  - A virtual WAN architecture that allows enterprises to leverage any combination of transport services to securely connect users to their applications
  - Uses a centralized control function to securely and intelligently redirect the traffic across the WAN
  - Enable cloud-first enterprises to deliver quality experiences to their users
  - Allows your WAN environment to be more dynamic and efficient
  - Reduces bottlenecks caused by your traditional, centralized WAN architecture
- *Multipoint Generic Routing Encapsulation (mGRE)*
  - A protocol that can be used to enable one node to communicate with many other nodes, essentially creating a point to multipoint link
  - NOT limited to point to point connections
  - Usually combined with the Dynamic Multipoint VPN, or DMVPN, protocol, as well, for security

Wireless Networks

Objectives:

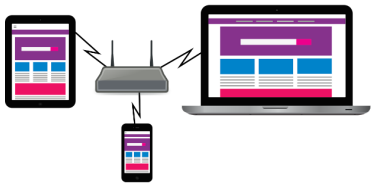
- 2.1 - Compare and contrast various devices, their features, and their appropriate placement on the network
- 2.4 - Given a scenario, install and configure the appropriate wireless standards and technologies
- 4.2 - Compare and contrast common types of attacks
- 4.3 - Given a scenario, apply network hardening techniques
- 5.4 - Given a scenario, troubleshoot common wireless connectivity issues

- **Wireless Networking**
  - *Wireless Local Area Network (WLAN)*
    - Allows users to roam within a coverage area
    - Popularity has increased exponentially
    - Convenient to use and expand network access throughout a room, floor, or building
    - IEEE 802.11 is the most common type
    - Other wireless options exist (used for PAN)
      - Bluetooth
      - Infrared (IR)
      - Near-Field Communications (NFC)
      - Ant+



      - Z-Wave

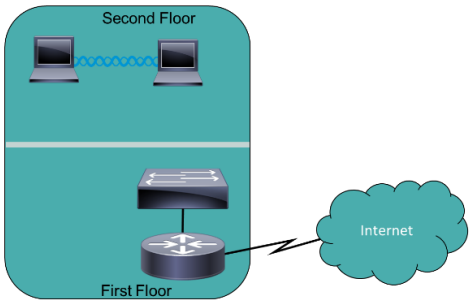
- *Ad Hoc*
  - Wireless devices communicate directly with each other without the need for a centralized access point
  - Peer-to-Peer connections
- Infrastructure



  - Wireless devices communicate with other wireless or wired devices through a wireless router or access point
  - Traditional WiFi in Home and Office networks
- *Wireless Access Point (AP or WAP)*
  - Expands wired LAN into the wireless domain
    - Does not interconnect two networks (not a router)
    - Functions as a hub
  - Connects wired LAN and wireless devices into the same subnet
  - All clients on an access point are on a single collision domain
- *Wireless Router*
  - Gateway device and base station for wireless devices to communicate with each other and connect to the Internet
  - Often combines many features into one device
    - Wireless Access Point (WAP or AP)
    - Router
    - Switch
    - Firewall

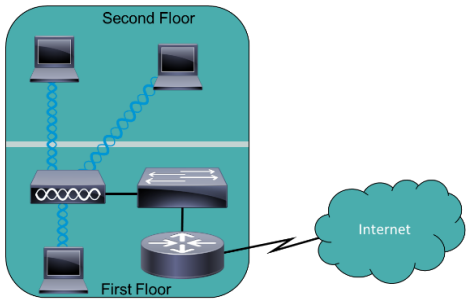
- Fiber, Cable, or DSL modem

- **WLAN Service Sets**
  - Independent Basic Service Set (IBSS)



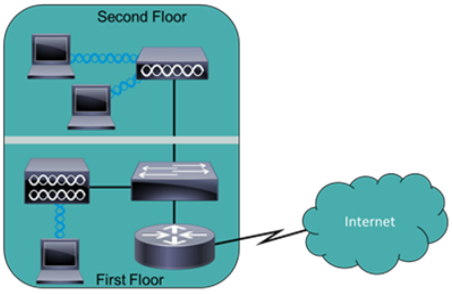
Contains only devices/clients with no APs
(AD-HOC WLAN)

  - Basic Service Set (BSS)



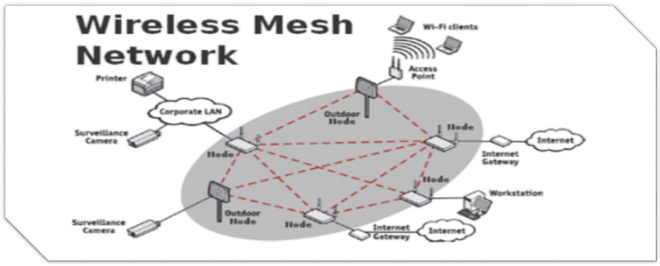
Only one AP connected to the network
(Example: SOHO network)

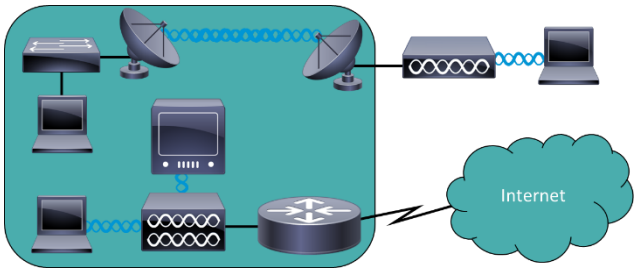
- Extended Service Set (ESS)

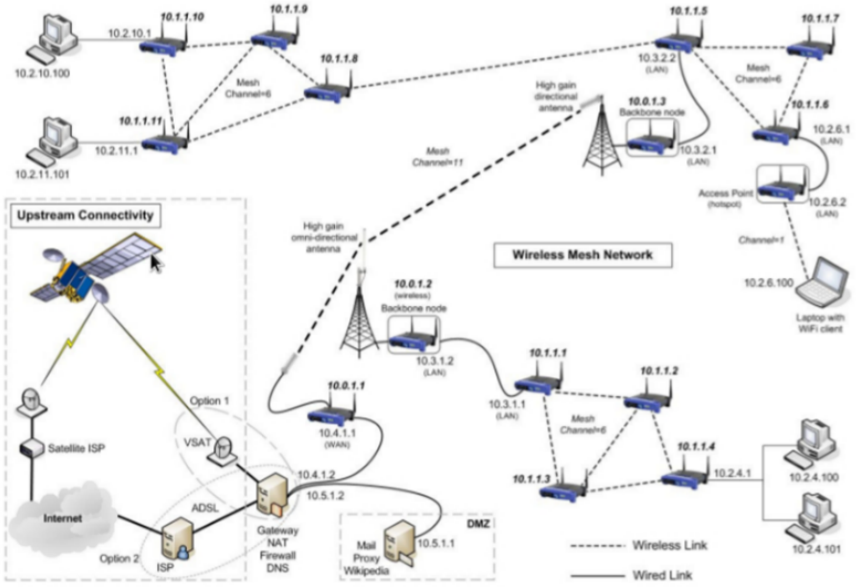


Contains multiple APs to provide coverage
(Example: College Campus)

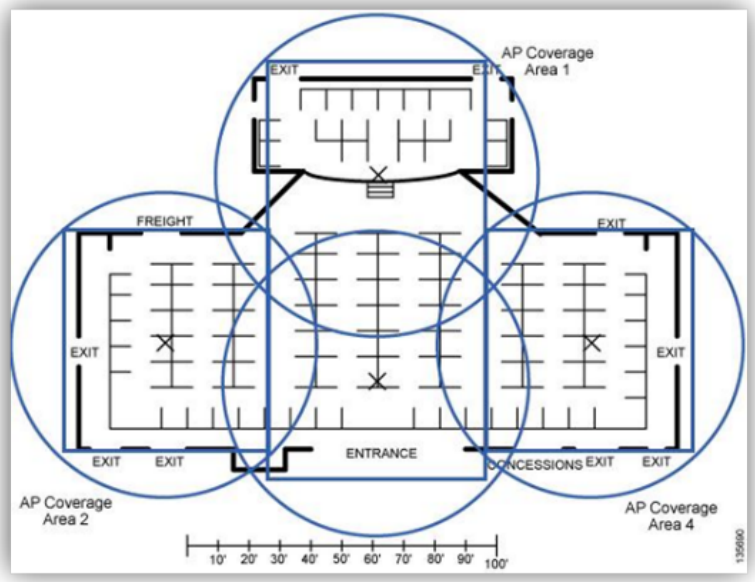
- Mesh Topology
  - May not use a centralized control
  - Range of combined wireless defines network
  - Uses WiFi, Microwave, Cellular, and more





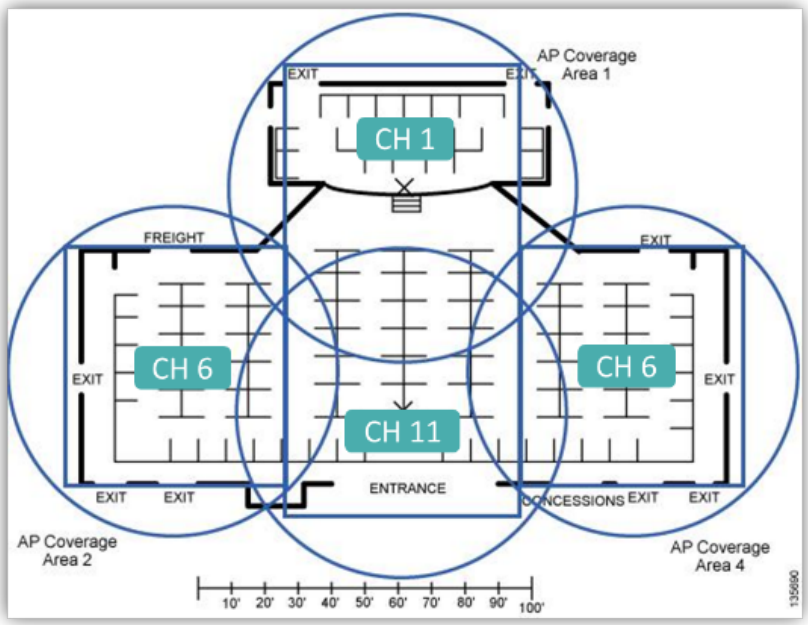


- AP Placement



- Careful planning is required to prevent the APs from interfering with one another and still maintaining the desired coverage area in ESS
- Coverage <u>should</u> overlap between APs to allow uninterrupted roaming from one cell to another but <u>can't</u> use overlapping frequencies

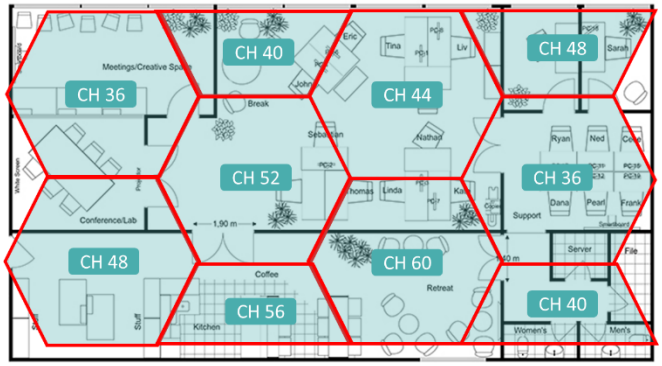
- AP Placement (2.4 Ghz)



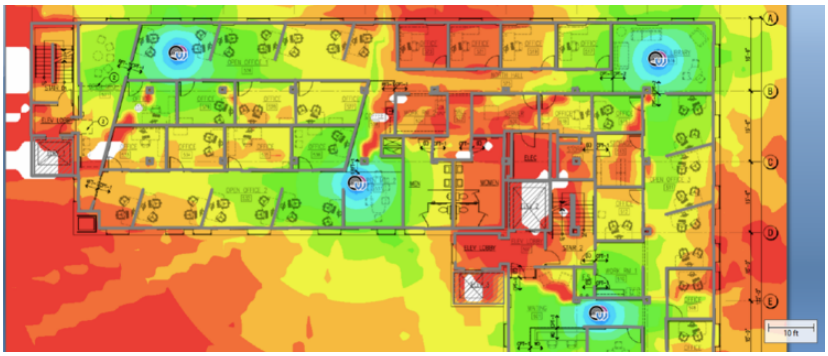
  - Non-overlapping coverage cells for 2.4 GHz band should have 10% to 15% coverage overlap in coverage area

- AP Placement (5 Ghz)

  - Identical channels should be separated by at least two cells instead of one



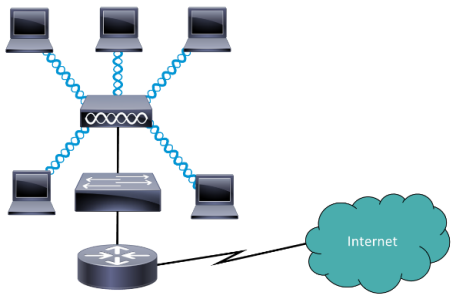
- Site Surveys
  - Wireless survey to determine coverage areas
  - Produces a heat map with coverage



- *Wireless Range Extenders*
  - Specialized device that overcomes distance limitations of wireless networks
  - Amplifies the signal and extends reachability or a wireless cell
  - Wireless repeater receives signal on one antenna and repeats it on other

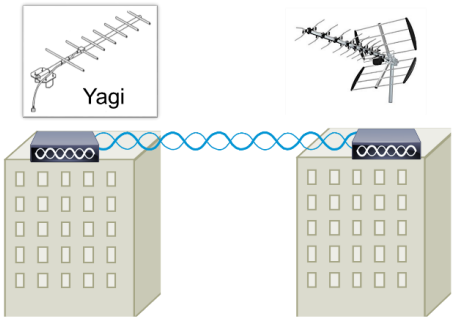
- **Wireless Antennas**
  - Antennas
    - Coverage areas vary based on the type used
    - Most SOHO wireless APs have fixed antennas
    - Enterprise-class APs support different types
    - Factors in antenna effectiveness
      - Distance
      - Pattern of Wireless Coverage
      - Environment (indoor/outdoor)
      - Avoiding Interference with other APs

- Omnidirectional Antenna



Radiates power equally in all directions

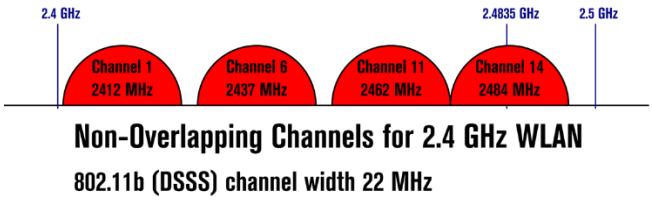
- Unidirectional Antenna



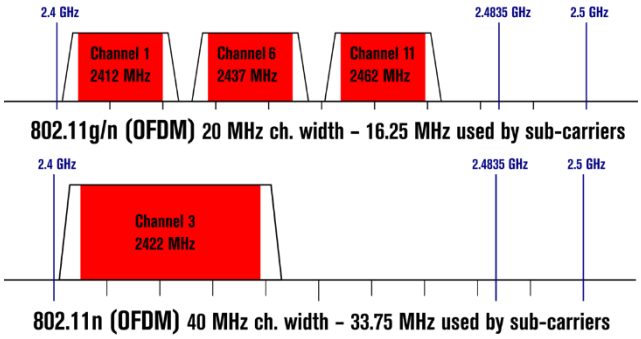
Focuses power in one direction
for covering greater distances

- **Wireless Frequencies**
  - Spread Spectrum Wireless Transmissions
    - Direct-Sequence Spread Spectrum (DSSS)
    - Frequency-Hopping Spread Spectrum (FHSS)
    - Orthogonal Frequency-Division Multiplexing (OFDM)
    - Only DSS and OFDM are commonly utilized in today's WLANs
  - *Direct-Sequence Spread Spectrum (DSSS)*
    - Modulates data over an entire range of frequencies using a series of signals known as chips

- More susceptible to environmental interference
- Uses entire frequency spectrum to transmit



- *Frequency-Hopping Spread Spectrum (FHSS)*
  - Devices hop between predetermined frequencies
  - Increases security as hops occur based on a common timer
- *Orthogonal Frequency Division Multiplexing (OFDM)*
  - Uses slow modulation rate with simultaneous transmission of data over 52 data streams
  - Allows for higher data rates while resisting interference between data streams



- Frequencies and Channels
  - IEEE 802.11 standards are differentiated by their characteristics, such as frequency range used
    - 2.4 GHz band
      - 2.4 GHz to 2.5 GHz range

- 5 GHz band
  - 5.75 GHz to 5.875 GHz range
- Each band has specific frequencies (or channels) to avoid overlapping other signals
- Channels 1, 6, and 11 will avoid overlapping frequencies in 2.4 GHz band

- *Channel Bonding*
  - Allows you to create a wider channel by merging neighboring channels into one
- 802.11 Wireless Standards

Standard	Band	Bandwidth
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n (Wi-Fi 4)	2.4 and 5 GHz	150 Mbps/ 600 Mbps (MIMO)
802.11ac (Wi-Fi 5)	5 GHz	3 Gbps (MU-MIMO)
802.11ax (Wi-Fi 6)	2.4, 5, and 6 GHz	9.6 Gbps (MU-MIMO)

  - 802.11 ax
    - 6 Ghz spectrum
    - Can reach speeds of up to 9.6 Gbps using MU-MIMO technology
    - Fully backward compatible with Wireless A, B, G, N, and AC devices

- *Radio Frequency Interference (RFI)*
  - Caused by using similar frequencies to WLAN
  - Common sources of interference
    - Other wifi devices (overlapping channels)
    - Cordless phones and baby monitors (2.4 GHz)
    - Microwave ovens (2.4 Ghz)
    - Wireless security systems (2.4 GHz)
    - Physical obstacles (Walls, appliances, cabinets)
    - Signal strength (Configurable on some devices)
- Carrier Sense Multiple Access/Collision (Avoidance/ Detection)
  - WLAN uses CSMA/CA to control access to medium, where wires Ethernet uses CSMA/CD
  - Listens for transmission to determine if safe to transmit
    - If channel is clear, transmits Request to Send (RTS)
    - Device waits for acknowledgment
    - If received an RTS, responds with Clear to Send (CTS)
    - If not received, device starts random back off timer

- **Wireless Security**
  - Wireless networks offer convenience, but also many security risks
    - Encryption of data transferred is paramount to increasing security
  - Pre-Shared Key
    - Both AP and client uses same encryption key
    - Problems
      - Scalability is difficult if key is compromised
      - All clients must know the same password

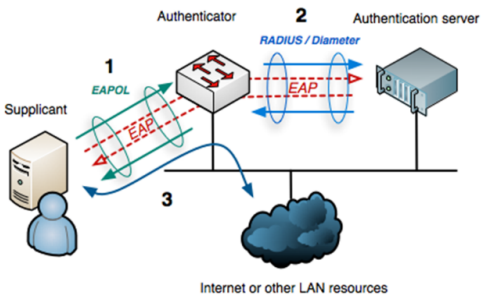
- *Wired Equivalent Privacy*
  - Original 802.11 wireless security standard
    - Claimed to be as secure as wired networks
  - Static 40-bit pre-shared encryption key
    - Upgraded to 64-bit and 128-bit key over time
  - Uses 24-bit Initialization Vector (IV)
    - Sent in clear text
  - Brute Force Attack within minutes using AirCrack-ng and other tools
- *Wi-Fi Protected Access (WPA)*
  - Replaced WEP and its weaknesses
  - Temporal Key Integrity Protocol (TKIP)
    - 48-bit Initialization Vector (IV) instead of 24-bit IV
    - Rivest Cipher 4 (RC4) used for encryption
  - Uses Message Integrity Check (MIC)
    - Confirms data was not modified in transit
  - Enterprise Mode WPA
    - Users can be required to authenticate before exchanging keys
    - Keys between client and AP are temporary
- *Wi-Fi Protected Access 2 (WPA2)*
  - Created as part of IEEE 802.11i standard
    - Requires stronger encryption and integrity checks
    - Integrity checking through CCMP
      - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
  - Uses Advanced Encryption Standard (AES)
    - 128-bit key or above

- Supports two modes
  - Personal mode with pre-shared keys
  - Enterprise mode with centralized authentication

- WiFi Exam Tips

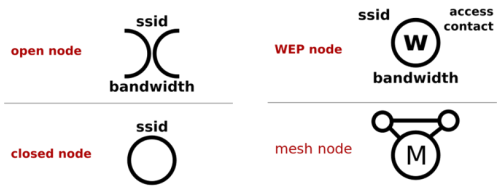
If you are asked about…	Look for the answer with…
Open	No security or protection
WEP	IV
WPA	TKIP and RC4
WPA2	CCMP and AES

- WEP and WPA/WPA2 Security Cracking
  - Utilities can capture wireless packets and run mathematical algorithms to determine the pre-shared key
- Network Authentication 802.1x
  - Each wireless user authenticates with their own credentials
  - Used also in wired networks
- Extensible Authentication Protocol (EAP)
  - Authentication performed using 802.1x
  - EAP-FAST
    - Flexible Authentication via Secure Tunneling
  - EAP-MD5
  - EAP-TLS



- *MAC Address Filtering*
  - Configures an AP with a listing of permitted MAC addresses (like an ACL)
  - Problems
    - Knowledgeable users can falsify their MAC easily using freely available tools
    - Examples
      - MAC Address Changer (Windows)
      - MacDaddyX (OSX)
      - Macchanger (Linux)
- *Network Admission Control (NAC)*
  - Permits or denies access to the network based on characteristics of the device instead of checking user credentials
  - Conducts a posture assessment of client
    - Checks the OS and antivirus version of client
- *Captive Portals*
  - Web page that appears before the user is able to access the network resources
  - Webpage accepts the credentials of the user and presents them to the authentication server
- *Geofencing*
  - GPS or RFID defines real-world boundaries
  - Barriers can be active or passive
  - Device can send alerts if it leaves area
  - Network authentication can use it to determine access
- Disable SSID Broadcast
  - Configures an AP to not broadcast the name of the wireless LAN

- Problem
  - Knowledgeable users can still easily find the SSID using wireless sniffing tools
- *Rogue Access Point*
  - Malicious users set up an AP to lure legitimate users to connect to the AP
  - Malicious users can then capture all the packets (data) going through the rogue access point
- Unsecured Wireless Networks
  - *War Driving*
    - Occurs when users perform reconnaissance looking for unsecured wireless networks
  - *War Chalking*
    - Occurs when users write symbols on a wall to notify others of AP characteristics



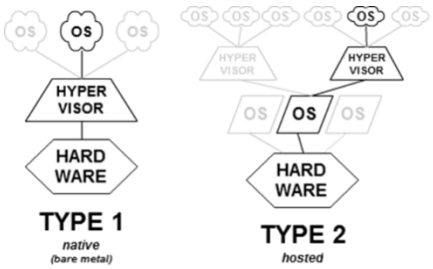
Cloud and the Datacenter

Objectives:

- 1.2 - Explain the characteristics of network topologies and network types
- 1.7 - Explain the characteristics of network topologies and network types
- 1.8 - Summarize cloud concepts and connectivity options
- 2.1 - Compare and contrast various devices, their features, and their appropriate placement on the network

- **Virtual Network Devices**
    - Major shift in the way data centers are designed, fielded, and operated
        - Virtualization is everywhere
            - Virtual Servers
            - Virtual Routers
            - Virtual Firewalls
            - Virtual Switches
            - Virtual Desktops
            - VoIP
            - Cloud Computing
            - Software-Defined Networking
    - *Virtual Servers*
        - Allows multiple virtual instances to exist on a single physical server Considerable cost savings for an IT budget
        - Allows for consolidation of physical servers
        - Multiple NICs increase bandwidth available

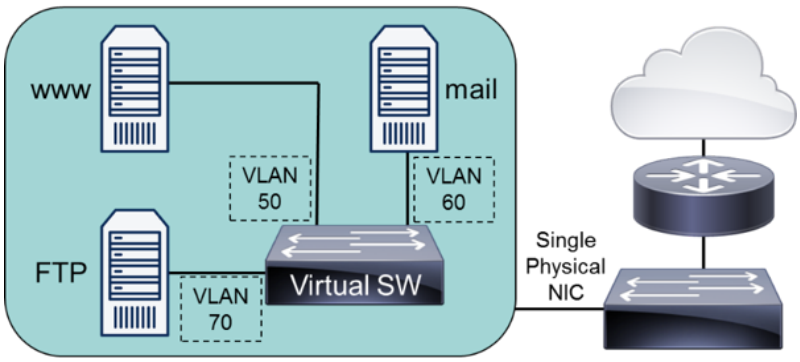
- *Hypervisor*



  - Specialized software that enables virtualization to occur
  - Hypervisor is the software that emulates the physical hardware
  - Also called a Virtual Machine Monitor (VMM)
  - Examples
    - VMWare ESXi
    - Microsoft Hyper-V
    - Virtual Box
    - VMWare Workstation
- Virtualized Storage Solutions
  - *Network Attached Storage (NAS)*
    - Disk storage is delivered as a service over TCP/IP
  - *Storage Area Network (SAN)*
    - Specialized LAN designed for data transfer/storage
    - Transfers data at block level with special protocol
    - *Fibre Channel (FC)*
      - Special purpose hardware providing 1-16 Gbps
    - *Fibre Channel over Ethernet (FCoE)*
      - Removes need for specialized hardware
      - Runs over your Ethernet networks

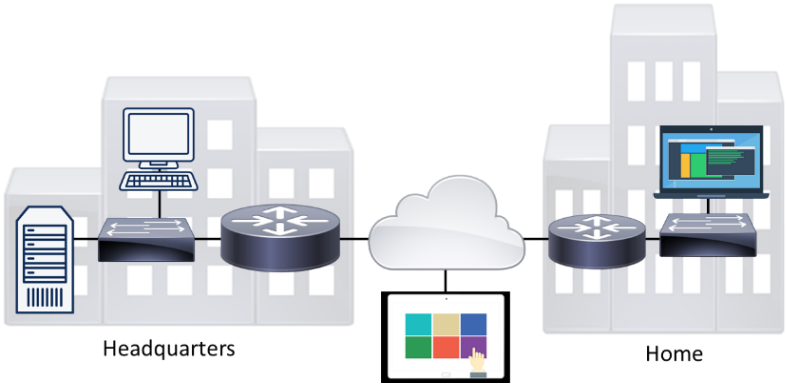
- *iSCSI (IP Small Computer System Interface)*
  - Lower cost, built using Ethernet switches (<10 Gbps)
  - Relies on configuration allowing jumbo frames over the network

- *Infiniband (Virtualized Storage)*
  - Switched fabric topology for high-performance computing
  - Very high throughput (>600 Gbps) with very low latency (0.5 µsec)
  - Direct or switched connection between servers and storage systems
- Virtual Firewalls and Routers
  - To fully virtualize your network, you will need a firewall and router
  - Manufacturer's offer virtualized versions of their most popular devices
  - Virtualized routers and firewalls provide the same features as their physical counterparts
- *Virtual Switches*

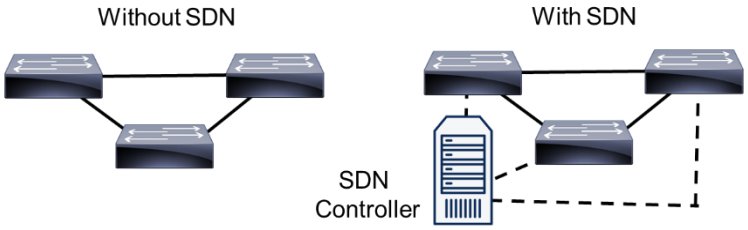


  - Allow the use of VLANs and trunking to divide up the broadcast domain
  - Layer 2 control provides VLANs and trunking
  - Provides Quality of Service and security

- *Virtual Desktops*



  - User's desktop computer is run in browser
  - Used from web, laptop, tablet, or phone
  - Easier to secure and upgrade for the admins
- *Software-Defined Networking (SDN)*

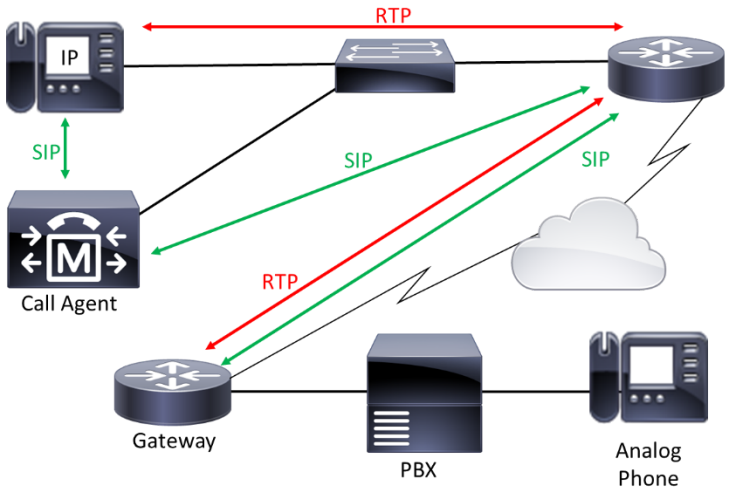


  - Provides the administrator with an easy-to-use front end to configure physical and virtual devices throughout the network
  - All the configurations are automatically done
  - Provides administrator and overview of the entire network

- **Voice over IP (VoIP)**
  - *Voice over IP (VoIP)*
    - Digitizes voice traffic so that it can be treated like other data on the network

- Uses the SIP (Session Initiation Protocol) to set up, maintain, and tear down calls
- VoIP can save a company money and provide enhanced services over a traditional PBX solution

- VoIP Topology
  - User's desktop computer is run in browser



- Virtual Private Branch Exchange (PBX) and VoIP
  - Ability to outsource your telephone system
  - Utilizes VoIP to send all data to provider, then provider connects it to telephone system

- **Cloud Computing**
  - Cloud Computing
    - *Private Cloud*
      - Systems and users only have access with other devices inside the same private cloud or system

- *Public Cloud*
  - Systems and users interact with devices on public networks, such as the Internet and other clouds
- *Hybrid Cloud*
  - Combination of private and public
- *Community Cloud*
  - Collaborative effort where infrastructure is shared between several organizations from a specific community with common concerns

- Models of Cloud Computing
  - Network as a Service (NaaS)
  - Infrastructure as a Service (Iass)
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
- *Network as a Service (NaaS)*
  - Allows outsourcing of the of a network to a service provider
  - Hosted off-site at the service provider's data center and the customer is billed for usage
  - Charged by hours, processing power, or bandwidth used like utility services
  - Amazon's VPC or Route 53 offerings
- *Infrastructure as a Service (IaaS)*
  - Allows outsourcing of the infrastructure of the servers or desktops to a service provider
  - Hosted off-site at the service provider's data center and the customer is billed for usage

        - Charged by hours, processing power, or bandwidth used like utility services
        - Examples
            - Amazon Web Services (AWS)
            - Microsoft's Azure
    - *Software as a Service (SaaS)*
        - User interacts with a web-based application
        - Details of how it works are hidden from users
        - Examples
            - Google Docs
            - Office 365
    - *Platform as a Service (PaaS)*
        - Provides a development platform for companies that are developing applications without the need for infrastructure
        - Dion Training uses PaaS for our courses
        - Examples
            - Pivotal
            - OpenShift
            - Apprenda
    - *Desktop as a Service (DaaS)*
        - Provides a desktop environment that is accessible through the Internet in the form of a cloud desktop or virtual desktop environment
            - Virtual Desktop Infrastructure (VDI)

- **Cloud Concepts**
    - *Elasticity*
        - Attempts to match the resources allocated with the actual amount of resources needed at any given point in time
        - Elasticity is focused on meeting the sudden increases and decreases in the workload
    - *Scalability*
        - Handles the growing workload required to maintain good performance and efficiency for a given software or application
            - Elasticity
                - Short-term addition or subtraction of resources
            - Scalability
                - Long-term planning and adoption
    - *Vertical Scaling (Scaling Up)*
        - Increasing the power of the existing resources in the working environment
    - *Horizontal Scaling (Scaling Out)*
        - Adding additional resources to help handle the extra load being experienced
            - Vertical - Scalability
            - Horizontal - Elasticity
        - Scaling out provides more redundancy and results in less downtime
    - *Multitenancy*
        - Allowing customers to share computing resources in a public or private cloud
            - Better storage/access

        - Better use of resources
        - Lower overall cost
    - Multitenancy might cause your data to be hosted on the same physical server as another organization's data
        - When an organization crashes a physical server, all of the organizations hosted on that same server are affected
        - An organization failing to secure its virtual environments hosted on a shared server poses a security risk for the other organizations hosting on that same server
    - Set up virtual servers in the cloud with proper failover, redundancy, and elasticity
        - Complex passwords
        - Strong authentication
        - Strong encryption
        - Strong policies
- *Virtual Machine (VM) Escape*
    - Occurs when an attacker breaks out of one of the isolated VMs and begins to directly interact with the underlying hypervisor
    - Host virtual servers on the same physical server as other VMs in the same network

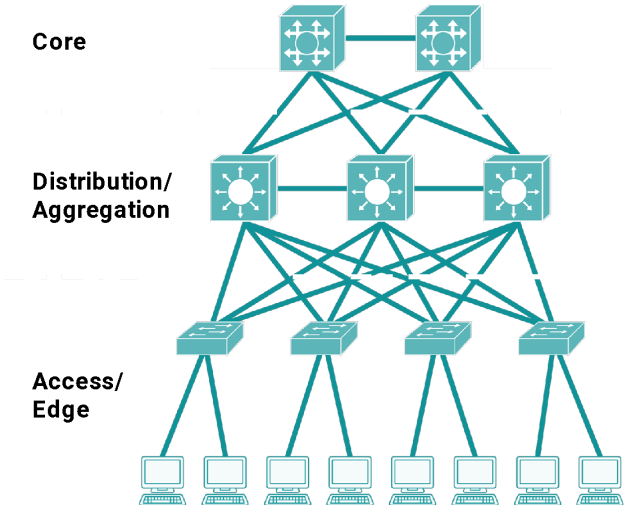
- **Infrastructure as Code (IAC)**
    - Enables managing and provisioning of infrastructure through code instead of through manual processes
        - Virtual machines
        - Virtual devices

- Scripted automation and orchestration
  - *Orchestration*
    - Process of arranging or coordinating the installation and configuration of multiple systems
      - Lower costs
      - Speed up deployments
      - Increase security
  - *Snowflake Systems*
    - Any system that is different from the standard configuration template used within your organization's IaC architecture
    - Keeping things consistent and using carefully-developed and tested scripts

- **Connectivity Options**
  - *Virtual Private Network (VPN)*
    - Establishes a secure connection between on-premises network, remote offices, client devices, and provider's global network
      - Amazon Web Services - Direct Connect Gateway
      - Microsoft Azure - Azure Private Link
  - *Private-Direct Connection*
    - Extends pre existing, on-premise data center into the provider's network to directly connect to your virtual private cloud network

	Private-Direct	VPN
Faster speed	✓	✗
Better performance	✓	✗
Supports multiple VPCs	✓	✗
Better redundancy	✓	✗
Cheaper	✗	✓

- **Datacenter Architecture**
  - *Datacenter*
    - Any facility that businesses and other organizations use to organize, process, store, and disseminate large amounts of data
  - Types
    - Three-tiered hierarchy
    - Software-defined networking
    - Spine and leaf architecture
    - Traffic flows
    - On-premise versus hosted data centers



- Benefits
  - Performance
  - Management
  - Scalability
  - Redundancy
- *Software-Defined Networking (SDN)*
  - Enables the network to be intelligently and centrally controlled, or programmed, using software applications
  - *Application Layer*
    - Focuses on the communication resource requests or information about the network as a whole
  - *Control Layer*
    - Uses the information from the applications and decides how to route a data packet on the network
  - *Infrastructure Layer*
    - Contains the network devices that receive information about where to move the data and then performs those movements

- Provides a layer of abstraction between the devices and the control and data flow that happen on the network

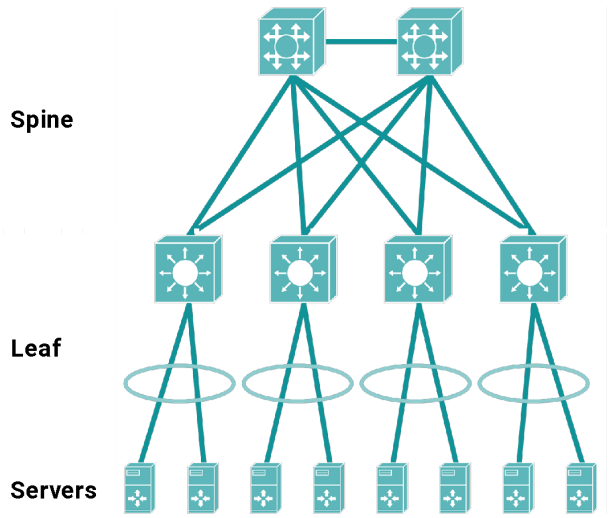
■ *Management Plane*

- Used to monitor traffic conditions and the status of the network

○ Architectures

■ *Spine and Leaf Architecture*

- An alternative type of network architecture that focuses on the communication within the datacenter itself



- Spine and leaf architecture can give faster speeds and lower latency
- This architecture can be used in combination with the standard three-tiered hierarchy
- *North-South*
  - Traffic that enters or leaves the data center from a system physically residing outside the datacenter
  - Northbound is data leaving the datacenter
  - Southbound is data entering the datacenter

- *East-West*
    - Refers to data flow within a datacenter
- *On-premise*
    - A traditional, private data infrastructure usually located in the same building as the main offices
- *Co-located*
    - A datacenter environment owned by another company
- *Cloud-based*
    - Migrating company data out of own server and datacenters and into a cloud service provider's servers and datacenters

Network Security

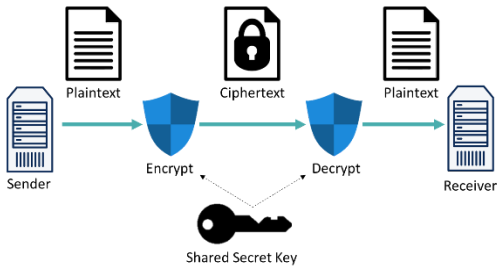
Objectives:

- 4.1 - Explain common security concepts
- 4.3 - Given a scenario, apply network hardening techniques
- 4.5 - Explain the importance of physical security

- **CIA Triad**
    - Network Security Fundamentals
        - Networks are increasingly dependent on interconnecting with other networks
        - Risks exist not just on the untrusted Internet, but also inside our own organization's networks and must be minimized or eliminated
        - Understanding the various threats facing our networks is important in order to best defend the network against the onslaught of cyber-attacks they are constantly facing
    - Network Security Goals
        - Commonly called the CIA Triad
            - Confidentiality
            - Integrity
            - Availability
    - *Confidentiality*
        - Keeping the data private and safe
            - Encryption
            - Authentication to access resources
        - Encryption ensures that data can only be read (decoded) by the intended recipient

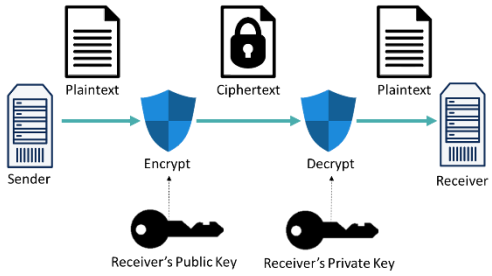
- Symmetric encryption
- Asymmetric encryption

- *Symmetric Encryption (Confidentiality)*
  - Both sender and receiver use the same key
  - *DES (Data Encryption Standard)*
    - Developed in the mid-1970s
    - 56-bit key
    - Used by SNMPv3
    - Considered weak today
  - *3DES (Triple DES)*
    - Uses three 56-bit keys (168-bit total)
    - Encrypt, decrypt, encrypt
  - *AES (Advanced Encryption Standard)*
    - Preferred symmetric encryption standard
    - Used by WPA2
    - Available in 128-bit, 192-bit, and 256-bit keys
  - Sender and receiver use the same key to encrypt and decrypt the messages

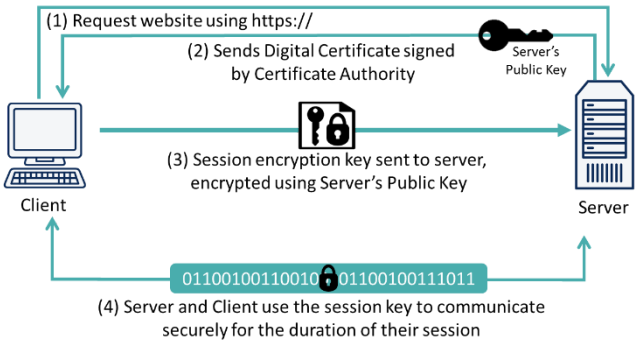


- *Asymmetric Encryption (Confidentiality)*
  - Uses different keys for sender and receiver
  - RSA is the most popular implementation

- RSA algorithm is commonly used with a public key infrastructure (PKI)
- PKI is used to encrypt data between your web browser and a shopping website
- Can be used to securely exchange emails
- Sender and receiver use different keys to encrypt and decrypt the messages



- Confidentiality with HTTPS
  - Uses asymmetrically encrypted messages to transfer a symmetric key



- *Integrity*
  - Ensures data has not been modified in transit
  - Verifies the source that traffic originates from
  - Integrity violations
    - Defacing a corporate web page
    - Altering an e-commerce transaction
    - Modifying electronically stored financial records

- *Hashing (Integrity)*
  - Sender runs string of data through algorithm
    - Result is a *hash* or *hash digest*
  - Data and its hash are sent to receiver
  - Receiver runs data received through the same algorithm and obtains a hash
  - Two hashes are compared
    - If the same, the data was not modified
- *Hashing Algorithms (Integrity)*
  - *Message Digest 5 (MD5)*
    - 128-bit hash digest

```
Jason (MD5)
472d46cb829018f9
dbd65fb8479a49bb
```

  - *Secure Hash Algorithm 1 (SHA-1)*
    - 160-bit hash digest

```
Jason (SHA-1)
E7e312fea4c2c1aad2bb
075d739111890e1ce08b
```

  - *Secure Hash Algorithm 256 (SHA-256)*
    - 256-bit hash digest

```
Jason (SHA-256)
7fa8a6e9fde2f4e1dfe6fb029af47c96
33d4b7a616a42c3b2889c5226a20238d
```

  - *Challenge-Response Authentication Mechanism Message Digest 5 (CRAMMD5)*
    - Common variant often used in e-mail systems
- *Availability*
  - Measures accessibility of the data
  - Increased by designing redundant networks
  - Compromised by
    - Crashing a router or switch by sending improperly formatted data

- Flooding a network with so much traffic that legitimate requests cannot be processed
    - Denial of Service (DoS)
    - Distributed Denial of Service

- **Threats and Vulnerabilities**
    - *Threat*
        - A person or event that has the potential for impacting a valuable resource in a negative manner
    - *Vulnerability*

        - A quality or characteristic within a given resource or its environment that might allow the threat to be realized
            - *Internal Threat*
                - Any threat that originates within the organization itself
            - *External Threat*
                - Any threat that could be people, like a hacker, or it can be an event or environmental condition

- Environmental Vulnerabilities
  - Undesirable conditions or weaknesses that are in the general area surrounding the building where a network is run
- Physical Vulnerabilities
  - Undesirable conditions or weaknesses in the building where the network is located
- Operational Vulnerabilities
  - Focuses on how the network and its systems are run from the perspective of an organization's policies and procedures
- Technical Vulnerabilities
  - System-specific conditions that create security weaknesses
    - *Common Vulnerabilities and Exposures (CVE)*
      - A list of publicly disclosed computer security weaknesses
    - *Zero-Day Vulnerability*
      - Any weakness in the system design, implementation, software code, or a lack of preventive mechanisms in place
        - CVEs (Known vulnerabilities)
        - Zero-Day (Brand new vulnerability)

- *Exploit*
  - Piece of software code that takes advantage of a security flaw or vulnerability within a system or network
  - Keep systems properly patched and antimalware software updated

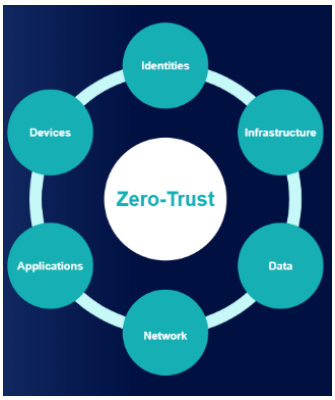
- **Risk Management**
    - The identification, evaluation, and prioritization of risks to minimize, monitor, and control the vulnerability exploited by a threat
    - *Risk Assessment*
        - A process that identifies potential hazards and analyzes what could happen if a hazard occurs
            - Security
            - Business
    - *Security Risk Assessment*
        - Used to identify, assess, and implement key security controls within an application, system, or network
    - *Threat Assessment*
        - Focused on the identification of the different threats that may wish to attack or cause harm to your systems or network
    - *Vulnerability Assessment*
        - Focused on identifying, quantifying, and prioritizing the risks and vulnerabilities in a system or network
            - Nessus
            - QualysGuard
            - OpenVAS
                - Threat controlled by the attacker of event
                - Vulnerability within your control
    - *Penetration Test*
        - Evaluates the security of an IT infrastructure by safely trying to exploit vulnerabilities within the systems or network

- *Posture Assessment*
  - Assesses cyber risk posture and exposure to threats caused by misconfigurations and patching delays
    - Define mission-critical components
    - Identify strengths, weaknesses, and security issues
    - Stay in control
    - Strengthen position
- *Business Risk Assessment*
  - Used to identify, understand, and evaluate potential hazards in the workplace
- *Process Assessment*
  - The disciplined examination of the processes used by the organization against a set of criteria
    - Determines if you are doing things right, and if you are doing the right things
- *Vendor Assessment*
  - The assessment of a prospective vendor to determine if they can effectively meet the obligations and the needs of the business

- **Security Principles**
  - *Least Privilege*
    - Using the lowest level of permissions or privileges needed in order to complete a job function or admin task
  - Role-based Access
    - *Discretionary Access Control (DAC)*
      - An access control method where access is determined by the owner of the resource
        - Every object in a system has to have an owner
        - Each owner must determine the access rights and permissions for each object
    - *Mandatory Access Control (MAC)*
      - An access control policy where the computer system gets to decide who gets access to what objects
        - Unclassified
        - Confidential
        - Secret
        - Top secret
  - *Role-Based Access Control (RBAC)*
    - An access model that is controlled by the system but focuses on a set of permissions versus an individual's permissions
    - Creating groups makes it easy to control permissions based around actual job functions
  - *Zero-Trust*
    - A security framework that requires users to be authenticated and authorized before being granted access to applications and data

- Reexamine all default access controls
- Employ a variety of prevention techniques and defense in depth
- Enable real-time monitoring and controls to identify and stop malicious activity quickly
- Ensure the network's zero-trust architecture aligns to a broader security strategy

- **Defense in Depth**



  - Cybersecurity approach in which a series of defensive mechanisms are layered in order to protect valuable data and information
    - Physical
    - Logic
    - Administrative
  - *DMZ*
    - A perimeter network that protects an organization's internal local area network from untrusted traffic

- *Screen Subnet*
  - Subnet in the network architecture that uses a single firewall with three interfaces to connect three dissimilar networks
    - Triple-homed firewall
- Separation of Duties
  - Prevent frauds and abuse by distributing various tasks and approval authorities across a number of different users
- *Dual Control*
  - Two people have to be present at the same time to do something
- *Split Knowledge*
  - Two people each have half of the knowledge of how to do something
- *Honeypot/ Honeynet*
  - Attracts and traps potential attackers to counteract any attempts at unauthorized access to a network
  - Think vertical through the layers as well as horizontal or lateral across the network using screen subnets

- **Multi Factor Authentication**
  - Authenticates or proves an identity using more than one method
    - Something you know
    - Something you have
    - Something you are
    - Something you do
    - Somewhere you are

- *Dictionary Attack*
  - Guesses the password by attempting to check every single word or phrase contained within a word list, called a dictionary
    - Do not use anything that looks like a regular word
- *Brute Force Attack*
  - Tries every possible combination until they figure out the password
    - Use a longer and more complicated password
      - Uppercase
      - Lowercase
      - Numbers
      - Special characters
    - For good security, use a minimum of 12 characters
- *Hybrid Attack*
  - Combination of dictionary and brute force attacks

Authentication	AKA	Examples
Something you know	Knowledge	• Usernames • Passwords • PINs • Personal question answers
Something you have	Possession	• Smartcards • RSA key fobs • RFID tags
Something you are	Inherence	• Fingerprints • Retina scans • Voice prints
Something you do	Action	• How you sign your name • How you draw a pattern • How you say a catchphrase
Somewhere you are	Location	• Geotagging • Geofencing

- **Authentication Methods**
  - *Local Authentication*
    - Process of determining whether someone or something is who or what it
      - Claims itself to be
      - Simplified version of X.500
  - *Lightweight Directory Access Protocol (LDAP)*
    - Validates a username and password combination against an LDAP server as a form of authentication
      - Port 389 LDAP
      - Port 636 LDAP Secure
  - *Active Directory (AD)*
    - Organizes and manages everything on the network, including clients, servers, devices, and users
  - *Kerberos*
    - Focused on authentication and authorization within a Windows domain environment
    - Provides secure authentication over an insecure network

- **Network Access Protocols**
  - *Remote Authentication Dial-In User Service (RADIUS)*
    - Provides centralized administration of dial-up, VPN, and wireless network authentication
      - Authentication
      - Authorization
      - Accounting

        - Commonly uses
            - Port 1812 Authentication messages
            - Port 1813 Accounting messages
        - Proprietary versions of RADIUS may also use
            - Port 1645 Authentication messages
            - Port 1646 Accounting messages
- *Terminal Access Controller Access Control System Plus (TACACS+)*
    - Used to perform the role of an authenticator in an 802.1x network
        - RADIUS (UDP)
        - TACACS+ (TCP)
        - Ensure Port 49 is open
        - Excellent if using Cisco devices
- *802.1x*
    - A standardized framework that's used for port-based authentication on both wired and wireless networks
        - Supplicant
        - Authenticator
        - Authentication server
- *Extensible Authentication Protocol (EAP)*
    - Allows for numerous different mechanisms of authentication
        - *EAP-MD5*
            - Utilizes simple passwords and the challenge handshake authentication process to provide remote access authentication

- *EAP-TLS*
  - Uses public key infrastructure with a digital certificate being installed on both the client and the server
- *EAP-TTLS*
  - Requires a digital certificate on the server and a password on the client for its authentication
- *EAP Flexible Authentication via Secure Tunneling (EAP-FAST)*
  - Uses a protected access credential to establish mutual authentication between devices
- *Protected EAP (PEAP)*
  - Uses server certificates and Microsoft's Active Directory databases to authenticate a client's password
- *Lightweight EAP (LEAP)*
  - A proprietary protocol that only works on Cisco-based devices

- **Network Access Control (NAC)**
  - Ensures a device is scanned to determine its current state of security prior to being allowed network access
  - *Persistent Agent*
    - A piece of software installed on a device requesting access to the network
  - *Non-Persistent Agent*
    - Requires the users to connect to the network and go to a web-based captive portal to download an agent onto their devices

- *IEEE 802.1x*
  - Used in port-based Network Access Control
    - *Time-based*
      - Defines access periods for given hosts on using a time-based schedule
    - *Location-based*
      - Evaluates the location of the endpoint requesting access using IP or GPS geolocation
    - *Role-based (Adaptive NAC)*
      - Reevaluates a device's authentication when it's being used to do something
    - *Rule-based*
      - Uses a complex admission policy that might enforce a series of rules with the use of logical statements

- **Physical Security**
  - Detection Methods
    - Security control used during an event to find out whether or not something malicious may have happened
      - *Wired*
        - Allows the device to be physically cabled from its camera all the way to a central monitoring station
      - *Wireless*
        - Easier to install, but they can interfere with other wireless systems, like 802.11 wireless networks

- Indoor and Outdoor
  - Indoor cameras tend to be lighter, cheaper, and easier to install
- *Infrared System*
  - Displays images based on the amount of heat in a room
    - Quickly and easily identify where a person is inside the room
    - Identify hot spots in the room and detect gear that could overheat before it actually does
- *Ultrasonic Camera*
  - A type of surveillance camera that uses sound-based detection
- *Asset Tag*
  - Identifies a piece of equipment using a unique serial number, code, or barcode
    - Reduce theft and helps to identify the device
- *Tamper Detection*
  - Ensures a network equipment has not been modified once labeled and stored
- *eFuse*
  - An electronic detection mechanism that can record the version of the IOS used by a switch

- Prevention Method
  - Security control used to prevent incidents from occurring
    - Access control hardware
    - Access control vestibules
    - Smart lockers
    - Locking racks
    - Locking cabinets

        - Employee training
    - *Access Control Vestibule (Mantrap)*
        - An area between two doorways that holds people until they are identified and authenticated
    - *Smart Locker*
        - A fully integrated system that allows you to keep your laptop, tablet, smartphone, or other valuables inside
            - 69% ROI
                - Small and medium sized business
            - 248% ROI
                - Large enterprises

- **Asset Disposal**
    - Occurs whenever a system is no longer needed by an organization
        - Perform a factory reset
        - Wipe the configuration
        - Sanitize the devices
    - *Factory Reset*
        - Removes all customer specific data that has been added to a network device since the time it was shipped from the manufacturer
            - Enable
            - Factory-reset all
            - Write-erase
        - NVRAM stores configuration files
        - Flash Module stores the Cisco IOS

- *Degaussing*
  - Exposes the hard drive to a powerful magnetic field to wipe previously written data from the drive
- *Purging/Sanitizing*
  - Removes data which cannot be reconstructed using any known forensic techniques
- *Clearing Technique*
  - Removes data with a certain amount of assurance that it can't be reconstructed
- *Data Remnants*
  - Leftover pieces of data that may exist in the hard drive which we no longer need
- Network Security Attacks
  - Our security goals (CIA) are subject to attack
  - Confidentiality attack
    - Attempts to make data viewable by an attacker
  - Integrity attack
    - Attempts to alter data
  - Availability attack
    - Attempts to limit network accessibility and usability

Network Attacks

Objective 4.2: Compare and contrast common types of attacks

- **Denial of Service (DoS) Attack**
  - Occurs when one machine continually floods a victim with requests for services
  - *TCP SYN Flood*
    - Occurs when an attacker initiates multiple TCP sessions, but never completes them
  - *Smurf Attack (ICMP Flood)*
    - Occurs when an attacker sends a ping to a subnet broadcast address with the source IP spoofed to be that of the victim server
  - *Distributed Denial of Service (DDoS) Attack*
    - Occurs when an attacker uses multiple computers to ask for access to the same server at the same time
      - *Botnet*
        - A collection of compromised computers under the control of a master node
      - *Zombie*
        - Any of the individually compromised computers

- **General Network Attacks**
  - *On-Path/ Man-in-the-Middle (MITM) Attack*
    - Occurs when an attacker puts themselves between the victim and the intended destination
  - *Session Hijacking*
    - Occurs when an attacker guesses the session ID that is in use between a client and a server and takes over the authenticated session

- *DNS Poisoning*
  - Occurs when an attacker manipulates known vulnerabilities within the DNS to reroute traffic from one site to a fake version of that site
- *DNSSEC*
  - Uses encrypted digital signatures when passing DNS information between servers to help protect it from poisoning
  - Ensure server has the latest security patches and updates
- *Rogue DHCP Server*
  - A DHCP server on a network which is not under the administrative control of the network administrators

- **Spoofing Attacks**
  - *Spoofing*
    - Occurs when an attacker masquerades as another person by falsifying their identity
  - *IP Spoofing*
    - Modifying the source address of an IP packet to hide the identity of the sender or impersonate another client
    - IP spoofing is focused at Layer 3 of the OSI model
  - *MAC Spoofing*
    - Changing the MAC address to pretend the use of a different network interface card or device
  - *MAC Filtering*
    - Relies on a list of all known and authorized MAC addresses
  - *ARP Spoofing*
    - Sending falsified ARP messages over a local area network

        - ARP spoofing attack can be used as a precursor to other attacks
        - Set up good VLAN segmentation within your network
    - *VLAN Hopping*
        - Ability to send traffic from one VLAN into another, bypassing the VLAN segmentation you have configured within your Layer 2 networks
    - *Double Tagging*
        - Connecting to an interface on the switch using access mode with the same VLAN as the native untagged VLAN on the trunk
    - *Switch Spoofing*
        - Attempting to conduct a Dynamic Trunking Protocol (DTP) negotiation
        - Disable dynamic switchport mode on your switch ports

- **Malware**
    - *Malware*
        - Designed to infiltrate a computer system and possibly damage it without the user's knowledge or consent
    - *Virus*
        - Made up of malicious code that is run on a machine without the user's knowledge and infects it whenever that code is run
    - *Worm*
        - A piece of malicious software that can replicate itself without user interaction
    - *Trojan Horse*
        - A piece of malicious software disguised as a piece of harmless or desirable software

- *Remote Access Trojan (RAT)*
  - Provides the attacker with remote control of a victim machine
- *Ransomware*
  - Restricts access to a victim's computer system or files until a ransom or payment is received
- *Spyware*
  - Gathers information about you without your consent
- *Keylogger*
  - Captures any key strokes made on the victim machine
- *Rootkit*
  - Designed to gain administrative control over a computer system or network device without being detected

- **Wireless Attacks**
  - *Rogue Access Point*
    - A wireless access point that has been installed on a secure network without authorization from a local network administrator
  - *Shadow IT*
    - Use of IT systems, devices, software, applications, or services without the explicit approval of the IT department
  - *Evil Twin*
    - Wireless access point that uses the same name as your own network
  - *Deauthentication*
    - Attempts to interrupt communication between an end user and the wireless access point

- *Dictionary Attack*
  - Guesses the password by attempting to check every single word or phrase contained within a word list, called a dictionary
  - Do not use anything that looks like a regular word
- *Brute Force Attack*
  - Tries every possible combination until they figure out the password
  - Use a longer and more complicated password
- *Hybrid Attack*
  - Combination of dictionary and brute force attacks
- *Wireless Interception*
  - Captures wireless data packets as they go across the airwaves

- **Social Engineering Attacks**
  - *Social Engineering*
    - Any attempt to manipulate users to reveal confidential information or perform actions detrimental to a system's security
    - The weakest link is our end users and employees
  - *Phishing*
    - Sending an email in an attempt to get a user to click a link
    - Sending out emails to capture the most people and doesn't really target any particular person or group
  - *Spearphishing*
    - More targeted form of phishing
  - *Whaling*
    - Focused on key executives within an organization or other key leaders, executives, and managers in the company

- *Tailgating*
  - Entering a secure portion of the organization's building by following an authorized person into the area without their knowledge or consent
- *Piggybacking*
  - Similar to tailgating, but occurs with the employee's knowledge or consent
- *Shoulder Surfing*
  - Coming up behind an employee and trying to use direct observation to obtain information
- *Dumpster Diving*
  - Scavenging for personal or confidential information in garbage or recycling containers

- **Insider Threat**
  - An employee or other trusted insider who uses their authorized network access in unauthorized ways to harm the company

- **Logic Bomb**
  - A specific type of malware that is tied to either a logical event or a specific time

Security Technologies

Objectives:

- 1.5 - Explain common ports and protocols, their application, and encrypted alternatives
- 2.1 - Compare and contrast various devices, their features, and their appropriate placement on the network
- 3.1 - Given a scenario, use the appropriate statistics and sensors to ensure network availability
- 4.1 - Explain common security concepts
- 4.3 - Given a scenario, apply network hardening techniques
- 4.4 - Compare and contrast remote access methods and security implications

- **Firewall**
    - Uses a set of rules defining the traffic types permitted or denied through device
        - Software or hardware
        - Virtual or physical
        - Host-based or network-based
        - Can perform Network Address Translation (NAT) and/or Port Address Translation (PAT)
    - *Stateful Firewall*
        - Inspects traffic as part of a session and recognizes where the traffic originated
    - *NextGen Firewall (NGFW)*
        - Third-generation firewall that conducts deep packet inspection and packet filtering

- *Access Control List (ACL)*
  - Set of rules applied to router interfaces that permit or deny certain traffic
    - Switch
      - MAC address
    - Router
      - IP address
    - Switch Firewall
      - IP address or port
        - Source/destination IP
        - Source/destination port
        - Source/destination MAC
- *Firewall Zone*
  - Firewall interface in which you can set up rules
    - Inside
      - Connects to corporate LAN
    - Outside
      - Connects to the Internet
    - Demilitarized Zone (DMZ)
      - Connects to devices that should have restricted access from the outside zone (like web servers)
- *Unified Threat Management (UTM) Device*
  - Combines firewall, router, intrusion detection/prevention system, anti-malware, and other features into a single device

- **IDS and IPS**
  - *Signature-based Detection*
    - Signature contains strings of bytes (a pattern) that triggers detection
  - *Policy-based Detection*
    - Relies on specific declaration of the security policy
  - *Statistical Anomaly-based Detection*
    - Watches traffic patterns to build baseline
  - *Non-statistical Anomaly-based Detection*
    - Administrator defines the patterns/baseline
      - *Network-based (NIDS/NIPS)*
        - A network device protects entire network
      - *Host-based (HIDS/HIPS)*
        - Software-based and installed on servers and clients
    - Network and host-based systems can work together for a more complete protection

- **Remote Access**
  - *Telnet Port 23*
    - Sends text-based commands to remote devices and is a very old networking protocol
    - Telnet should never be used to connect to secure devices
  - *Secure Shell (SSH) Port 22*
    - Encrypts everything that is being sent and received between the client and the server

- *Remote Desktop Protocol (RDP) Port 3389*
  - Provides graphical interface to connect to another computer over a network connection
- *Remote Desktop Gateway (RDG)*
  - Provides a secure connection using the SSL/TLS protocols to the server via RDP
    - Create an encrypted connection
    - Control access to network resources based on permissions and group roles
    - Maintain and enforce authorization policies
    - Monitor the status of the gateway and any RDP connections passing through the gateway
- *Virtual Private Network (VPN)*
  - Establishes a secure connection between a client and a server over an untrusted public network like the Internet
- *Virtual Network Computing (VNC) Port 5900*
  - Designed for thin client architectures and things like Virtual Desktop Infrastructure (VDI)
- *Virtual Desktop Infrastructure (VDI)*
  - Hosts a desktop environment on a centralized server
  - Desktop as a Service (DaaS)
- *In-Band Management*
  - Managing devices using Telnet or SSH protocols over the network
- *Out-of-Band Management*
  - Connecting to and configuring different network devices using an alternate path or management network

        - Prevents a regular user's machine from connecting to the management interfaces of your devices
        - Out-of-band networks add additional costs to the organization
    - *Authentication*
        - Confirms and validates a user's identity
        - Gives the user proper permissions to access a resource
    - *Password Authentication Protocol (PAP)*
        - Sends usernames and passwords in plain text for authentication
    - *Challenge Handshake Authentication Protocol (CHAP)*
        - Sends the client a string of random text called a challenge which is then encrypted using a password and sent back to the server
    - *MS-CHAP*
        - Microsoft proprietary version that provides stronger encryption keys and mutual authentication
    - *Extensible Authentication Protocol (EAP)*
        - Allows for more secure authentication methods to be used instead of just a username and a password
        - Use EAP/TLS in conjunction with a RADIUS or TACACS+ server

- **Virtual Private Networks (VPNs)**
    - Extends a private network across a public network and enables sending and receiving data across shared or public networks
        - Site to site
        - Client to site
        - Clientless

- *Full Tunnel VPN*
  - Routes and encrypts all network requests through the VPN connection back to the headquarters
- *Split Tunnel VPN*
  - Routes and encrypts only the traffic bound for the headquarters over the VPN, and sends the rest of the traffic to the regular Internet
    - For best security, use a full tunnel
    - For best performance, use a split tunnel
- *Clientless VPN*
  - Creates a secure, remote-access VPN tunnel using a web browser without requiring a software or hardware client
- *Secure Socket Layer (SSL)*
  - Provides cryptography and reliability using the upper layers of the OSI model, specifically Layers 5, 6, and 7
- *Transport Layer Security (TLS)*
  - Provides secure web browsing over HTTPS
  - SSL and TLS use TCP to establish their secure connections between a client and a server
- *Datagram Transport Layer Security (DTLS)*
  - UDP-based version of the TLS protocol which operates a bit faster due to having less overhead
- *Layer 2 Tunneling Protocol (L2TP)*
  - Lacks security features like encryption by default and needs to be combined with an extra encryption layer for protection

- *Layer 2 Forwarding (L2F)*
  - Provides a tunneling protocol for the P2P protocol but also lacks native security and encryption features
- *Point-to-Point Tunneling Protocol (PPTP)*
  - Supports dial-up networks but also lacks native security features except when used with Microsoft Windows
- *IP Security (IPSec)*
  - Provides authentication and encryption of packets to create a secure encrypted communication path between two computers

- **IP Security (IPSec)**
  - Provides authentication and encryption of data packets to create an secure encrypted communication path between two computers
    - Confidentiality
      - Using data encryption
    - Integrity
      - Ensuring data is not modified in transit
    - Authentication
      - Verifying parties are who they claim to be
    - Anti-Replay
      - Checking sequence numbers on all packets prior to transmission
        - Key exchange request
        - IKE Phase 1
        - IKE Phase 2
        - Data transfer
        - Tunnel termination

- *Main Mode*
  - Conducts three two-way exchanges between the peers, from the initiator to the receiver
    - *First Exchange*
      - Agrees upon which algorithms and hashes will be used to secure the IKE communications throughout the process
    - *Second Exchange*
      - Uses a Diffie-Hellman exchange to generate shared secret keying material so that the two parties can prove their identities
    - *Third Exchange*
      - Verifies the identity of the other side by looking at an encrypted form of the other peer's IP address
- Authentication methods used
  - Encryption and hash algorithms used
  - Diffie-Hellman groups used
  - Expiration of the IKE SA
  - Shared secret key values for the encryption algorithms
- *Aggressive Mode*
  - Uses fewer exchanges, resulting in fewer packets and faster initial connection than main mode
    - Diffie-Hellman public key
    - Signed random number
    - Identity packet
    - Negotiate the IPSec SA parameters protected by an existing IKE SA
    - Establish IPSec SA

- Periodically renegotiate IPSec SAs to maintain security
- Perform additional Diffie-Hellman exchanges, if needed

- *Quick Mode*
  - Only occurs after IKE already established the secure tunnel in Phase 1 using either main or aggressive mode
- *Diffie-Hellman Key Exchange*
  - Allows two systems that don't know each other to be able to exchange keys and trust each other
    - PC1 sends traffic to PC2 and then RTR1 initiates creation of IPSec tunnel
    - RTR1 and RTR2 negotiate Security Association (SA) to form IKE Phase 1 tunnel (ISAKMP tunnel)
    - IKE Phase 2 tunnel (IPSec tunnel) is negotiated and set up
    - Tunnel is established and information is securely sent between PC1 and PC2
    - IPSec tunnel is torn down and the IPSec SA is deleted
- *Transport Mode*
  - Uses packet's original IP header and used for client-to-site VPNs
  - By default, maximum transmission unit (MTU) size in most networks is 1500 bytes
- *Tunneling Mode*
  - Encapsulates the entire packet and puts another header on top of it
  - For site-to-site VPNs, you may need to allow jumbo frames
    - Transport
      - Client to site

        - Tunneling
            - Site to site
    - *Authentication Header (AH)*
        - Provides connectionless data integrity and data origin authentication for IP datagrams and provides protection against replay attacks
    - *Encapsulating Security Payload (ESP)*
        - Provides authentication, integrity, replay protection, and data confidentiality
        - In transport mode, use AH to provide integrity for the TCP header and ESP to encrypt it
        - In tunneling mode, use AH and ESP to provide integrity and encryption of the end payload

- **Simple Network Management Protocol (SNMP)**
    - *Managed Device*
        - Any device that can communicate with an SNMP manager known as the management information base (MIB)
    - *Simple Network Management Protocol (SNMP)*
        - Used to send and receive data from managed devices back to a centralized network management station
    - *Granular*
        - Sent trap messages get a unique objective identifier to distinguish each message as a unique message being received
    - *Management Information Base (MIB)*
        - The structure of the management data of a device subsystem using a hierarchical namespace containing object identifiers

- *Verbose*
  - SNMP traps may be configured to contain all the information about a given alert or event as a payload
- SNMPv1 and SNMPv2
  - Use a community string to give them access to the device as their security mechanism
  - Default community strings of public (read-only) or private (read-write) devices are considered a security risk
- *SNMPv3*
  - Provides three security enhancements which added integrity, authentication, and confidentiality to the SNMP protocol
    - Integrity
      - Message hashing
    - Authentication
      - Source validation
    - PoE+ 802.3at Confidentiality
      - DES 56-bit encryption

- **Network Logging**
  - *System Logging Protocol (Syslog)*
    - Sends system log or event messages to a central server, called a syslog server
      - Security Information Management (SIM)
      - Security Event Management (SEM)
      - Security Information and Event Management (SIEM)

- *Client*
  - Device sending the log information to the syslog server
- *Server*
  - Receives and stores the logs from all of the clients

Level	Condition	Indication
0	Emergency	The system has become unstable
1	Alert	A condition should be corrected immediately
2	Critical	A failure in the system's primary application requires immediate attention
3	Error	Something is preventing proper system function
4	Warning	An error will occur if action is not taken soon
5	Notice	The events are unusual
6	Information	Normal operational message that requires no action
7	Debugging	Useful information for developers

- *Traffic Log*
  - Contains information about the traffic flows on the network
  - Traffic logs allow for investigation of any abnormalities
- *Audit Log/ Audit Trail*
  - Contains a sequence of events for a particular activity
- *Application Log*
  - Contains information about software running on a client or server
    - Informational
    - Warning
    - Error

- *Security Log*
  - Contains information about the security of a client or server
- *System Log*
  - Contains information about the operating system itself

- **Security Information and Event Management (SIEM)**
  - Provides real-time or near-real-time analysis of security alerts generated by network hardware and applications
  - Gathers logs and data from all sorts of different systems
    - *Log Collection*
      - Provides important forensic tools and helps address compliance reporting requirements
    - *Normalization*
      - Maps log messages into a common data model, enabling the organization to connect and analyze related events
    - *Correlation*
      - Links the logs and events from different systems or applications into a single data feed
    - *Aggregation*
      - Reduces the volume of event data by consolidating duplicate event records and merging them into a single record
    - *Reporting*
      - Presents the correlated, aggregated event data in real-time monitoring dashboards for analysts or long-term summaries for management
        - Software

        - Hardware
        - Managed service
- Log all relevant events and filter out anything that is considered to be irrelevant data
- Establish and document the scope of the events
- Develop use cases to define a threat
- Plan incident responses for given scenarios or events
- Establish a ticketing process to track all the flagged events
- Schedule regular threat hunting with cybersecurity analysts
- Provide auditors and analysts an evidence trail
- Syslog protocol using UDP Port 514 or TCP Port 1468

Network Hardening

Objective 4.3: Given a scenario, apply network hardening techniques

- **Hardening**
  - Securing a system by reducing its surface of vulnerabilities
  - Healthy balance between operations and security

- **Patch Management**
  - Involves planning, testing, implementing, and auditing of software patches
    - Provides security
    - Increases uptime
    - Ensures compliance
    - Improves features
  - Ensure patches don't create new problems once installed
    - *Planning*
      - Tracks available patches and updates and determines how to test and deploy each patch
    - *Testing*
      - Tests any patch received from a manufacturer prior to automating its deployment through the network
      - Have a small test network, lab, or machine for testing new patches before deployment
    - *Implementing/Implementation*
      - Deploys the patch to all of the workstations and servers that require it

- Disable the Windows Update service from running automatically on the workstation
- Also implement patching through a mobile device manager (MDM), if needed

  - *Auditing*
    - Scans the network and determines if the patch was installed properly and if there are any unexpected failures that may have occurred
    - Also conduct firmware management for your network devices

- **Password Security**
  - *Password Policy*
    - Specifies minimum password length, complexity, periodic changes, and limits on password reuse
  - *Strong Password*
    - Sufficiently long and complex which creates lots of possible combinations for brute force attacks to be completed in time
      - Long vs Complex
      - Passwords should be up to 64 ASCII characters long
      - Password aging policies should not be enforced
      - Change default passwords

- **Unneeded Services**
  - A service is an application that runs in the background of an operating system or device to perform a specific function
    - Disable any services that are not needed for business operations

- *Least Functionality*
  - Process of configuring a device, a server, or a workstation to only provide essential services required by the user
    - AutoSecure CLI command can be used on Cisco devices

- **Port Security and VLANs**
  - *Port Security*
    - Prevents unauthorized access to a switchport by identifying and limiting the MAC addresses of the hosts that are allowed
  - *Static Configuration*
    - Allows an administrator to define the static MAC addresses to use on a given switchport
  - *Dynamic Learning*
    - Defines a maximum number of MAC addresses for a port and blocks new devices that are not on the learned list
  - *Private VLAN (Port Isolation)*
    - A technique where a VLAN contains switch ports that are restricted to using a single uplink
      - Primary
      - Secondary isolated
      - Secondary community
  - *Primary VLAN*
    - Forwards frames downstream to all of the secondary VLANs
  - *Isolated VLAN*
    - Includes switch ports that can reach the primary VLAN but not other secondary VLANs

- *Community VLAN*
  - Includes switch ports that can communicate with each other and the primary VLAN but not other secondary VLANs
    - *Promiscuous Port (P-Port)*
      - Can communicate with anything connected to the primary or secondary VLANs
        - Host Ports
        - Isolated Ports (I-Port)
        - Community Ports (C-Port) df
    - *Isolated Port (I-Port)*
      - Can communicate upwards to a P-Port and cannot talk with other I-Ports
    - *Community Port (C-Port)*
      - Can communicate with P-Ports and other C-Ports on the same community VLAN
  - Default VLAN is known as VLAN 1
- *Native VLAN*
  - VLAN where untagged traffic is put once it is received on a trunk port

- **Inspection and Policing**
  - *Dynamic ARP Inspection (DAI)*
    - Validates the Address Resolution Protocol (ARP) packets in your network
    - Ensures only valid ARP requests and responses are relayed across the network device
    - Invalid ARP packets are dropped and not forwarded

- *DHCP Snooping*
  - Provides security by inspecting DHCP traffic, filtering untrusted DHCP messages, and building and maintaining a DHCP snooping binding table
- *Untrusted Interface*
  - Any interface that is configured to receive messages from outside the network or firewall
- *Trusted Interface*
  - Any interface that is configured to receive messages only from within the network
  - Configure switches and VLANs to allow DHCP snooping
- *IPv6 Router Advertisement Guard (RA-Guard)*
  - Mitigates attack vectors based on forged ICMPv6 router advertisement messages
  - Operates at Layer 2 of the OSI model for IPv6 networks to specify which interfaces are not allows to have router advertisements on
- *Control Plane Policing (CPP)*
  - Configures a QoS filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches
    - Data plane
    - Management plane
    - Control plane
    - Service plane
- *Control Plane Policing (CPP)*
  - Configures a QoS filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches

- **Securing SNMP**
    - *SNMP*
        - Allows us to easily gather information from our various network devices back to a centralized management server
        - Community strings grant access to portions of the device management planes
            - Ensure you are NOT using SNMP v1 or SNMP v2
                - SNMP v3 uses encoded parameters to provide its authentication as a part of the SNMP architecture
            - Combine with whitelisting of the Management Information Base (MIB)
            - Use authPriv on your devices
            - Ensure all SNMP administrative credentials have strong passwords
            - Follow the principles of least privilege
                - Role separation between polling/receiving traps (for reading)
            - Configuring users or groups (for writing)
            - Apply and extend access control lists to block unauthorized access
            - Keep system images and software up-to-date
            - Segregate SNMP traffic onto a separate management network

- **Access Control List (ACL)**
    - A list of permissions associated with a given system or network resource
        - Block SSH for a single computer based on its IP address
        - Block any IP using port 110
        - Block any IP and any port from outside the LAN

        - Block incoming requests from private loopback and multicast IP ranges
        - Block incoming requests from protocols that should only be used locally
        - Block all IPv6 traffic or allow it to only authorized hosts and ports
    - *Explicit Deny*
        - Blocks matching traffic
    - *Implicit Deny*
        - Blocks traffic to anything not explicitly specified
    - *Role-Based Access*
        - Defines the privileges and responsibilities of administrative users who control firewalls and their ACLs

- **Wireless Security**
    - *MAC Filtering*
        - Defines a list of devices and only allows those on your Wi-Fi network
            - Explicit allow
            - Implicit allow
            - Always use explicit allow
            - Don’t rely on it as your only wireless network protection
    - *Wireless Client Isolation*
        - Prevents wireless clients from communicating with one another
        - Wireless access points begin to operate like a switch using private VLANs
    - *Guest Network Isolation*
        - Keeps guests away from your internal network communications
    - *Pre-Shared Key (PSK)*
        - Secures wireless networks, including those protected with WEP, WPA, WPA2, and WPA3

        - Ensure you choose a long and strong password
    - *Extensible Authentication Protocol (EAP)*
        - Acts as a framework and transport for other authentication protocols
    - *Geofencing*
        - A virtual fence created within a certain location
    - *Captive Portal*
        - A web page displayed to newly connected Wi-Fi users before being granted broader access to network resources

- **IoT Considerations**
    - Understand your endpoints
    - Track and manage your devices
    - Patch vulnerabilities
    - Conduct test and evaluation
    - Change defaults credentials
    - Use encryption protocols
    - Segment IoT devices

Network Availability

Objectives:

- 2.2 - Compare and contrast routing technologies and bandwidth management concepts
- 3.3 - Explain high availability and disaster recovery concepts and summarize which is the best solution

- **Network Availability**
    - Measure of how well a computer network can respond to connectivity and performance demands that are placed upon it

- **High Availability Networks**
    - *High Availability*
        - Availability is measured by uptime
        - Five nines of availability (99.999%)
        - Maximum of 5 minutes of downtime per year
            - *Availability*
                - Concerned with being up and operational
            - *Reliability*
                - Concerned with not dropping packets
            - *Mean Time to Repair (MTTR)*
                - Measures the average time it takes to repair a network device when it breaks
            - *Mean Time Between Failures (MTBF)*
                - Measures the average time between failures of a device

- Redundant Network with Single Points of Failure
    - Link Redundancy (Multiple connections between devices)
        - Internal Hardware Redundancy (Power supplies and NICs)
- Redundant Network with No Single Points of Failure
    - Link Redundancy (Multiple connections between devices)
        - Redundancy of Components (Switches and Routers)
- Hardware Redundancy
    - Takes many forms
    - Devices with two network interface cards (NICs), hard drives, or internal power supplies
    - Often found in strategic network devices
        - Routers, Switches, Firewalls, and Servers
        - Not often found in clients due to costs and administrative overhead involved in management
            - Active-Active
                - Multiple NICs are active at the same time
                - NICs have their own MAC address
                - Makes troubleshooting more complex
            - Active-Passive
                - One NIC is active at a time
                - Client appears to have a single MAC address
- Network Interface Card Teaming
    - Using a group of network interface cards for load balancing and failover on a server or other device
- Layer 3 Redundancy
    - Clients are configured with a default gateway (router)

- If the default gateway goes down, they cannot leave the subnet
- Layer 3 Redundancy occurs with virtual gateways
    - *Hot Standby Router Protocol (HSRP)*
        - Proprietary first-hop redundancy by Cisco
        - Allows for active router and standby router
        - Creates virtual router as the default gateway
    - *Virtual Router Redundancy Protocol (VRRP)*
        - IETP open-standard variant of HSRP
        - Allows for active router and standby router
        - Creates virtual router as the default gateway
    - *Gateway Load Balancing Protocol (GLBP)*
        - Proprietary first-hop redundancy by Cisco
        - Focuses on load balancing over redundancy
        - Allows for active router and standby router
        - Creates virtual router as the default gateway
    - *Link Aggregation Control Protocol (LACP)*
        - Achieves redundancy by having multiple links between devices
        - Load balancing occurs over multiple links
        - Multiple links appear as single logical link
- *Multipathing*
    - Creates more than one physical path between the server and its storage devices for better fault tolerance and performance

- **Designing Redundant Networks**
    - Design Considerations
        - Where will redundancy be used?
            - Module (or Parts) Redundancy
            - Chassis Redundancy
        - What software redundancy features are appropriate?
        - What protocol characteristics affect design requirements?
        - What redundancy features should be used to provide power to an infrastructure device?
        - What redundancy features should be used to maintain environmental conditions?
    - Best Practices
        - Examine the technical goals
        - Identify the budget to fund high availability features
        - Categorize business applications into profiles
            - Each requires a certain level of availability
        - Establish performance standards for high-availability solutions
            - Performance standards will drive how success is measured
        - Define how to manage and measure the high-availability solution
            - Metrics help quantify success to decision makers
    - <u>Remember</u>
        - Existing networks can be retrofitted, but it reduces the cost by integrating high availability practices and technologies into your initial designs

- **Recovery Sites**
  - *Cold Sites*
    - An available building that does not have any hardware or software in place or configured
    - While recovery is possible, it is going to be slow and time-consuming
  - *Warm Sites*
    - An available building that already contains a lot of the equipment
    - Restoral time is between 24 hours and seven days
  - *Hot Sites*
    - An available building that already has the equipment and data in place and configured
    - Minimal downtime and with nearly identical service levels maintained
  - *Cloud Site*
    - Allows for the creation of a recovery version of an organization's enterprise network in the cloud
      - *Recovery Time Objective (RTO)*
        - Time and service level within which a business process must be restored after a disaster to avoid unacceptable consequences
        - How much time did it
          take to recover after the notification of a business process disruption?
        - Use either a hot site or a cloud site for low RTO situations

        - *Recovery Point Objective (RPO)*
            - Interval of time during a disruption before data lost exceeds the BCP's maximum allowable threshold or tolerance
    - Backup and Recovery
        - *Full*
            - Complete backup is the safest and most comprehensive; Time consuming and costly
        - *Incremental*
            - Backup only data changed since last backup
        - *Differential*
            - Only backups data since the last full backup
        - *Snapshots*
            - Read-only copy of data frozen in time (VMs)

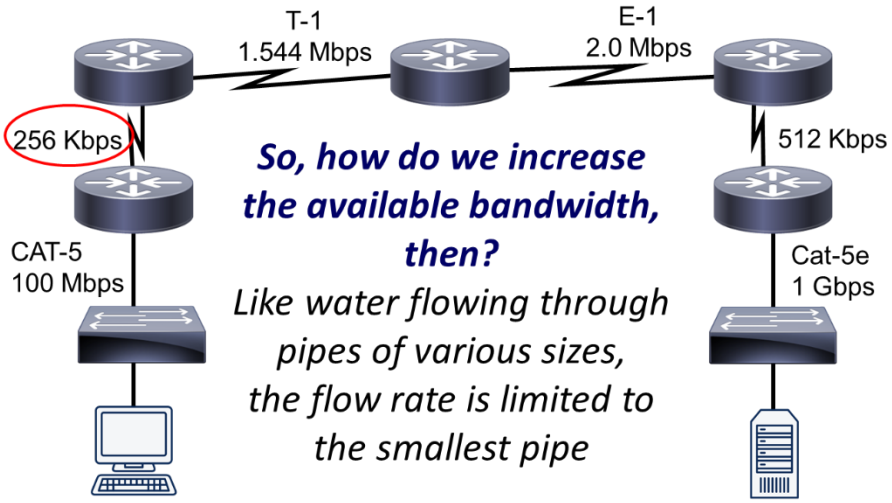
- **Facilities Support**
    - *Uninterruptible Power Supply (UPS)*
        - Provides emergency power to a load when the input power source or main power fails
        - Great for short duration power outages (less than 15 minutes)
    - *Power Distribution Unit (PDU)*
        - Distributes electric power, especially to racks of computers and networking equipment located within a data center
        - PDUs combined with a UPS or a generator can provide power during a blackout

- *Generator*
  - Provides long-term power during a power outage in a region
    - Takes a while to start up
    - Hot and cold aisle concept
- *Wet Pipe System*
  - Using a sprinkler system and pipes that always contain water
- *Pre-Action System*
  - A detector actuation like a smoke detector and a sprinkler must be tripped prior to water being released

- **Quality of Service (QoS)**
  - Need for Quality of Service (QoS)
    - Networks carry data, voice, and video content
    - Convergence of media on the network requires high availability to ensure proper delivery
    - Optimizing the network to efficiently utilize the bandwidth to deliver useful solutions to network users is crucial to success and cost savings
  - *Quality of Service (QoS)*
    - Enables strategic optimization of network performance for different types of traffic
      - Identifies types of traffic needing priority
      - Determines how much bandwidth required
      - Efficiently uses WAN link's bandwidth
      - Identifies types of traffic to drop during network congestion

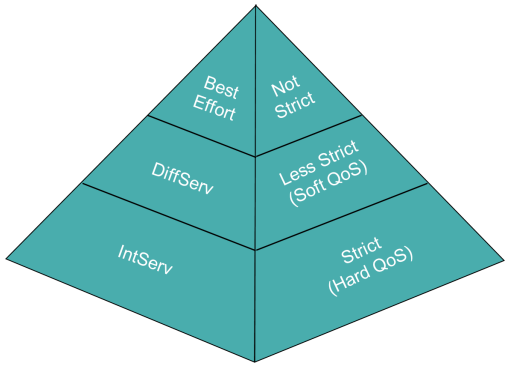
- For example
  - Voice (VoIP) and Video should have higher priority levels (less latency)

- Categories of QoS
  - *Delay*
    - Time a packet travels from source to destination
    - Measured in milliseconds (ms)
  - *Jitter*
    - Uneven arrival of packets
    - Especially harmful in VoIP
  - *Drops*
    - Occurs during link congestion
    - Router's interface queue overflows and causes packet loss
- "Effective" Bandwidth



- **QoS Categorization**
    - Purpose of QoS
        - To categorize traffic, apply a policy to those traffic categories, and prioritize them in accordance with a QoS policy
    - Categorization of Traffic
        - Determine network performance requirements for various traffic types (Voice, Video, Data)
        - Categorize traffic into specific categories:
            - Low delay
                - Voice
                - Streaming Video
            - Low priority
                - Web browsing
                - Non-mission critical data
        - Document your QoS policy and make it available to your users

- Ways of Categorizing Traffic



  - Best Effort
    - Does not truly provide QoS to that traffic
    - No reordering of packets
    - Uses FIFO (first in, first out) queuing
  - Integrated Services (IntServ or Hard QoS)
    - Makes strict bandwidth reservations
    - Reserves bandwidth by signaling devices
  - Differentiated Services (DiffServ or Soft QoS)
    - Differentiates between multiple traffic flows
    - Packets are “marked”
    - Routers and switches make decisions based on those markings
- Methods of Categorizing Traffic
  - Classification
  - Marking
  - Congestion management
  - Congestion avoidance
  - Policing and shaping
  - Link efficiency

- **QoS Mechanisms**
    - Ways of Categorizing Traffic
        - Classification
        - Marking
        - Congestion management
        - Congestion avoidance
        - Policing and shaping
        - Link efficiency
    - Classification of Traffic
        - Traffic is placed into different categories
        - For example, the E-mail class might contain various types of traffic
            - POP3
            - IMAP
            - SMTP
            - Exchange
        - Classification does not alter any bits in the frame or packet
    - Marking of Traffic
        - Altered bits within a frame, cell, or packet indicates handling of traffic
        - Network tools make decisions based on markings
    - Congestion Management
        - When a device receives traffic faster than it can be transmitted, it buffers the extra traffic until bandwidth becomes available
            - Called queuing
        - Queuing algorithm empties the packets in specified sequence and amount

- Queuing algorithms types
  - Weighted fair queuing
  - Low-latency queuing
  - Weighted round-robin

- Congestion Avoidance
  - Newly arriving packets would be discarded if the device's output queue fills to capacity
  - Random Early Detection (RED) is used to prevent this from occurring
    - As the queue fills, the possibility of a discard increases until it reaches 100%
    - If at 100%, all traffic of that type is dropped
    - RED instead drops packets from selected queues based on defined limits
  - If TCP traffic, it will be retransmitted
  - If UDP, it will simply be dropped
- Policing and Shaping
  - *Policing*
    - Typically discards packets that exceed a configured rate limit (speed limit)
    - Dropped packets result in retransmissions
    - Recommended for higher-speed interfaces
  - *Shaping*
    - Buffers (delays) traffic exceeding configured rate
    - Recommended for slower-speed interfaces

- Link Efficiency: Compression
  - Packet payload is compressed to conserve bandwidth
  - VoIP payload can be reduced by 50%
    - Payload size from 40 bytes to 20 bytes
  - VoIP header can be reduced by 90-95%
    - Uses RTP header compression (cRTP)
    - Header size goes from 40 bytes to 2 to 4 bytes
  - Utilized on slower-speed links to make most of limited bandwidth
- Link Efficiency: LFI
  - Link Fragmentation & Interleaving (LFI)
  - Fragments large data packets and interleaves smaller data packets between the fragments
  - Utilized on slower-speed links to make the most of limited bandwidth

Network Policies

Objective 3.2: Explain the purpose of organizational documents and policies

- **IT Governance**
  - Used to provide a comprehensive security management framework for the organization
    - Policies
    - Standards
    - Baselines
    - Guidelines
    - Procedures

- **Policy**
  - Defines the role of security inside of an organization and establishes the desired end state for that security program
    - Organizational
    - System-specific
    - Issue-specific

- **Organizational**
  - Provides framework to meet the business goals and define the roles, responsibilities, and terms associated with it

- **System-specific**
    - Addresses the security of a specific technology, application, network, or computer system

- **Issue-specific**
    - Addresses a specific security issue such as email privacy, employee termination procedures, or other specific issues

- **Standard**
    - Implements a policy in an organization

- **Baseline**
    - Creates a reference point in network architecture and design

- **Guideline**
    - Recommended action that allows for exceptions and allowances in unique situations

- **Procedure**
    - Detailed step-by-step instructions created to ensure personnel can perform a given task or series of actions

- **Plans and Procedures**
    - *Change Management*
        - Structured way of changing the state of a computer system, network, or IT procedure

- Make sure the risks are considered prior to implementing a system or network change
  - Planned
  - Approved
  - Documented

- *Incident Response Plan*
  - Contains instructions to help network and system administrators detect, respond to, and recover from network security incidents
    - Preparation
    - Identification
    - Containment
    - Eradication
    - Recovery
    - Lessons learned
- *Disaster Recovery Plan*
  - Documents how an organization can quickly resume work after an unplanned incident
    - *Business Continuity Plan*
      - Outlines how a business will continue operating during an unplanned disruption in service
      - A disaster recovery plan will be referenced from a business continuity plan
    - *System Life Cycle Plan*
      - Describes the approach to maintaining an asset from creation to disposal

- *Planning*
    - Involves the planning and requirement analysis for a given system, including architecture outlining and risk identification
- *Design*
    - Outlines new system, including possible interconnections, technologies to use, and how it should be implemented
- *Transition*
    - Actual implementation, which could involve coding new software, installing the systems, and network cabling and configurations
- *Operations*
    - Includes the daily running of the assets, as well as updating, patching, and fixing any issues that may occur
- *Retirement*
    - End of the lifecycle and occurs when the system or network no longer has any useful life remaining in it

- *Standard Operating Procedure*
    - A set of step-by-step instructions compiled by an organization to help its employees carry out routine operations

- **Hardening and Security Policies**
  - *Password Policy*
    - A set of rules created to improve computer security by motivating users to create and properly store secure passwords
  - *Acceptable Use Policy (AUP)*
    - A set of rules that restricts the ways in which a network resource may be used and sets guidelines on how it should be used
  - *Bring Your Own Device (BYOD) Policy*
    - Allows employees to access enterprise networks and systems using their personal mobile devices
    - Create a segmented network where the BYOD devices can connect to
  - *Remote Access Policy*
    - A document which outlines and defines acceptable methods of remotely connecting to the internal network
  - *Onboarding Policy*
    - A documented policy that describes all the requirements for integrating a new hire into the company and its cultures
  - *Offboarding Policy*
    - A documented policy that covers all the steps to successfully part ways with an employee who's leaving the company
  - *Security Policy*
    - A document that outlines how to protect the organization's systems, networks, and data from threats
  - *Data Loss Prevention Policy*
    - A document defining how organizations can share and protect data
    - Data loss prevention policy minimizes accidental or malicious data loss

        - Set proper thresholds for your DLP policy

- **Common Agreements**
    - *Non-Disclosure Agreement (NDA)*
        - Defines what data is confidential and cannot be shared outside of that relationship
        - A non-disclosure agreement is an administrative control
            - Fines
            - Forfeiture of rights
            - Jail time
    - *Memorandum of Understanding (MOU)*
        - Non-binding agreement between two or more organizations to detail what common actions they intend to take
        - Often referred to as a letter of intent
        - Usually used internally between two business units
    - *Service-Level Agreement (SLA)*
        - Documents the quality, availability, and responsibilities agreed upon by a service provider and a client

Network Management

Objectives:

- 3.1 - Given a scenario, use the appropriate statistics and sensors to ensure network availability
- 3.2 - Explain the purpose of organizational documents and policies

- **Network Management**
  - The process of administering and managing computer networks

- **Common Documentation**
  - *Physical Network Diagram*
    - Shows the actual physical arrangement of the components that make up the network
  - *Logical Network Diagram*
    - Illustrates the flow of data across a network and shows how devices communicate with each other
  - *Wiring Diagram*
    - Labels which cables are connected to which ports
  - *Radio Frequency (Wireless) Site Survey*
    - Planning and designing a wireless network to deliver the required wireless solution
  - *Wired Site Survey*
    - Determines if a site has the right amount of power, space, and cooling to support a new upgrade or installation
  - *Audit and Assessment Report*
    - Delivered after a formal assessment has been conducted

- Audit and Assessment Report
    - Executive summary
    - Scope and objectives
    - Assumptions and limitations
    - Methods and tools
    - Environment and system diagram
    - Security requirements
    - Findings and recommendations
    - Audit results

- *Baseline Configurations*
    - Set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on
    - Changes will be properly tested and approved to be part of the new baseline

- **Performance Metrics**
    - *Network Performance Monitoring*
        - Monitors the performance from the end user's workstation to the final destination they are trying to reach
            - *Latency*
                - Time that it takes for data to reach its destination across a network
                - High latency slows down overall network performance
            - *Bandwidth*
                - Maximum rate of data transfer across a given network

- *Throughput*
  - Actual measure of how much data is successfully transferred from the source to a destination
- *Jitter*
  - When a time delay in the sending of data packets over a network connection occurs

■ Ensure that your network is using QoS properly

- **Sensors**
  - Monitors a device's temperature, CPU usage, and memory, which could indicate if it is operating properly or is about to fail
  - Minor Temperature Threshold
    - Used to set off an alarm when a rise in temperature is detected but hasn't reached dangerous levels yet
  - Major Temperature Threshold
    - Used to set off an alarm when temperature reaches dangerous conditions
      - 5-40% CPU utilization
        - Misconfigured network
        - Network under attack
          - Minor
          - Severe
          - Critical
      - 40%
        - Normal conditions
      - 60-70%
        - Busier times

        - Layer 3 80%
            - Peak times

- **NetFlow Data**
    - *Full Packet Capture*
        - Used to capture the entire packet, including the header and the payload for all traffic entering and leaving a network
    - *Flow Analysis*
        - Relies on a flow collector to record the metadata and statistics about network traffic rather than recording each frame
        - Highlights trends and patterns
    - *NetFlow*
        - Defines a particular traffic flow based on the different packets that share the same characteristics
            - Protocol interface
            - IP version/type
            - Source/destination IP
            - Source/destination port
            - IP service type
    - *Zeek*
        - Passively monitors a network like a sniffer, but only logs full packet capture data of potential interest
        - Performs normalization of the data and stores it as a tab-delimited or JSON-formatted text files

- *Multi Router Traffic Grapher (MRTG)*
  - Creates graphs showing traffic flows through the network interfaces of routers and switches by polling the appliances using SNMP

- **Interface Statistics**
  - *Link State*
    - Communicates whether a given interface has a cable connected to it and a valid protocol to use for communication
  - *Drop*
    - Used to count the number of packets that have been dropped
  - *Flush*
    - Used to count Selective Packet Discards (SPD) that have occurred
  - *Selective Packet Discards (SPD)*
    - Drops low priority packets when the CPU is too busy so it can save capacity for higher priority packets as a form of QoS
  - *Runt*
    - An Ethernet frame that is less than 64 bytes in size
  - *Giant*
    - Any Ethernet frame that exceeds the 802.3 frame size of 1518 bytes
  - *Throttle*
    - Occurs when the interface fails to buffer the incoming packets
  - *CRC*
    - Number of packets received that failed the cyclic redundancy checksum, or CRC check upon receipt

- *Frame*
  - Used to count the number of packets where a CRC error and a non-integer number of octets was received
- *Overrun*
  - Used to count how often the interface was unable to receive traffic due to an insufficient hardware buffer
- *Ignored*
  - Used to count the number of packets that the interface ignored since the hardware interface was low on internal buffers
- *Underrun*
  - Number of times the sender has operated faster than the router can handle, causing buffers or dropped packets
- *Babble*
  - Used to count any frames that are transmitted and are larger than 1518 bytes
- *Late Collision*
  - Used to count the number of collisions that occur after the interface has started transmitting its frame
- *Deferred*
  - Used to count the number of frames that were transmitted successfully after waiting because the media was busy
- *Output Buffer Failure*
  - Number of times a packet was not output from the output hold queue because of a shortage of shared memory
- *Output Buffer Swapped Out*
  - Number of packets stored in main memory when the queue is full

- **Environmental Sensors**
    - Environmental monitoring
        - Network devices operate between 50 and 90 ºF
        - Maintain a humidity range of 40-60%
            - Cool
            - At the right humidity
            - Receives clean power
            - Flood-free

Troubleshooting Physical Networks

Objectives:

- 5.1 - Explain the network troubleshooting methodology
- 5.2 - Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools

- **Network Troubleshooting Methodology**
    - Identify the problem
    - Establish a theory to determine the cause
    - Test the theory to determine the cause
    - Establish a plan of action to resolve the problem and identify potential effects
    - Implement the solution or escalate as necessary
    - Verify the whole system functionality and if applicable, implement preventive measures
    - Document findings, actions, outcomes, and lesson learned
        - Gather more details
        - Identify symptoms
        - Check for changes
        - Duplicate problem
    - How to implement the network troubleshooting methodology
        - Approach multiple problems individually
            - Top-to-bottom
            - Bottom-to-top
            - Divide and conquer
        - If confirmed, determine next steps
        - If unconfirmed, reestablish new theory or escalate

- **Cable Review**

CATEGORY	STANDARD	BANDWIDTH	DISTANCE
CAT 5	100BASE-TX	100 Mbps	100 meters
CAT 5e	1000BASE-T	1000 Mbps	100 meters
CAT 6	1000BASE-T/ 10GBASE-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

    - Coaxial
        - 100 Mbps, 500 meters
    - Coaxial Twinaxial
        - 10 Gbps, 5 meters
        - 100 Gbps, 7 meters

STANDARD	MODE	BANDWIDTH	DISTANCE
100BASE-FX	MMF	100 Mbps	2 kilometers
100BASE-SX	MMF	100 Mbps	300 meters
1000BASE-SX	MMF	1000 Mbps	220-550 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

- Protecting your network from electromagnetic interference (EMI)
  - The extra shielding helps protect the STP cables from EMI and power frequency interruptions
  - Fiber cables are immune to EMI
- *Plenum Cable*
  - Used when running cables horizontally in a building across a particular level
- *Riser Cable*
  - Used to run network cables vertically between floors in a building in a cable riser or elevator shaft
  - Riser cables cannot be used in plenum spaces since they are not made from PVC or FEP
    - *Rollover/Console Cable*
      - A type of null-modem cable that is used to connect a computer terminal to a router's console port

- *Crossover Cable*
  - Connects two Ethernet network devices directly, such as two computers without a switch or a router in between
- *Power Over Ethernet (or PoE)*
  - Passes electric power over twisted pair Ethernet cable to powered devices
  - PoE provides 15.4 to 60 watts of power using two twisted pairs, and between 60-100 watts of power using all four

- **Cabling Tools**
  - *Snips or Cutters*
    - Used to simply cut a piece of cable off a larger spool or run of cable
    - Looks a lot like a pair of scissors, but uses stronger blades to cut twisted copper cables, coaxial, cables, or even larger cable bundles
  - *Cable Strippers*
    - Strips the end of the cable to prepare it the attachment of a RJ-45 or other type of connector
  - *Cable Crimper*
    - Used to attach the connector to the end of the cable
    - support both RJ-45 and RJ-11 connectors
    - If you are working with coaxial cables, then you will need a cable crimper that supports an RG-6 or RG-59 connector
  - *Cable Tester*
    - Verifies continuity for each wire in the cable to ensure there are no breaks

- Verifies the pinouts of the connectors
- Different testers for different cable types

- *Multi-tester*
  - Supports not just ethernet cables using RJ-45, but also BNC connectors for coaxial cables, as well as IDE, PATA, SATA, RJ-45, fiber, DB25, DB9s and anything else that you might need to test
- *Wire Map Tool*
  - Like a cable tester, but it works specifically for twisted pair ethernet cables
  - It can diagnose any issues with that cable
    - *Open Pair*
      - Occurs when one or more of the conductors in the pair are not connected to a pin at one or the other end
    - *Short Pair*
      - Occurs when the conductors of a wire pair are connected to each other at any location in the cable
    - *Short Between Pairs*
      - Occurs when the conductors of two wires in different pairs are connected at any location in the cable
    - *Reversed Pair*
      - Occurs when the two wires in a single pair are connected to the opposite pins of the pair at the other end of the cable
    - *Crossed Pairs*
      - Occur when both wires of one color pair are connected to the pins of a different color pair at the opposite end

- *Split Pairs*
    - Occur when the wire from one pair is split away from the other and crosses over a wire in an adjacent pair

- *Cable Certifier*
    - Used with an existing cable to determine its Category or data throughput
- *Multimeter*
    - Checks the voltage or the amperage or the resistance of a copper cable
    - Used to verify if a cable is broken or not
    - Used to check coaxial cables to ensure there is no cuts or breaks in the middle of a patch cable, or test power sources or power cords
- *Punch-Down Tool*
    - Used to terminate wires on a punch-down block, stripping off the insulation
    - Used with 66 block or 110 block, network jacks, and patch panels
- *Toner Generator/Probe*
    - Allows technicians to generate a tone at one end of a connection and use the probe to audibly detect the wire pair connected to the tone generator
    - Often called a “Fox and Hound”
    - Fox is a tone generator
    - Hound is a toner probe
- *Loopback Adapter*
    - Connects transmit pins (or fibers) to receive pins (or fiber) to test a network interface
        - Ethernet Pinout
            - Pins 1 to 3 (Tx+ to Rx+)
            - Pins 2 to 6 (Tx- to Rx-)

- Fiber
    - Transmit fiber to Receive fiber
    - Used with diagnostic software to test Ethernet connectivity of a client

- *Time-domain Reflectometer (TDR)*
    - Locate breaks in a copper cable and provide an estimate of the severity and the distance to the break
        - Optical Time-domain Reflectometer (OTDR)
            - Used for fiber optic cables
- *Fiber Light Meter*
    - A device that provides a continuous wave of stable source of energy for attenuation measurements
- *Fusion Splicer*
    - A machine that is used to permanently join two fibers together
- *Tap*
    - A simple device that connects directly to the cabling infrastructure to split or copy packets for use in analysis, security, or general network management
- *Spectrum Analyzer*
    - A device that measures and displays signal amplitude (strength) as it varies by frequency within its frequency range (spectrum)

- **Cable Signal Issues**
    - *Attenuation*
        - Loss of signal strength on a network cable or connection over the length of the cable
        - Twisted pair cables can transmit data over a maximum distance of 100 meters
        - Coaxial cables can transmit data over a maximum distance of 500 meters
            - Frequency
            - Noise
            - Physical surroundings
        - The higher the frequency, the higher the bandwidth

CATEGORY	FREQUENCY
CAT 5e	100 MHz
CAT 6	250 Mhz
CAT 6a	500 MHz
CAT 7	600 MHz

        - Noise
            - Additional electrical or radio frequency noise in the areas where your network cables are operating
                - Use the proper cables for the physical environment you are operating in
                - Shorten the distance

        - Use an amplifier or repeater
    - Clean and polish both ends of fiber cable and connectors or switch to a cable with higher quality
- *Interference*
    - Occurs when multiple cables in the same frequency band are operating in close proximity to each other
    - Use high quality twisted pair cables or higher category rated cables
    - Plan cable runs to operate in parallel to any high power cables
- *Decibel (dB) Loss*
    - Measures the amount of signal deterioration we are experiencing on a given connection
        - Copper
            - decrease in voltage
        - Fiber
            - amount of lost light

- **Copper Cable Issues**
    - There are many types of issues that could occur within your copper cables
        - Incorrect pinouts
            - By default, the patch panel should use the TIA-568B pinout, with pins 1 through 8 being connected as:
                - White/Orange – Orange – White/Green – Blue – White/Blue – Green – White/Brown – Brown

        - Bad port
            - If you suspect a bad port on a switch or router, you should connect a loopback plug to the port on that device and run a test using specialized software
        - Open
            - There is nothing on the other end of the connection or there's a break in the wires between the source and the destination
        - Short
            - Indicates there are two wires are connected together somewhere in the connection

- **Fiber Cable Issues**
    - *Transceiver*
        - A transmitter and a receiver combined into a single device that converts a network connection from one type to another
        - They are designed to support a certain type of connection and a certain cable type
    - *Dry Cleaning*
        - Using light pressure while rubbing the end face of a fiber cable or connector with a dry-cleaning cloth in one direction
    - *Wet Cleaning*
        - Moistening a piece of lint-free cloth with a fiber optic cleaning solution and wiping the end face of the cable or connector

- **Ethernet Issues**
  - *Duplex Mismatch*
    - When one device thinks the connection is full duplex and the other thinks it is half duplex
    - Ensure both devices are configured to auto negotiate the connection properly

Troubleshooting Wireless Networks

Objective 5.4: Given a scenario, troubleshoot common wireless connectivity issues

- **Bandwidth**
  - Theoretical speed of data going across the network

- **Throughput**
  - Actual speed of data on the network

Network	Bandwidth	Throughput
802.11a	54 Mbps	20-30 Mbps
802.11b	11 Mbps	5-7 Mbps
802.11g	54 Mbps	30-32 Mbps
802.11n	600 Mbps	140-150 Mbps
802.11ac	1300 Mbps	100-500 Mbps
802.11ax	10 Gbps	600-900 Mbps

Network	Distance Indoors	Distance Outdoors
802.11a	35 meters	100 meters
802.11b		
802.11g		
802.11n	70 meters	250 meters
802.11ac	50 meters	100 meters
802.11ax		

  - *Received Signal Strength Indication (RSSI)*
    - Estimated measure of the power level that a radio frequency client device is receiving from a wireless access point or wireless router
  - *Effective Equivalent Isotropic Radiated Power (EIRP)*
    - Maximum power radiated from an ideal isotropic antenna, given its antenna gain, and the transmitter power of the radio frequency system
  - *Decibels over isotropic (dBi)*
    - Tells signal strength being radiated from a wireless access point

- **Wireless Considerations**
  - *Vertical Antenna*
    - Radio frequency waves extend outward in all directions away from the antenna and the wireless access point at an equal power level
  - *Dipole Antenna*
    - Produces radio frequency waves extending outward in two directions
  - *Yagi Antenna*
    - A unidirectional antenna that sends the radio frequency waves in only one direction
  - *Parabolic Grid Antenna*
    - Allows the radio waves to be transmitted in only one direction over a longer distance than a Yagi antenna
    - Choose a parabolic or Yagi antenna for site-to-site connections
    - For indoor use, you are more likely to use omnidirectional and unidirectional antennas
  - *Polarization*
    - The orientation of the electric field (or transmission) from the antenna
    - Most Wi-Fi networks use vertical polarization
  - *Channel Utilization*
    - A statistic or measure of the amount of airtime utilization that occurs for a particular frequency or channel
    - Keep channel utilization under 30% to have a faster wireless network
    - Access points and clients form a single broadcast domain when they operate on the same channel

- *Clear Channel Assessment (CCA)*
  - Listens to see if another device is actively transmitting on the channel before attempting to send frames on that channel
  - High channel utilization leads to slower throughput for wireless networks
- *Site Survey*
  - Process of planning and designing a wireless network to provide the required wireless solution
    - Configure devices to use less utilized channels
    - Ensure proper coverage of the entire work areas
    - Ensure wireless network is not being blocked or interfering with physical obstacles within the building
  - How does a site survey work?
    - Wireless client sends a probe request to discover any 802.11 wireless networks in proximity to itself
    - Receiving access point checks to see if it can support the data rate the client requested
    - Wireless client sends a low-level 802.11 authentication frame to the access point to begin authentication
    - Access point receives authentication frame and responds with an acknowledgement to continue the handshake
    - Wireless client chooses the access point it wants to associate with and sends an association request
    - Access point processes the association request if the information sent matches its capabilities
    - Client is fully connected and associated and can now conduct any data transfer it needs and use the wireless network

        - Basics steps
            - Scan airwaves
            - Find access points
            - Request association
            - Authenticate
            - Contact DHCP server
        - Clients should be located in high signal strength areas to speed up the association process

- **Coverage and Interference**
    - *Coverage*
        - A measure of how much area around a wireless transmitter is there sufficient signal strength for wireless devices to utilize
            - Client
            - RSSI (decibel)
            - Access Point
        - EIRP (dBi)
        - Signal booster
        - Larger antenna
        - Wireless repeater
        - Second access point
    - *Interference*
        - Occurs when multiple wireless networks communicate on the same channel using the same frequency
        - Use channels 1, 6, and 11 in the 2.4 GHz spectrum
        - Ensure a 10-15% overlap between access points for sufficient coverage

- *Attenuation*
  - Reduction of signal strength between the transmission and receipt of the signal
- *Multipath Reception*
  - Occurs when the transmitted signal bounces off walls and other physical objects and then is redirected to the receiver
    - Client Disassociation
      - *Idle Timeout*
        - Occurs when there's no traffic within 300 seconds
        - Send a keep alive packet every few minutes to remain connected
      - *Session Timeout*
        - Occurs when there's no traffic within 1800 seconds
      - *Wireless Network Change*
        - Occurs whenever the wireless local area network is changed
      - *Manual Deletion*
        - Occurs whenever a client is removed by an administrator
      - *Authentication Timeout*
        - Occurs when the authentication or key exchange process fails to finish in time
      - *Access Point Radio Reset*
        - Occurs when a change is made to the wireless network

- *Deauthentication Attack*
  - A common wireless attack used by hackers to disassociate wireless clients and make them attempt to reconnect to the access point

- **Incorrect Configurations**
  - Wrong SSID
    - *Service Set Identifier (SSID)*
      - Natural language name used to identify a wireless network in an 802.11 network
  - Incorrect passphrase
    - *Passphrase/Pre-Shared Key*
      - Used to encrypt and decrypt data sent and received by a wireless network
  - Encryption mismatch
    - Occurs when the client and the access point are using different encryption types
      - WEP – RC4
      - WPA – TKIP
      - WPA2 – AES
    - To fix this, attempt to reinstall the drivers for your wireless adapter
      - Change protocol type
      - Disable antivirus tools
      - Reinstall drivers

- **Captive Portal Issues**
  - *Captive Portal*
    - A web page displayed to newly-connected Wi-Fi users before being granted broader access to network resources
  - *HTTP Redirect*
    - Redirects all traffic to a web server which then redirects them to a captive portal using a 302 HTTP status code
  - *ICMP Redirect*
    - Sends error messages and operational information indicating the success or failure of communicating with another IP address
  - *DNS Redirect*
    - The client is redirected by the onboard DNS server to the captive portal webpage
      - Open a web browser and try to go to any website, such as Google.com or Facebook.com
      - If that doesn't work, determine your default gateway for the wireless network and enter http:// and the default gateway's IP address, then press enter
      - If that doesn't work, then verify your DNS server IPs are not set to something manually like 8.8.8.8, and instead allow DHCP to auto-configure your DNS server when connecting to the wireless network
        - Then, reattempt step 1, opening a web browser and going to any website again

Network Tools and the Command

Objective 5.3: Given a scenario, use the appropriate network software tools and commands

Software Tools		
Wi-Fi analyzers	Protocol analyzers and packets capturing	Bandwidth speed tests
Port scanners	iPerf	NetFlow analyzers
TFTP servers	Terminal emulators	IP scanners

Command Line Tools		
ping	ipconfig	ifconfig and ip
nslookup and dig	traceroute and tracert	arp
netstat	hostname	route
telnet	tcpdump	nmap

Basic Network Platform Commands
show interface
show config
show route

- **Software Tools**
  - *Wireless Analyzer*
    - Ensures you have the proper coverage and helps prevent overlap between wireless access point coverage zones and channels

- *Protocol Analyzer*
  - Used to capture and analyze signals and data traffic over a communication channel
- *Packet Capturing Tool*
  - Used to capture packets running over a network connection in real time and then save them for later analysis
    - Ethereal
    - Protocol expert
    - Netasyst
    - Network analyzer
    - Observer
    - LanHound
    - EtherPeek
    - tcpdump
    - WinDump
    - PRTG network monitor
    - SolarWinds
    - NetworkMiner
- *Bandwidth Speed Test*
  - Verifies the real-world throughput from a client device all the way out to the Internet and back
- *Port Scanner*
  - Determines which ports are open on a network
- *iPerf*
  - Gathers an active measurement of the maximum achievable bandwidth on an IP-based network

- *NetFlow Analyzer*
  - Performs monitoring, troubleshooting and in-depth inspection, interpretation, and synthesis of traffic flow data
- *Trivial File Transfer Protocol (TFTP)*
  - Protocol for exchanging files between two TCP/IP machines
- *TFTP Server*
  - Used for simple file transfers on a network and boot-loading of remote devices
- *Terminal Emulator*
  - Allows a host computer to access another computer through a command-line interface or a graphical one using either Telnet or SSH
  - Always use SSH instead of Telnet
    - Other terminal emulators:
      - Cmder
      - ZOC
      - Mintty
    - If you are working on a Linux client:
      - GNOME
      - Konsole
      - xterm
    - If you are working on an OS X client:
      - iTerm2
      - MacTerm
      - Kitty

- *IP Scanner*
  - Used to search for and detect IP addresses and other information related to devices on the network

- **Ping and Traceroute**
  - *Ping*
    - Used to check IP connectivity between two devices, most often for network troubleshooting
    - Similar to Windows version, except it runs forever by default (like –t in Windows)
  - *Traceroute/ Tracert*
    - Displays the path between your device (the source) and the destination IP address, showing each route hop along the path
  - *Hop*
    - Any router or firewall that is in the path of the transmission from the client to the destination
      - If cannot ping google.com
        - ping 8.8.8.8
      - If cannot ping 8.8.8.8
        - ping default gateway
      - If cannot ping default gateway
        - ping local client's IP address
      - If cannot ping local IP address
        - ping local host of 127.0.0.1

- **ipconfig, ifconfig, and ip**
  - *IP Configuration (ipconfig)*
    - Displays all of the current TCP/IP network configuration values and refreshes DHCP and DNS settings for a Windows client/server
  - *Interface Configuration (ifconfig)*
    - Command line tool used in Unix, Linux, and OS X systems to display IP address information
    - ifconfig is considered officially deprecated
  - *ip*
    - Assigns an address to a network interface or configures network interface parameters on a Unix, Linux, or OS X operating system

- **nslookup, dig, and hostname**
  - *Name Server Lookup (nslookup)*
    - Used to query the DNS to provide the mapping between domain names and IP addresses or other DNS records
    - In Windows, use set q=mx to search for mail exchange records
    - In Linux, use set type=mx to search for mail exchange records
  - *dig*
    - Used to conduct queries against DNS nameservers and is only available for Linux, Unix, and OS X systems by default
  - *hostname*
    - Used to display the hostname portion of the full computer name for a given system

- **arp, route, nbtstat, netstat**
  - *Address Resolution Protocol (ARP)*
    - Used to display and modify entries in the Address Resolution Protocol (or ARP) cache on a system
    - An ARP entry in the cache will get deleted after 21,600 seconds (6 hours)
      - arp -d
  - *route*
    - Used to view and manipulate the IP routing table in a Windows, Linux, Unix, or OS X system
  - *Default Route*
    - Route that takes effect when no other route is available for an IP destination address
  - *nbtstat*
    - Used to view the current connections and statistics for devices communicating using the NetBIOS over TCP/IP protocol
  - *Network Statistics (netstat)*
    - Displays information for IP-based connections on a client including its current sessions, its source and destination IPs, and port numbers

- **telnet, tcpdump, and nmap**
  - *telnet*
    - Provides a bidirectional interactive text-oriented communication facility using a virtual terminal connection
  - *tcpdump*
    - Allows for the display of TCP/IP and other packets being transmitted or received over a network to the client's screen

- *Network Mapper (nmap)*
  - Discovers hosts and services on a computer network by sending packets and analyzing the responses

- **Network Platform Commands**
  - *Network Platform*
    - Refers to any router, switch, or firewall, regardless of the brand or manufacturer
      - Cisco
        - show interface
      - Juniper
        - show interfaces
      - PoE+ 802.3at Sidewinder
        - cf interface
      - Cisco
        - show config
      - Juniper
        - show configuration
      - PoE+ 802.3at Sidewinder
        - cf config
      - Cisco
        - show route
      - Juniper
        - show route
      - PoE+ 802.3at Sidewinder
        - cf route status

- *show interface*
  - Displays statistics for the network interfaces on the device
- *show config*
  - Displays the current system configuration on the screen
- *show route*
  - Displays the current state of the routing table on the device

Troubleshooting Network Issues

Objective 5.5: Given a scenario, troubleshoot general networking issues

- **Troubleshooting Network Issues**
  - Startup Configuration
    - Stored in NVRAM and contains the commands needed to initially configure a router
  - Running Configuration
    - Actively being used by the router at that moment
  - *VLAN Assignment/Tagging*
    - Practice of segmenting an IT organization's network, separating users into respective network sections
    - VLAN Membership Policy Server (VMPS), client, server, and database
  - *Network Performance Baseline*
    - Defines the normal working conditions of an enterprise network infrastructure

- **Collisions and Broadcast Storms**
  - *Collision*
    - Occurs when two hosts on the network transmit at the same time which causes the signals to combine on the network medium
    - Collisions occur in both wired and wireless networks
  - *Collision Domain*
    - Network segment where simultaneous data transmissions collide with one another
    - Use any Layer 2 device to break apart collision domains
      - Turn off auto negotiation

- Hardcode lower speed
- Change to half-duplex

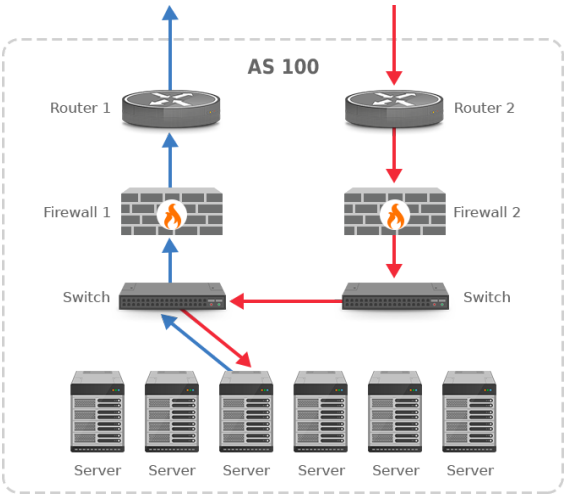
- *Broadcast Storm*
  - Occurs when a network system is overwhelmed by continuous multicast or broadcast traffic
    - Layer 2
      - FF:FF:FF:FF:FF:FF
    - Layer 3
      - 255.255.255.255
- *Broadcast Domain*
  - A logical division of computer network where all nodes can reach each other by broadcast at the data link layer
  - Layer 2 devices will not break up a broadcast domain
    - Too large singular broadcast domain
      - Use a router to break up subnets into separate broadcast domains
    - Large volume of DHCP requests
      - Discover
      - Offer
      - Request
      - Acknowledge
    - Loops are created in the switching environment
      - Enable Bridge Protocol Data Units (BPDU) on managed switches
      - Enforce a maximum number of MAC addresses per port

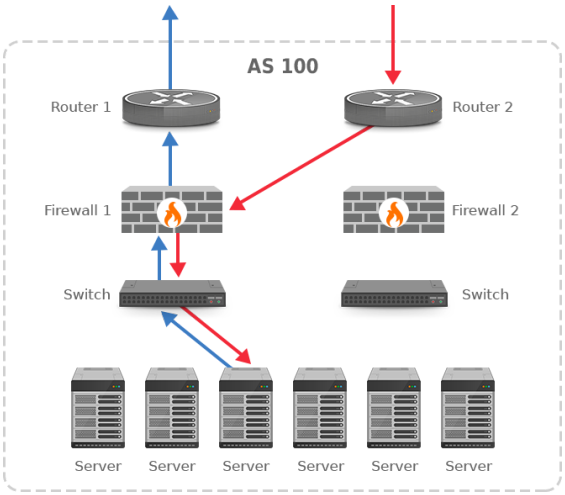
        - Break up large broadcast domains into smaller domains using routers and Layer 3 switches

- **Duplicate Addresses**
    - *MAC Address*
        - Used to uniquely identify a network interface card on a given network
            - D2:51:F1:3A:34:65
                - Vendor code: D2:51:F1
                - Unique Value: 3A:34:65
        - MAC addresses are only used in your Layer 2 networks
        - Logical Domain Manager
        - Listens to multicast messages on a network and keeps track of the MAC addresses being used
        - Enable port security on your switches
    - *Duplicate IP Address/ IP Address Conflict*
        - Occurs when another computer on the same network has an identical IP to another workstation or server on the same network
            - Static IP address issue
            - DHCP server issue
            - Rogue DHCP server

- **Routing Issues**
    - *Multicast Flooding*
        - No specific host is associated with the multicast MAC address in the CAM table of the switch

- *Asymmetrical Routing*
  - Network packets leave via one path and return via a different path
  - Routing issues cause issues with dropped packet flows





- Missing Routes
  - When a router cannot reach a destination because there is a missing route in the routing table

- **Loops**
  - *Switching/Bridge Loop*
    - Switching loops are usually an issue with how STP is configured
  - *Routing Loop*
    - Formed when an error occurs in the operation of the routing algorithm and creates a circular route amongst a group of network devices
    - Routing loops are caused by logical Layer 3 circular connections that may exist in a routing table
      - Time to Live (TTL)

- *Split Horizon*
  - Routing configuration that stops a route from being advertised back in the direction from which it came
    - ip split-horizon
    - no ip split-horizon
- *Route Poisoning*
  - Increasing a router's metric to an infinitely high number after detecting one of its connected routes has failed
- *Hold-Down Timer*
  - Prevents bad routes from being restored and passed to other routers by accident
    - Hold-down period
    - 180 seconds (3 minutes)
  - Statically-created routes are given a metric of 1 by default

- **DHCP Issues**
  - *Dynamic Host Configuration Protocol (DHCP)*
    - Automatically assigns an IP address, subnet mask, default gateway, and DNS server's IP address to a client when it joins a network
  - *Rogue DHCP Server*
    - A DHCP server on a network which is not under the administrative control of the network administrators
      - DHCP Snooping
      - Port Security
      - Intrusion Detection

- DHCP Scope Exhaustion
    - Occurs when the DHCP server runs out of valid IPs to assign to the clients requesting access on the network
        - 192.168.1.0/24
        - 192.168.1.1
        - 192.168.1.255
            - Default Lease Time
                - 1440 seconds (1 day)
                - 7 days
                - 30 days
            - Default Lease Time
                - 1440 seconds (1 day)
                - 7 days
                - 30 days
            - Default Lease Time
                - 1440 seconds (1 day)
                - 7 days
                - 30 days

- **IP and VLAN Settings**
    - Make sure you check your configuration and that there is proper routing setup between the VLANs, because this is the number one cause of issues when you're dealing with VLANs that won't communicate
        - *IP Address*
            - Occur when you have an incorrect IP address, subnet mask, gateway, or DNS server IP address assigned to a client

        - Subnet mask
        - Default gateway IP
        - DNS Server IP
            - Make sure you have a working DNS server and the IP is properly entered on the client

- **Firewall Issues**
    - *Firewall*
        - Network security device that monitors and filters incoming and outgoing network traffic based upon established rule sets
    - *Host-Based Firewall*
        - Runs on an individual computer or device connected to the network to protect that one device
    - *Network-Based Firewall*
        - Deployed in line with the network traffic flow to monitor and filter incoming and outgoing network traffic based on established rule sets
            - Access to protected resources from unprotected networks is not working
            - Access to unprotected resources from protected networks is not working
            - Access to the firewall and its configurations is not working
            - Access Control List (ACL)
        - Provides security by blocking unauthorized users and allowing authorized users to access specific resources

- **DNS and NTP Issues**
    - DNS
        - Matches domain names with the corresponding IP addresses used by a server
            - Issue on a single network client or on a larger network?
            - Connectivity between client and DNS server?
            - A records and CNAME records properly created?
                - **nslookup**
                    - Time to live (TTL) set correctly?
    - *DNS Latency*
        - Time and delay that occurs whenever users request a particular domain name
    - *NTP*
        - Allows synchronization of system clocks between different layers of a hierarchical, semi-layered system of time sources
            - Not received
            - Not processed
            - Errors or packet loss
        - Ensure network client is operating the NTP service
            - Network saturation
            - Network connectivity

- **Network Performance Issues**
  - High CPU usage
  - High bandwidth usage
  - Poor connectivity
  - Network malfunction

- **DNS problems**
  - High CPU usage increases latency, jitter, and packet loss
  - Use a cable tester for twisted pair connections or a fiber light meter for fiber optic connections

- **Other Issues**
  - Low optical link budgets
    - Optical Link Budget is a calculation that considers all the anticipated losses along the length of a fiber optic connection
      - Reduced transmission
      - Slow connection speeds
      - Connection downtime
        - 0.25 dB per km for a standard fiber optic cable
        - Calculate optical link budget by using power budget minus the loss over the fiber cable's distance
  - Certificate issues
    - A digital Certificate is used as a credential to facilitate verification of identities between users in a transaction
  - Licensed feature issues

- BYOD challenges
  - Bring Your Own Device (BYOD) policies allows a user to bring their own smartphones, laptops, and other devices to work and use them on the organization's network
    - Decrease in Capital Expenditures
    - Increase in Operational Expenditures
- Hardware failures