CompTIA Network+ (N10-009) Study Notes

Introduction

- **Introduction**
    - CompTIA Network+ Certification Exam
        - First networking certification for IT or cybersecurity entry
        - Foundation in configuring, managing, and troubleshooting network infrastructure
        - Designed for beginners with less than one year of IT experience or CompTIA A+ certified
        - Assumes knowledge from CompTIA A+ exams
    - Course Structure
        - Builds on hardware, software, and computer network basics
        - Emphasis on enterprise network configuration, management, and troubleshooting
        - Designed to be a full textbook replacement
            - Use official CompTIA Network+ student guide for additional resource

- ○ Exam Overview

  - ■ Five Domains

    - ● 23% – Networking Concepts

    - ● 20% – Network Implementation

    - ● 19% – Network Operations

    - ● 14% – Network Security

    - ● 24% – Network Troubleshooting

  - ■ Under each of domains are specific objectives provided in CompTIA Exam Objectives document

  - ■ Total of 90 minutes for up to 90 questions

    - ● Including multiple choice, multiple select, and performance-based questions with varying numbers of each

    - ● Scaled score of 720/900 needed to pass (75%)

    - ● Exam fee required, vouchers available for purchase

- ○ Study Approach

  - ■ Not covered in order of exam objectives for better learning flow

    - ● Start with basics, then move to physical infrastructure, switching, IP addressing, routing, network services, WAN connections, cloud, virtualization, security concepts and attacks, monitoring, automation, orchestration, documentation, processes, and disaster recovery, and troubleshooting concepts

  - ■ Specific objectives covered per section, mapped back to exam objectives

- - ■ Access to closed captions, variable speed playback, and downloadable study guide
  - ○ Tips for Success
    - ■ Use closed captions, adjust playback speed as needed
    - ■ Download and use the provided study guide for note-taking
    - ■ Join the Facebook group or Discord server for community support
    - ■ Utilize Q&A support for course-related questions
  - ○ Remember to utilize all available resources and practice exams to prepare thoroughly for the CompTIA Network+ Certification Exam

- **Exam Tips**
  - ○ Exam Questions
    - ■ Read each question multiple times to understand exactly what is being asked
    - ■ Look out for distractors or red herrings in the answer choices
  - ○ Keywords
    - ■ Pay close attention to words in questions that are bold, italicized, or in all uppercase, as they are deemed important
  - ○ Answer Selection
    - ■ Base your answers on CompTIA Network+ knowledge from the course or official textbook, not personal workplace experience

- - ■ Best Answer
      - ● Select the best answer, which is true most often or in the most cases, even if there are several potentially correct answers
  - ○ Key Concepts
    - ■ Understand the key concept the test writer is asking about in each question to help you choose the right answer
  - ○ Keyword Association
    - ■ Associate certain words with concepts
    - ■ Examples
      - ● Encryption for confidentiality
      - ● Hashing for integrity
      - ● Redundancy and resiliency for availability
  - ○ Term Recognition
    - ■ Recognize terms rather than memorizing them word for word, as there are no fill-in-the-blank questions on the exam
  - ○ Tool Knowledge
    - ■ Understand what tools are used for rather than knowing specific commands or syntax
  - ○ Question Types
    - ■ Expect multiple-choice or multiple-selection questions, plus a few performance-based questions (PBQs)

- ○ Vendor Neutrality

    - ■ Understand concepts in a vendor-neutral and generic context, not specific to any particular vendor or equipment

- ○ Exam Strategy

    - ■ Try to understand the key concept being asked, rather than fighting the exam or test questions

- ○ Study Plan

    - ■ Use a study plan to ensure you cover all material and have time for practice exams and review

- ○ Study Duration

    - ■ Aim to study intensively over a few weeks rather than spreading your study over several months, to retain information better

- ○ Certification Timeline

    - ■ Set a target date for earning your certification and plan your study schedule accordingly, focusing on completing sections daily

- **Our Lab Environment**

    - ○ Lab Environment

        - ■ Premium course experience at diontraining.com includes hands-on labs
            - ● Labs cover Windows desktops, servers, Linux servers, network infrastructure, and more

- ■ Labs designed, built, and operated by CompTIA, integrated into diontraining.com courses
- ■ CompTIA CertMaster Labs
  - ● Labs mirroring real-world tasks, enhancing understanding of course materials
  - ● Crucial for mastering performance-based questions (PBQs) on exams
- ○ Support Options
  - ■ Technical issues
    - ● Use the "Help" tab in the lab environment to contact CompTIA for support
  - ■ Conceptual or Instructional issues
    - ● Contact Dion Training support team via Discussions/Q&A tab or email
- ○ Lab Operation Tips
  - ■ Only one lab can run at a time
  - ■ Launch and exit labs properly to avoid issues
  - ■ Contact support promptly for a smoother learning experience
- ○ Labs are vital for certification and real-world readiness
- ○ Use labs for practice, confidence-building, and skill enhancement
- ○ CompTIA and Dion Training support teams are available for assistance

Network Fundamentals

Objectives:

- 1.2 - Compare and contrast networking appliances, applications, and functions
- 1.6 - Compare and contrast network topologies, architectures, and types
- 2.3 - Given a scenario, select and configure wireless devices and technologies

- **Introduction**
  - Network encompass a diverse range of connections extending to both wireless and wired networks

- **Network Components**
  - *Clients*
    - Devices that users use to access the network (e.g., workstations, laptops, tablets)
  - *Servers*
    - Provide resources to the network (e.g., email servers, file servers)
  - *Hubs*
    - Older technology connecting devices but not commonly used due to limitations
  - *Switches*
    - Smarter hubs that ensure security and efficient bandwidth utilization

- *Wireless Access Points (WAPs)*
    - Enable wireless devices to connect to a wired network using radio frequency waves
- *Routers*
    - Connect different networks, make intelligent forwarding decisions based on IP addresses
- *Firewalls*
    - Security barrier between internal network and the internet, monitor and control traffic
- *Load Balancers*
    - Distribute network/application traffic across servers, preventing bottlenecks
- *Proxy Servers*
    - Act as intermediaries between user devices and the internet, enhancing security and privacy
- *Intrusion Detection Systems (IDS)*
    - Detect unauthorized access or anomalies
- *Intrusion Prevention Systems (IPS)*
    - Detect and take action to prevent intrusion
- *Controllers*
    - Manage flow control in software-defined networking (SDN), offering flexibility and efficiency

- ○ *Network-attached Storage (NAS) Devices*
    - ■ Dedicated file storage systems providing data access to authorized clients
- ○ *Storage Area Networks (SANs)*
    - ■ High-speed networks for consolidated block-level data storage, enhancing accessibility
- ○ *Media*
    - ■ Physical materials for data transmission (e.g., copper cables, fiber optic cables)
- ○ *Wide Area Network (WAN) Links*
    - ■ Connect networks over large areas (e.g., between cities), essential for global connectivity
- ○ Key Takeaway
    - ■ Understanding these network components is crucial for efficient and secure data transmission in information technology, aiding in network design, management, problem-solving, and security implementation

- ● **Network Resources**
    - ○ *Client/Server Model*
        - ■ Utilizes a dedicated server for centralized access to files, scanners, printers, and resources
        - ■ Easy administration and backup due to a central server

- Benefits
  - Centralized administration
  - Easier management
  - Better scalability
- Drawbacks
  - Higher cost
  - Requires dedicated hardware and specialized skillset
- Leading model in business networks
- *Peer-to-Peer Model*
  - Direct sharing of resources among peers (laptops, desktops)
  - Difficult administration and backup due to dispersed files on different machines
  - Drawbacks
    - Redundancy
    - Complex management
    - Scalability issues
  - Useful for low-cost setups, exemplified by Napster a decade ago
  - Benefits
    - Low cost
    - No specialized infrastructure or hardware
  - Drawbacks
    - Decentralized management

- Poor scalability for large networks
■ Not recommended for business networks

- **Network Geography**
  - *Personal Area Network (PAN)*
    - ■ Smallest network type
    - ■ Covers about 10 feet or less
    - ■ Examples are Bluetooth and USB
    - ■ Connection within arm's reach
  - Local Area Network (LAN)
    - ■ Common in office buildings
    - ■ Limited distance
      - Up to 100 meters
      - CAT 5 cabling
    - ■ Can use WiFi (IEEE 802.11) or Ethernet (IEEE 802.3)
    - ■ Examples include Office, school, and home
  - *Campus Area Network (CAN)*
    - ■ Building-centric LAN
    - ■ Spans numerous buildings in an area
    - ■ Covers several miles
    - ■ Examples are College campuses, business parks, military bases

- *Metropolitan Area Network (MAN)*
    - Connects locations across the entire city
    - Larger than CAN
        - Up to 25 miles
    - Examples are City departments, multiple campuses in a city
- *Wide Area Network (WAN)*
    - Connects geographically disparate internal networks
    - Large geographic coverage
        - Across states, countries, or globally
    - Can consist of lease lines or VPNs.
    - Examples are Internet, private connections between offices across the country
- Important Standards
    - PAN – Bluetooth, USB (considered personal area networks)
    - LAN – IEEE 802.3 (Ethernet)
    - CAN – connects multiple LANs, forming a larger network
    - MAN – spans an entire city, connecting different locations
    - WAN – encompasses large geographic areas, connecting internal networks globally
- Memory Aid
    - PAN (Personal Area Network) – arm's reach
    - LAN (Local Area Network) – limited to about 100 meters

- CAN (Campus Area Network) – spans buildings in an area

- MAN (Metropolitan Area Network) – across the city, up to 25 miles

- WAN (Wide Area Network) – geographically extensive, even global

- **Understanding Network Geography: Practical Example**

- **Wired Network Topology**
    - *Network Topology*
        - Refers to the arrangement of elements in a computer network
        - Includes links, nodes, clients, and servers
    - Diagram Types
        - *Physical Topology*
            - Describes physical cabling and device connections
            - Represents real-world layout using floorplans
        - *Logical Topology*
            - Describes how data flows in the network
            - Focuses on the logical connection rather than physical placement
    - Six Wired Network Topologies
        - *Point-to-Point Topology*
            - Direct connection between two devices
            - Simple, reliable for small-scale connections
            - Not scalable

- - Used in WAN connections for remote offices
- **■** *Ring Topology*
  - Circular data path with each device connected to two others
  - Unidirectional flow prevents collisions
  - Creates a single point of failure situation unless there are redundant connections for failover
  - Common in FDDI (Fiber Distributed Data Interface) for long-distance fiber optic networks
- **■** *Bus Topology*
  - All devices connected to a central cable (bus)
  - Data accessible to all, but only intended recipient processes it
  - Easy to install
  - If the main cable fails, the network won't work
  - The more devices connected to the network, the more collisions will occur
  - Older technology, not common in modern networks
- **■** *Star Topology*
  - Each node connected to a central point (network switch).
  - Robust, but network depends on the central point's functionality
    - ○ If the central point fails, the entire network fails
  - Common in home networks

- ■ *Hub-and-Spoke Topology*
    - ● Variation of star topology with a central hub connected to multiple spokes
    - ● Nodes transmit data to the hub before reaching the final destination
    - ● Used in airline and telecommunications networks
    - ● Less expensive for larger networks
- ■ *Mesh Topology*
    - ● Point-to-point connections between every device for redundancy
    - ● Two types
        - ○ Full mesh – every node connected to every other
        - ○ Partial mesh – some nodes fully interconnected, others connected to one or two devices
    - ● Provides robustness and redundancy but can be complex and costly
    - ● Mesh Topology Formula
        - ○ Full mesh connections formula
            - ■ n (n-1)/2
            - ■ n is the number of nodes
- ○ Understanding different topologies is crucial for network design
    - ■ Each topology has unique advantages and disadvantages
    - ■ Practicality varies based on the scale and requirements of the network

- **Wireless Network Topology**
  - *Infrastructure Mode*
    - Centralized wireless network with a wireless access point
    - Similar to a star topology in a physical network
    - Common in homes
      - Connects to an outside provider through a cable or fiber modem
    - Supports wireless security controls
  - *Ad Hoc Mode*
    - Decentralized wireless network
    - Operates like a peer-to-peer network
    - No routers or access points
      - Devices connect directly
    - Dynamic routing decisions made on the fly
    - Allows for dynamic joining and leaving of devices
      - Resembling old-school chat rooms
  - *Wireless Mesh*
    - Unique interconnection of different nodes, devices, and radios
    - Creates a mesh topology for expansion and redundancy
    - Combines various technologies for connectivity
      - Bluetooth, WiFi, microwave, cellular, satellite
    - Enables large-scale network access in harsh environments
    - Uses different radio frequencies to establish reliable connections

- ■ Use Cases for Wireless Mesh
    - Post-disaster scenarios
    - Humanitarian assistance missions
    - Combining microwave, satellite, cellular, and WiFi for reliable and redundant networks
        - ○ Satellite for long distances
        - ○ Microwaves for medium ranges
        - ○ Wireless for short distances

- **Datacenter Topology**
    - ○ *Datacenter*
        - ■ Any facility composed of networked computers and storage that businesses and other organizations use to organize, process, store, and disseminate large amounts of data
    - ○ Three-Tiered Hierarchy
        - ■ *Core Layer*
            - Houses high-performance routers, merging geographically separated networks
            - Backbone of the network
        - ■ *Distribution/Aggregation Layer*
            - Provides boundary definition through access lists and filters
            - Defines policies for the network at large

- Uses layer 3 switches for routing between subnets
    - Ensure the packets are properly routed between different subnets and VLANs
- *Access/Edge Layer*
    - Connects endpoint devices using regular switches
    - Used to ensure the packets are converted to frames and delivered to the correct end point devices
- Having 3 layers provides better
    - Performance
    - Management
    - Scalability
    - Redundancy
- It also helps with troubleshooting because the layers and devices provide points at which parts of the network can be isolated to determine problems and maintain the rest of the network while the isolated part is fixed
- *Collapsed Core*
    - Network architecture where the core and distribution layers are merged into a single layer
    - Creates a two tiered core
    - Simplified architecture for medium to small datacenters
    - May not be suitable for larger and more complex networks

- ○ *Spine and Leaf Architecture*
    - ■ An alternative type of network architecture that is used specifically within datacenters
    - ■ Focuses on communication within datacenters, particularly server farms
    - ■ Consists of 2 switching layers
        - ● *Leaf*
            - ○ Consists of all the access switches that will aggregate traffic from the different servers and then connect directly into the spine layer
        - ● *Spine*
            - ○ Contains switches that interconnect all the leaf layer switches into a full-mesh topology
    - ■ Enhances speed, and reduces latency compared to traditional three-tiered hierarchy
    - ■ Works well with a Software Defined Network (SDN)
    - ■ Can also be used in combination with the standard three-tiered hierarchy
        - ● Servers in the datacenter connect to leaf layers
        - ● Spine connects to the core layer of the three-tiered hierarchy
- ○ Traffic Flows
    - ■ *North-South Traffic*
        - ● Traffic that enters (Southbound traffic) or leaves (North traffic) data center from a system outside

- *East-West Traffic*
    - Data flow within a datacenter
    - Example: In a spine and leaf architecture, all data flow between servers is considered east-west traffic
    - Prevalent with SDN, virtualization, and converged networks

OSI Model (& TCP Model Ports/Protocol)

Objective 1.1: Explain concepts related to the Open Systems Interconnection (OSI) reference model

- **Introduction**
    - Open Systems Interconnect Model (OSI)
        - Developed in 1977 by the International Organization for Standardization
        - OSI is a reference model
            - Used to categorize the functions of a network
            - Useful for troubleshooting
    - Networks today operate under the TCP/IP mode
    - Layers
        - Physical - Layer 1
        - Data Link - Layer 2
        - Network - Layer 3
        - Transport - Layer 4
        - Session - Layer 5
        - Presentation - Layer 6
        - Application - Layer 7
    - Networks are designed to make data flow across networks

- ○ Names of data as it flows through the OSI model

  - ■ Bits - Layer 1

  - ■ Frames - Layer 2

  - ■ Packets - Layer 3

  - ■ Segments - Layer 4

  - ■ Data - Layer 5

  - ■ Data - Layer 6

  - ■ Data - Layer 7

- **Layer 1 (Physical)**

  - ○ *Physical Layer Overview (Layer 1)*

    - ■ First layer of the OSI model where transmission of bits across the network occurs and includes physical and electrical network characteristics

    - ■ Data type occurs as bits

      - ● Binary bits represented as a series of 1s and 0s

  - ○ *Transition Modulation*

    - ■ Switching between levels to represent 1 or 0

      - ● Copper Wire (Cat5/Cat6) – Uses voltage (0V for 0, +5V/-5V for 1)

      - ● Fiber Optic Cable – Uses light (on for 1, off for 0)

  - ○ Connector Standards

    - ■ RJ-45 Connector – Used in CAT5/CAT6 cables

    - ■ Wiring Standards

- TIA/EIA-568A
- TIA/EIA-568B
  - Crossover cables – TIA/EIA-568A on one end, and TIA/EIA-568B on the other end
  - Straight-through cables – TIA/EIA-568B on both ends
- Physical Topology
  - Different physical network layouts
    - Bus
    - Ring
    - Star
    - Hub-and-Spoke
    - Full Mesh
    - Partial Mesh
  - Based on how cables are physically connected
- Synchronization
  - *Asynchronous Communication*
    - Start and stop bits for out-of-sync data transmission
  - *Synchronous Communication*
    - Real-time communication using a common time source
- Bandwidth Utilization
  - *Broadband*
    - Divides bandwidth into separate channels (e.g., cable TV)

- ■ *Baseband*
  - ● Uses all frequency of the cable all the time (e.g., telephone)
- ○ *Multiplexing*
  - ■ Involves taking some limited amount of resource and using it more efficiently
    - ● Allows multiple people to use a baseband connection at the same time
  - ■ *Time Division Multiplexing (TDM)*
    - ● *Allocates dedicated time slots*
  - ■ *Statistical Time Division Multiplexing (StatTDM)*
    - ● Dynamically allocates time slots based on when people need it
  - ■ Frequency Division Multiplexing (FDM)
    - ● Divides the medium into channels
- ○ Layer 1 Devices
  - ■ Cables – media
    - ● Fiber optic
    - ● Ethernet
    - ● Coaxial
  - ■ Wireless Media
    - ● Bluetooth
    - ● Wi-Fi
    - ● Near field communication

- Infrastructure Devices
  - Hubs
  - Access points
  - Media converters
- ○ Layer 1 Device Characteristics
  - Simply repeat whatever they receive
  - No logic or decision-making at Layer 1

- **Layer 2 (Data Link Layer)**
  - *Data Link Layer (Layer 2)*
    - Responsible for packaging bits from Layer 1 into frames and transmitting them across the network
    - Performs error detection and correction, identifies devices using MAC addresses, and provides flow control
  - *MAC Address (Media Access Control Address)*
    - A means for identifying a device physically and allowing it to operate on a logical topology
    - A unique 48-bit physical addressing system is assigned to every network interface card (NIC) produced
      - Written in hexadecimal numbers
      - First 24 bits – identify the manufacturer
      - Remaining 24 bits – identify the specific device

- Crucial for logical topology – identifying devices on the network
  - *Logical Link Control (LLC)*
    - Provides connection services and acknowledges message receipt, ensuring controlled data flow
    - Most basic form of flow control
      - Limits data sent by a sender and prevents receiver overwhelm
    - Uses a checksum to detect corrupted data frames
  - Synchronization Methods at Layer 2
    - *Isochronous Mode*
      - Common reference clock
      - Time slots for transmissions
      - Less overhead
    - *Synchronous Method*
      - Devices use the same clock, with beginning and ending frames, and control characters for synchronization
    - *Asynchronous*
      - Devices reference own clock cycles
      - No strict control over communication timing
  - Layer 2 Devices
    - Network Interface Cards (NICs)
    - Bridges

- ■ <u>Switches</u>
    - ● Intelligent use of logic to learn and send data to specific devices based on MAC addresses
- ○ Switch Operation
    - ■ Switches use CAM tables with MAC addresses to identify physical ports connected to devices
    - ■ Enables selective data transmission to specific areas in the network.

- **Layer 3 (Network Layer)**
    - ○ *Network Layer (Layer 3)*
        - ■ Concerned with routing and forwarding traffic using logical addresses
    - ○ Logical Addressing
        - ■ IP variants – common logical addressing schemes
            - ● IPv4 – written in dotted octet notation which are four sets of numbers separated by dots (e.g., 172.16.254.1)
            - ● IPv6
        - ■ Other protocols – these were replaced by IP (Internet Protocol)
            - ● AppleTalk
            - ● IPX (Internetwork Packet Exchange)
    - ○ Switching/Routing Methods
        - ■ *Packet Switching (Routing)*
            - ● Data is divided into packets and then forwarded

- Most commonly used method
  - *Circuit Switching*
    - A dedicated communication link is established between two devices
  - *Message Switching*
    - Data is divided into messages which may be stored and then forwarded
- Route Discovery and Selection
  - Routers maintain routing tables for determining the best path
    - Dynamic protocols (e.g., RIP, OSPF) enable routers to share and update route information
  - Routing protocols help decide how data is going to flow across the network and how the routers are going to communicate that information
- Connection Services at Layer 3
  - Augments Layer 2 services
  - Involves flow control
    - Prevents sender from overwhelming the receiver
  - *Packet reordering*
    - Ensures data packets arrive and are reassembled in the correct order

- ○ *Internet Control Message Protocol (ICMP)*
    - ■ Used for sending error messages and operational information to an IP destination
    - ■ *PING*
        - ● Most commonly used ICMP
        - ● Helps troubleshoot network issues by testing connectivity and response times
    - ■ *Traceroute*
        - ● Traces the route of a packet through the network
- ○ Devices and Protocols
    - ■ Routers
    - ■ Multi-layer switches
        - ● Combines Layer 2 switch and Layer 3 router features
        - ● <u>A switch is always a Layer 2 device, unless specifically mentioned that it is a multi-layer switch, then it is considered as a Layer 3 device</u>
    - ■ Layer 3 protocols
        - ● IPv4
        - ● IPv6
        - ● ICMP
- ○ <u>IP and routers are commonly encountered Layer 3 devices in exams</u>

- **Layer 4 (Transport Layer)**
  - *Transport Layer (Layer 4)*
    - Dividing line between the upper layers and the lower layers of the OSI model
    - Upper Layers
      - Transport
      - Session
      - Presentation
      - Application
  - *Segments*
    - Data Type in Transport Layer
  - Protocols in Layer 4
    - *TCP (Transmission Control Protocol)*
      - Connection-oriented protocol that is a reliable way to transport segments across the network
      - With acknowledgement
      - Uses Three-Way Handshake
        - SYN – synchronization
        - SYN-ACK – synchronization - acknowledgement
        - ACK – acknowledgement
      - Windowing for flow control

- Used for all network data that needs to be assured to get to its final destination
    - *UDP (User Datagram Protocol)*
        - A connectionless protocol that is an unreliable way to transport segments (datagram)
        - Used for audio and visual streaming
        - No three-way handshake and less overhead
        - No acknowledgment or retransmission
- Remember the data types in Layer 4 for the exam
    - Segment – data type for TCP
    - Datagram – data type for UDP
- TCP vs. UDP
    - TCP
        - Reliable
            - Uses Three-way Handshake
        - Connection-oriented
        - Segment retransmission and flow control through windowing
        - Sequencing
        - Acknowledgment of segments
    - UDP
        - Unreliable
            - No Three-way Handshake

- Connectionless

- No retransmission and no windowing

- No sequencing

- No acknowledgment of datagrams

- ○ *Windowing*

  - ■ Allows clients to adjust the amount of data in each segments during transmission

  - ■ Optimize throughput and bandwidth

  - ■ Open or close window based on retransmissions

- ○ *Buffering*

  - ■ Occurs when devices allocate memory to store segments if bandwidth is not readily available

  - ■ *Buffer*

    - ● Temporary storage for segments

  - ■ Prevents overflow by clearing segments

- ○ Layer 4 Devices

  - ■ Protocols

    - ● TCP and UDP

  - ■ Devices

    - ● WAN accelerators

    - ● Load balancers and firewalls

- **Layer 5 (Session Layer)**
  - *Session Layer (Layer 5)*
    - Manages sessions, ensuring separate conversations to prevent data intermingling
  - *Setting Up Session*
    - Checking of user credentials and assigning numbers to sessions to help identify
  - *Maintaining Session*
    - Continuous data transfer between parties
    - If connection breaks, it will require re-establishment
    - Includes acknowledgement of data
  - *Tearing Down a Session*
    - Ending a session once communication goals are achieved
    - Mutual agreement or one party disconnects
  - Layer 5 Devices and Protocols
    - *H.323*
      - Used for setting up, maintaining, and tearing down voice and video connections
      - Operates over the real-time transport protocol (RTP)
    - *NetBIOS*
      - Utilized by computers for file sharing over a network
      - Commonly associated with Windows file sharing

- ○ <u>Layer 5 issues involve protocols and software rather than specific devices</u>

- **Layer 6 (Presentation Layer)**
  - ○ *Presentation Layer (Layer 6)*
    - ■ Responsible for <u>formatting data</u> for exchange and securing it through <u>encryption</u>
  - ○ *Data Formatting*
    - ■ Formatting data by a computer to have compatibility between different devices
    - ■ Formats
      - ● *American Standard Code for Information Interchange (ASCII)*
        - ○ Text-based language to use
        - ○ Ensures data is readable by receiving system
        - ○ Provides proper data structures
        - ○ Negotiates data transfer syntax for the Application Layer (Layer 7)
      - ● GIFs – motion pictures
      - ● JPEG – photographs
      - ● PNG – Internet images
    - ■ Formats enable compatibility between different devices

- ○ *Encryption*
    - ■ Used to scramble data in transit to keep it secure and provide data confidentiality
    - ■ *Transport Layer Security (TLS)*
        - ● Ensures secure data transfer
        - ● Creates an encrypted tunnel, protecting sensitive information
- ○ *Scripting languages* in Layer 6
    - ■ Control how ASCII text is displayed on the screen
        - ● HTML
        - ● XML
        - ● PHP
        - ● JavaScript
- ○ *Standard text formats*
    - ■ Different ways of displaying text using ones and zeros
        - ● ASCII
        - ● Unicode
        - ● EBCDIC
- ○ *Image formats*
    - ■ Different graphical representations of 1s and 0s
        - ● GIFs
        - ● JPEGs
        - ● TIFFs

- SVGs
- PNGs
  - *Movie file formats*
    - 1s and 0s formatted to create watchable videos
      - MP4s
      - MPEGs
      - MOV
  - Encryption Algorithms
    - Scrambles data to provide confidentiality and security during transit and storage
      - TLS
      - SSL (Secure Sockets Layer)
    - Focus on Security

- **Layer 7 (Application Layer)**
  - *Application Layer (Layer 7)*
    - Provides application-level services where users communicate with the computer
    - Focus on lower-level applications
      - File transfer
      - Network transfer

- ○ *Application Services*
    - ■ Unites components for more than one network application
        - ● File transfer
        - ● File sharing
        - ● Email
            - ○ Low-level protocols
                - ■ POP3 (Post Office Protocol 3)
                - ■ IMAP (Internet Message Access Protocol)
                - ■ SMTP (Simple Mail Transfer Protocol)
        - ● Remote access
        - ● Network management
        - ● Client-server processes
- ○ *Service Advertisement*
    - ■ Applications send announcements to other devices on the network
    - ■ Devices advertise the services they offer
        - ● Printers and file servers managed by Active Directory
        - ● Self-advertising devices like wireless printers
- ○ Layer 7 Protocols
    - ■ Email Applications
        - ● POP3
        - ● IMAP
        - ● SMTP

- ■ Web Browsing
    - ● HTTP
    - ● HTTPS
- ■ Domain Name Service (DNS)
- ■ File Transfer Protocols
    - ● FTP
    - ● FTPS
    - ● SFTP
- ■ Remote Access
    - ● Telnet
    - ● SSH
    - ● SNMP

- **Encapsulation and Decapsulation**
    - ○ *Encapsulation*
        - ■ Process of putting headers and sometimes trailers around data
    - ○ *Decapsulation*
        - ■ Removing the applied encapsulation to access the original data
    - ○ OSI Model Layers
        - ■ Moving down from Layer 7 to 1 – encapsulation
        - ■ Moving up from Layer 1 to 7 – decapsulation

- *Protocol Data Units (PDUs)* in OSI Model

  - A single unit of information transmitted in a computer network

    - Terminology used for each layer is written as L(layer number) PDU

      - Example – L7 PDU for Layer 7

  - There are special names for the PDUs for layers 1, 2, 3, and 4

    - Layer 1 – Bits

    - Layer 2 – Frames

    - Layer 3 – Packets

    - Layer 4 – Segments (TCP) or Datagrams (UDP)

- TCP Header (Layer 4)

  - 10 mandatory fields, totalling 20 bytes of information

    - Source port

    - Destination port

    - Sequence number

    - Acknowledgment numbers

    - TCP data offset

    - Reserved data – always set to zero

    - Control flags

      - SYN – synchronize connection in three-way handshake

      - ACK – acknowledgment of the successful receipt of data

      - FIN (Finished) – tears down connections created by three-way handshake

- ○ RST (Reset) – used when an unexpected packet is received

- ○ PSH (Push) – ensures data is given priority

- ○ URG (Urgent) – identifies incoming data as urgent

- Window size

- TCP checksum

- Urgent pointer

- mTCP – optional

○ UDP Header (Layer 4)

■ 8-byte header

- Source port

- Destination port

- Length – indicates the total packet bytes

- Checksum – not mandatory

○ IP Header (Layer 3)

■ Contains various fields

- Version

- Length of IP header

- Type of service

- Total length of packet and header

- Identifier

- Flags

- Fragmented offset

- Time to live

- Protocol

- Header checksum

- Source IP Address

- Destination IP Address

- Options and Padding

○ Ethernet Header (Layer 2)

■ Features a few things

- Destination MAC Address

- Source MAC address

○ *MAC Address*

■ Physical address that is used to identify a network

card on a local area network

■ Processed by switches

- *EtherType field*

○ Used to indicate which protocol is encapsulated in the

payload of a frame

■ IPv4 or IPv6

- VLAN Tag – optional

○ IEEE 802.1Q

○ IEEE 802.1AD

- A frame being sent at Layer 2 will also contain a payload
    - *Payload*
        - Data that being sent across the network
        - 42 bytes – using VLANs
        - 46 bytes – no VLANs
        - *Maximum Transmission Unit (MTU)*
            - Maximum size for payload
                - 1500 bytes for Ethernet
    - *Jumbo Frames*
        - Frames larger than 1500 bytes
        - Require reconfiguring MTU
- Data Transmission
    - Encapsulation of data and adding header at each layer
        - Layer 4 – source/destination ports
        - Layer 3 – source/destination IP addresses
        - Layer 2 – soure/destination MAC addresses
        - Layer 1 – data transmitted as 1s and 0s
    - Decapsulation at each intermediate device until the final host is reached
    - Final host decapsulates to Layer 7 for application understanding

- **Understanding the OSI Model: Practical Example**

Ports and Protocols

Objective 1.4: Explain common networking ports, protocols, services, and traffic types

- **Introduction**
    - *Port*
        - Virtual entry/exit point for communications used by software applications to exchange information
    - *Protocol*
        - Set of rules and conventions for data exchange between network devices

- **Network Port Fundamentals**
    - *IP address*
        - Used to direct data to the correct system in a network
    - *Port*
        - A logical opening in a computer
        - Identifies specific applications or services on a computer that represents a service or application
        - Numbered from 0 to 65,535
    - Three Groups of Ports
        - Well-known ports
            - Numbered from 0 to 1,023 Ephemeral ports (49,152-65,535)

- Examples
  - FTP (20, 21)
  - SMTP (25)
  - HTTP (80)
  - HTTPS (443)
- Registered ports
  - Numbered from 1,024 to 49,151
- *Ephemeral Ports*
  - Temporary, short-lived ports for dynamic use
  - Numbered from 49,152 to 65,535
  - No registration is required and anyone can use them
- Both Well-known and Registered Ports are registered with IANA for specific applications or services
- Data Transfer Example
  - Client communicates with a website using IP addresses and ports
  - Client's source IP and random ephemeral port connect to the website's destination IP and default port (e.g., 80)
- Two-Way Communication
  - Web server responds using its well-known port (e.g., 80) back to the client's ephemeral port
  - Two-way communication is established between client (ephemeral port) and web server (port 80)

○ Ephemeral ports opened for specific tasks and closed after data transmission.

○ In subsequent communications, the client uses the well-known port (e.g., 80) but selects a new random ephemeral port

○ Communication Flow

■ Source IP and port initiate communication

■ Data is transmitted

■ Ports closed when the task is completed

● **Transmission Control Protocol (TCP)**

○ *Transmission Control Protocol (TCP)*

■ Fundamental protocol in the Internet Protocol Suite that governs data exchange over the internet

■ Ensures reliable delivery of packets

● Error checking

● Data sequencing

● Acknowledgment

■ <u>Operates at the transport layer of the OSI model</u>

■ Breaks down larger messages into smaller packets for efficient data transfer and reassembles at the destination

○ *<u>Three-Way Handshake</u>*

■ Initiated to establish a connection between two systems

● SYN (Synchronize)

https://www.DionTraining.com

- - - SYN-ACK (Synchronize-Acknowledgement)

      - ACK (Acknowledgement)

    - Ensures readiness for secure data transmission

  - Error Checking and Flow Control

    - Error checking

      - Uses sequence numbers and acknowledgment messages

      - Detects and retransmits lost or corrupted packets

    - Flow control

      - Prevents overwhelming the receiver

      - *Windowing*

        - Controls the amount of data sent at a time

        - Allows dynamic adjustment based on network conditions

  - *Ports*

    - Numerical identifiers for services or applications in TCP/IP suite

    - Distinguish between different services on the same server

    - Each connection identified by source and destination IP addresses and ports

      - e.g., secure websites use port 443 (HTTPS)

    - Enable multiple network applications on the same server

  - TCP's Role in Internet Communication

    - Ensures reliability and ordered delivery between client and server

    - <u>Operates at the transport layer of the OSI model</u>

- Utilizes packetization, acknowledgment, and error checking

- Three-way handshake establishes a secure connection

- Ports facilitate the logical differentiation of services on a single machine

- **User Datagram Protocol (UDP)**
  - *User Datagram Protocol (UDP)*
    - Communication protocol used for time-sensitive transmissions on the internet
      - Ideal for applications prioritizing speed over error checking
      - Low latency and reduced processing overhead.
      - Lacks error checking and recovery services like TCP
    - Operates at the transport layer, similar to TCP
    - Connectionless communication model
  - Packet Structure
    - *Datagrams*
      - Term for data packets in UDP
      - Sent without prior setup of transmission channels
      - Contains source/destination port numbers, length field, and checksum
      - Smaller and simpler headers (8 bytes) compared to TCP (20-60 bytes)

- ○ UDP's Stateless Nature

    - ■ UDP does not maintain connection state or track packets

    - ■ Often referred to as a "fire and forget" protocol

    - ■ No waiting for acknowledgments, leading to faster transfer rates

- ○ Reliability Trade-off

    - ■ UDP is less reliable due to lack of packet tracking

    - ■ Suitable for scenarios where speed is crucial, and packet loss is acceptable

- ○ Use Cases

    - ■ Used in applications like live broadcasts, online gaming, and VoIP calls

    - ■ Effective for simple request-response communications (e.g., DNS lookup)

- ○ UDP utilizes ports to differentiate between multiple services on the same client/server

- ○ UDP relies on application-level error handling due to lack of built-in error recovery

- ○ UDP contains a checksum in the header for minimal protection against data corruption

- ○ UDP is not as robust as TCP in ensuring data integrity and delivery

- **Internet Control Message Protocol (ICMP)**
  - *Internet Control Message Protocol (ICMP)*
    - An integral part of the Internet Protocol Suite which is considered to be a network layer protocol for diagnosing network communication issues
    - Not used for data transmission between systems unlike TCP and UDP
    - Operates at the network layer of the OSI model
  - ICMP Messages
    - Used for indicating host or service unreachability, expired time to live, and router buffer issues
  - Ping Utility
    - Utilizes ICMP to test host reachability on an IP network
    - Measures roundtrip time (latency) for network connection
  - ICMP Message Structure
    - Header
      - Type – indicates the type of ICMP message (1 byte)
      - Code – provides additional context about the message type (1 byte)
      - Checksum – used for error checking the message header and data (2 bytes)
  - ICMP Reliability and Design
    - Lacks reliability mechanisms like TCP
      - No guaranteed delivery, ordering, or error correction

- ■ Designed for speed and simplicity, not data integrity or security
  - ○ Security Concerns
    - ■ ICMP can be used in attacks
      - ● ICMP Flood Attack
        - ○ Overwhelms target with echo request packets, leading to Denial of Service (DoS) Attack
        - ○ Amplified up to Distributed Denial of Service (DDoS) Attack to be effective
      - ● Ping of Death
        - ○ Exploits vulnerabilities in older systems, causing system crashes
  - ○ Modern Security Measures
    - ■ Many modern systems are not vulnerable to Ping of Death due to improved security measures
    - ■ Network administrators may choose to block ICMP traffic for security but face challenges in troubleshooting network issues

- **Web Ports and Protocols**
  - ○ *Web Ports and Protocols*
    - ■ Standardized rules and numerical gateways that govern data transmission and communication on the internet for websites

- ○ Two Fundamental Ports
    - ■ Port 80 (HTTP)
        - ● *HTTP (Hypertext Transfer Protocol)*
            - ○ An application layer protocol. This designed to enable communications between clients and servers
            - ○ Uses port 80 by default
            - ○ Foundation of data communication on the worldwide web
            - ○ Requests and receives web content in plain text
        - ● HTTP over Port 80 lacks security makes data vulnerable to eavesdropping and attacks
    - ■ Port 443 (HTTPS)
        - ● *HTTPS (Hypertext Transfer Protocol Secure)*
            - ○ Similar to HTTP but adds encryption via SSL/TLS
            - ○ Uses port 443
            - ○ Encrypts data, securing it from interception or tampering
- ○ Importance of HTTPS (Port 443)
    - ■ Vital for websites handling sensitive data like banking, e-commerce, or login pages
    - ■ Automatic redirection from insecure HTTP (port 80) to secure HTTPS
    - ■ Encryption ensures secure transmission of sensitive information

- ○ Key Differences between HTTP (Port 80) and HTTPS (Port 443)
    - ■ Security and Encryption
        - ● HTTP (port 80) – unencrypted, plain text
        - ● HTTPS (port 443) – encrypted using SSL/TLS, more secure against data breaches
    - ■ Default Usage
        - ● HTTP (port 80) – traditional, default for unsecured browsing
        - ● HTTPS (port 443) – introduced later, became default for secure browsing in recent years
    - ■ Search Engine Optimization (SEO) and Trust
        - ● HTTPS (port 443) – favored for increased security and ranked higher by search engines due to user trust and encryption

- **Email Ports and Protocols**
    - ○ *Email Ports and Protocols*
        - ■ Govern the transmission of emails across the Internet
        - ■ Ensure efficient sending, receiving, and management of messages
    - ○ Main Email Protocols
        - ■ *SMTP (Simple Mail Transfer Protocol)*
            - ● The standard protocol used for sending emails over the internet
            - ● Operates over port 25
                - ○ Default port used by email servers

- - ○ Insecure because data is sent in plain text
  - Only used for sending emails
  - *SMTPS (SMTP Secure)*
    - ○ A secure variant of SMTP
    - ○ Not really a protocol itself, but a way to secure the SMTP protocol by transporting it via the secure socket layer or transport layer security protocols
    - ○ Operates over ports 465 or port 587
- *POP3 (Post Office Protocol version 3)*
  - Used to retrieve emails from a remote server to a local client
  - Operates over port 110
  - Designed to download and delete messages from the server
  - Transmits emails in plain text (insecure)
  - *POP3S (POP3 Secure)*
    - ○ A secure variant of POP3 that overcomes the limitations of POP3
    - ○ Operates over port 995 via SSL/TLS
- *IMAP (Internet Message Access Protocol)*
  - Offers more flexibility than POP3
  - Operates over port 143
  - Allows managing emails directly on the server, synchronizing across multiple devices

- Transmits emails in plain text (insecure)
- *IMAPS (IMAP Secure)*
    - A variant of IMAP that can provide a secure and encrypted connection by transmitting data inside of an encrypted SSL/TLS using the standard IMAP protocol
    - Operates over port 993
- SMTP and SMTPS are used for sending emails
- POP3 and IMAP are both used for receiving emails
    - IMAP offers more sophisticated email management
- Understanding protocols ensures secure and efficient email communication
- Configure systems with secure variants to protect against security threats

- **File Transfer Ports and Protocols**
    - *File Transfer Ports and Protocols*
        - Specialized rules and procedures that are utilized for the transmission of files across networks
    - *FTP (File Transfer Protocol)*
        - Oldest protocol for file transfer
        - Ports:
            - Port 20 – actual data transfer
            - Port 21 – sending control commands
        - Lack of encryption poses security risks

- ■ Transmissions are sent in plain text

- ■ Widely used for its simplicity across platforms

- ○ *SFTP (Secure File Transfer Protocol)*

  - ■ Addresses FTP security concerns

  - ■ Also stands for SSH File Transfer Protocol

  - ■ Operates on port 22 – standard port for SSH connections

  - ■ Encrypts data for secure file transmissions

- ○ *TFTP (Trivial File Transfer Protocol)*

  - ■ Basic version of FTP that lacks authentication and directory browsing

  - ■ Operates on port 69

  - ■ Designed for sending files when minimal security is sufficient

- ○ *SMB (Server Message Block)*

  - ■ A network file sharing protocol that allows applications to read and write to files and request services from the server programs

  - ■ Operates on port 445

  - ■ Predominantly used for Windows file sharing

  - ■ *Samba*

    - ● A cross-platform version of SMB that exists on Linux systems

  - ■ Almost exclusively used inside of LANs and it is not a protocol to send data across the Internet

- ○ Key Considerations for Protocol Selection

  - ■ Align security requirements, network environment, and functionality

- FTP – basic transfers (ports 20, 21)

- SFTP – secure transfers (port 22)

- TFTP – simple, unsecured transfers (port 69)

- SMB – Windows file sharing in LANs (port 445)

- **Remote Access Ports and Protocols**

  - *Remote Access Ports and Protocols*

    - Build and manage systems and networks remotely from anywhere in the world

    - Crucial for interconnected environments, allowing control over systems, commands, and files.

  - Remote Access Protocols

    - *SSH (Secure Shell)*

      - Protocol for secure remote login and network services over an unsecure network

      - Operates on port 22

      - Provides a secure channel, strong authentication, and encrypted data communication

      - Used by network administrators for remote control of web and server applications

    - *Telnet*

      - Early remote log-in protocol

- Operates on port 23

- Allows remote login to another computer on the same network

- Transfers data in plain text, making it susceptible to eavesdropping and on-path attacks

- Replaced by SSH due to lack of encryption

- *RDP (Remote Desktop Protocol)*

  - Proprietary protocol by Microsoft for graphical user interface remote connection

  - Operates on port 3389

  - Allows remote access to a window system, supporting different network topologies

  - Supports data encryption, smart card authentication, and bandwidth reduction

- Considerations

  - Choose the appropriate protocol based on security requirements and specific tasks

  - SSH is recommended for secure command-line management.

  - Telnet should be avoided due to its lack of encryption

  - RDP is essential for secure graphical access to Windows-based systems

- **Network Service Ports and Protocols**
  - *Network Services, Ports, and Protocols*
    - Fundamental services for smooth digital communication and network management
    - Different services that ensure that the network devices can discover each other, communicate efficiently, and relay important system information to each other
  - *DNS (Domain Name System)*
    - Used for translating human-friendly domain names to IP addresses
    - Operates on ports 53 (UDP by default) for queries and responses
    - Uses TCP for larger messages
  - *DHCP (Dynamic Host Configuration Protocol)*
    - Automates the assignment of IP addresses and networking parameters to client devices
    - Listens on port 67 (UDP) for client requests
    - Responds on port 68 (UDP)
  - *SQL Services*
    - Refers to protocols used by database servers for managing queries
    - Microsoft SQL Server operates on port 1433
    - MySQL Server on port 3306
  - *SNMP (Simple Network Management Protocol)*
    - Used for collecting information and configuring network devices

- - Operates on <u>port 161</u> (UDP) for polling

    - Operates on <u>port 162</u> (UDP) for unsolicited trap messages

    - Crucial for <u>network diagnostics and performance monitoring</u>

  - *Syslog (System Logging)*

    - Standard for message logging allowing devices to send <u>event</u> messages across IP networks

      - *Syslog Server*

        - Event message collector where syslog messages are sent to

    - <u>Operates on port 514</u>

      - Uses <u>UDP by default</u>

      - Can use <u>TCP for reliability</u>

- **Other Network Service Ports and Protocols**

  - *Other Network Service Ports and Protocols*

    - Refers to different network, service, ports, and protocols that play a pivotal role in the network, time synchronization, and the establishment of communication sessions, as well as directory services

    - Crucial for organizing and providing access to distributed information located all across the network

  - *Network Time Protocol (NTP)*

    - Used to synchronize clocks of computers over a network

- **Vital for time-dependent processes**, timestamping events, transaction logging, and security protocols

- **Operates over port 123** using the User Datagram Protocol (UDP)

- Example

  - Ensures consistency between server and client times, affecting encryption and decryption functions

○ *Session Initiation Protocol (SIP)*

- Initiates, maintains, and terminates real-time sessions for voice, video, and messaging

  - Common usage includes <u>Voiceover IP applications</u> for internet phone calls

- Operates over <u>port 5060</u> (traditionally) on both UDP and TCP for unencrypted signaling

- Uses <u>port 5061</u> using TCP with TLS (Transport Layer Security) for encrypted signaling

○ *Lightweight Directory Access Protocol (LDAP)*

- Protocol for accessing and maintaining distributed directory information services over an IP network

- Used to look up personal information in email programs

- Ports

  - <u>LDAP (Insecure): Communicates over port 389</u> using both TCP and UDP

- <u>LDAPS (Secure)</u>: Encrypted with SSL or TLS, runs over <u>port 636</u>
  using TCP

https://www.DionTraining.com

Media and Connectors

Objectives:

- 1.5 - Compare and contrast transmission media and transceivers
- 5.5 - Given a scenario, use the appropriate tool or protocol to solve networking issues

- **Copper Media**
  - *IEEE 802.3 Standard*
    - Defines physical and data link layers, including MAC, for wired Ethernet networks
    - Commonly used in Local Area Networks (LANs)
  - *Twisted Pair Cables*
    - A type of wiring in which two conductors of a single circuit are twisted together
    - Twisting reduces electromagnetic interference and crosstalk
    - Unshielded Twisted Pair (UTP)
      - Composed of pairs of wires twisted together without additional shielding being added to the cable
      - Lightweight, flexible, and cost-effective
    - Shielded Twisted Pair (STP)
      - Includes shielding for better EMI protection
      - More expensive, bulkier, and more difficult to install

- Categories
  - CAT 5
  - CAT 5e
  - CAT 6
  - CAT 6a
  - CAT 7
  - CAT 8

○ *Coaxial Cables*

- A fundamental part of networking and broadcasting for decades
- Consists of single copper conductor at its core, with insulating layer and conductive shield
- RG-6
  - Used to support faster internet speed in most residential installations
  - Standard for modern coaxial cable
  - Supports up to 1 Gbps at up to around 300-meter distance
- RG-59
  - Older standard for coaxial cables
  - Not commonly used anymore
- Direct Attach Copper (DAC) Cables
  - Fixed assembly copper cabling for short distances
  - Connects switches, routers, or servers

- Supports up to 100 Gbps at short distances
  - Twinaxial Cable
    - Often a component of DAC assembly
    - Considered as another specialized form of cabling
    - Two insulated copper conductors
    - Used in SFP+ and QSFP applications
    - Supports 10 Gbps to 100 Gbps, up to 100 meters
- Plenum vs. Non-Plenum Cables
  - Plenum – Fire-retardant, suitable for air circulation spaces
  - Non-Plenum – Less fire-resistant, used where fire risk is lower
  - Plenum meets strict fire safety standards of NFPA and NEC
- It is important to <u>remember the basic speed and distance for each type of cable</u>
  - CAT 5 – 100 Mbps at 100 meters
  - CAT 5e – 1Gbps at 100 meters
  - CAT 6 – 1Gbps at 100 meters; 10 Gbps at 55 meters
  - CAT 6a – 10 Gbps at 100 meters
  - CAT 7 – 10 Gbps at 100 meters
  - CAT 8 – 10-25 or 40 Gbps at 30 meters
  - RG-6 – 1 Gbps at 300 meters
  - Twinaxial – 10 Gbps or more at 10 meters
  - DAC – 100 Gbps at 15 meters (active cables); 100 Gbps at 7 meters (passive cables)

- ○ Importance of Copper Media

  - Versatile and robust for various networking needs

  - Lower cost, easier to install and maintain

  - Remains vital in network infrastructure

- **Copper Network Connections**

  - ○ *Registered Jack (RJ-X)*

    - A standard telecommunication network interface

    - RJ-11 and RJ-45

      - Crucial for voice and data networks

      - Use twisted pair cables

  - ○ *Radio Guide (RG-X)*

    - Series for coaxial cables, used in high-speed internet, television, and radio connections

    - Commonly used cables

      - RG-6 – for cable TV

      - RG-59 – for older applications

  - ○ Connectors

    - *RJ-11*

      - Standard for telephone wiring

      - 6P2C configuration (6 positions, 2 conductors)

      - Smaller size

      - Not suitable for high-speed data transmission

- ■ *RJ-45*

    - ● Standard for data networks (Ethernet)

    - ● 8P8C configuration (8 positions, 8 conductors)

    - ● Widely used for computers, switches, routers in local area networks

    - ● Compatible with CAT 5 to CAT 8 cables – supporting higher bandwidths with higher CAT numbers

- ■ *F-Type Connector*

    - ● Screw-on connector used with RG-6 and RG-59 coaxial cables

    - ● Standard for cable TV, satellite, and cable internet connections

- ■ *BNC Connector (Bayonet Neill-Concelman)*

    - ● Coaxial connector with a secure bayonet locking mechanism

    - ● Used with RG-6 or RG-59 coaxial cables

    - ● "Push and twist" style connector

    - ● Common in professional video connections and radio frequency applications

    - ● Introduced in the 1940s, often erroneously called British Naval Connector

- ○ Application Specifics

    - ■ RJ-11 – for voice-based communication networks (telephones)

    - ■ RJ-45 – for data devices in data networks (computers, printers, switches, routers)

■ F-Type – for coaxial cables in cable TV, satellite, and cable internet connections

■ BNC – for professional video connections and radio frequency applications

● **Building a Copper Cable: Demonstration**

● **Fiber Media**

○ *Fiber Media*

■ Transmits data using light, not electrical impulses

■ Offers significant advantages over traditional copper media-based networks

○ Advantages of Fiber Media

■ Immunity to EMI

● Light-based transmission is not affected by electromagnetic interference (EMI)

● Doesn't require shielding like copper cables

■ Longer transmission distances with minimal signal loss

● Fiber optic cables can span hundreds of miles

● Suitable for local connections and transcontinental data transmission

- - Higher data transfer speeds
    - Can reach speeds beyond 10 Gbps
  - Drawbacks
    - Cost
      - Fiber media is more expensive than copper
    - Complexity
      - Requires specialized tools and training for installation and repair
  - Two Main Types of Fiber Optic Cables
    - Single-Mode Fiber (SMF)
      - Designed for long-distance communication
      - Small glass core allows light to travel in a single path without dispersion
        - 8.3 to 10 microns in diameter
      - Preferred for backbone installations and connections over vast areas
      - Yellow sheath
      - For long-range transmissions with higher bandwidth
    - Multi-Mode Fiber (MMF)
      - Tailored for shorter distances
        - 2 kilometers to 1 mile
      - Larger fiber core size allows light to travel in multiple paths
        - 50 to 100 microns

- Suitable for connecting servers to switches within buildings or campuses

- Aqua blue or orange sheath

- For internal network infrastructures, offering cost-effectiveness and ease of installation

- **Fiber Network Connections**
  - *Fiber Network Connections*
    - Created by connecting a fiber optic cable to two different devices
  - *Fiber Connectors*
    - Enable a quicker connection and disconnection from the network
    - Two different sets of connectors on the cable:
      - For transmission side
      - For receive side
    - Types:
      - SC Connector (Subscriber Connector)
        - Square shape with push-pull design
        - Widely used in single-mode fibers
        - Common in telecommunications and data networking
        - Used in FTTH deployments for reliability and ease of use
      - LC Connector (Lucent Connector)
        - Compact size with push-pull mechanism

- ○ Favored in high-density applications like data centers
- ○ Often shipped as paired cables for transmit and receive sides
- ○ Features high-precision alignment, ensuring efficient data transmission and minimized potential data loss
- ● ST Connector (Straight Tip Connector)
  - ○ Round shape with twist-lock mechanism
    - ■ Critically important when operating in any kind of environment where movement or vibrations might occur
  - ○ Reliable connection, commonly used in multi-mode fiber optics
  - ○ Well-suited for outdoor applications due to its durability
- ● MTRJ Connector (Mechanical Transfer-Registered Jack)
  - ○ Small, rectangular design housing transmit and receive fibers
  - ○ Suitable for space-constrained applications like office LANs
  - ○ Offers high-density capabilities with an RJ-style latch mechanism
  - ○ Offers cost-effective solution for densely populated network environments

- MPO Connector (Multi-fiber Push On Connector)
    - Designed for multiple fibers in a single connector
    - Essential in high-density applications such as data centers and high-speed networks
    - Enables quick and efficient connections, crucial for rapid scalability
- Each type of connector can be polished or shaped
- *Back Reflection*
    - Occurs when a portion of transmitted light in a fiber optic cable reflects back toward the source, potentially degrading the signal
    - Minimizing back reflection is crucial for maintaining signal integrity and optimizing data transmission
- Polish Types:
    - PC (Physical Contact) Style
        - Having slight curvature in the fiber face to lower back reflection over standard straight-cut fiber
        - Provides the least effective reduction in back reflection
        - Best suited for short-distance or lower-speed data transmissions
    - UPC (Ultra Physical Contact) Style
        - Having dome-shaped end-face for better core alignment
        - Offers lower back reflection than PC style
        - Suitable for general broadband applications

- APC (Angled Physical Contact) Style
  - Uses an <u>8-degree angled</u> polish to greatly reduce back reflection
  - Lowest amount of back reflection
  - Well-suited for high bandwidth and long-distance applications, such as undersea cable networks
- Regular updates on connectors and standards are essential for efficient network design and maintenance

- **Transceivers**
  - *Transceiver*
    - A device capable of both transmitting and receiving data
    - Blend of "transmitter" and "receiver"
    - Utilizes specific protocols for data transmission and reception
  - *Protocols*
    - Set of rules governing data transmission and reception
    - Main protocols:
      - *Ethernet*
        - Family of networking technologies for LANs, MANs, and WANs
        - Facilitates communication and data transfer
        - Defines physical standards, electrical standards, and data formats

- ○ Supports various data rates and media types
- Fibre Channel (FC)
  - ○ High-speed network technology that connects computer data storage to servers inside storage area networks
  - ○ Handles large data volumes quickly and reliably
  - ○ Supports optical fiber and copper-based media
  - ○ Key features:
    - ■ High throughput
    - ■ Low latency
    - ■ Advanced data integrity
- ○ Transceiver Functions
  - ■ Converts data between different protocols
  - ■ Enables communication between Ethernet and Fibre Channel networks
  - ■ Converts media types in Layer 1 (e.g., fiber to copper, copper to fiber)
- ○ Form Factors
  - ■ SFP (Small Form Factor Pluggable)
    - A compact hot pluggable optical module
    - Can be pulled in or pulled out without turning off the associated router or switch
    - Up to 4.25 Gbps
  - ■ SFP+
    - Faster version of SFP

- Up to 16 Gbps
  - QSFP (Quad Small Form Factor Pluggable)
    - Up to 40 Gbps
  - QSFP+
    - Slightly faster version of QSFP
    - Up to 41.2 Gbps
  - QSFP28
    - Up to 100 Gbps
  - QSFP56
    - Up to 200 Gbps
- QSFP modules are faster than SFP modules
- Transceivers convert light signals to electrical impulses

Distribution Systems

Objectives:

- 2.4 - Explain important factors of physical installations
- 5.5 - Given a scenario, use the appropriate tool or protocol to solve networking issues

- **Cable Distribution Systems**
  - *Cable Distribution System Overview*
    - Organized system connecting network backbone to end users via distribution frames
    - Design should be hierarchical for logical and functional placement within buildings
  - Components of Cable Distribution Systems
    - *Demarcation Point*
      - Location at which the Internet Service Provider (ISP) connection ends, and network infrastructure and cabling actually begins
      - Marks entrance of WAN into facility
      - Responsibility shifts to organization beyond this point
    - *Main Distribution Frame (MDF)*
      - Primary starting point for interior cabling distribution
      - Houses main point of presence router and backbone switch
        - Backbone switch connects all network components

- *Intermediate Distribution Frame (IDF)*
  - Branches out from MDF to serve smaller areas
  - Contains edge switches for local connections
  - *Cable Trays*
    - A unit or assembly of units that form a rigid structural system to securely support the cables and raceways
      - Horizontal – installed in drop ceilings or beneath raised floors
      - Vertical – vertical cross-connect, minimizing vertical cable crossings between floors
- *Racks*
  - Hold network equipment for efficient space management
  - Various types:
    - 2-post – for lighter equipment/patch pannels/network cabling
    - 4-post – for heavier equipment
    - Wall-mounted – space-saving solution for smaller equipment
    - Rack enclosures – for high-value equipment
- *Patch Panels*
  - Organize and facilitate connections within network infrastructure

- Utilize both sides
    - Front – network jacks (RJ-45 network ports)
    - Back – 110 punchdown block
- *110 Block*
    - A type of punchdown block used for both voice and data applications that rely on CAT 5 or newer copper-based networks
    - Installed using a punchdown tool
- Preferred over direct connections for network maintenance and port protection

- *Fiber Distribution Panels*
    - Facilitate fiber connections without punchdown blocks
    - Uses SC, LC, ST, or MTRJ
    - Can act as a converter for types of fiber connection
- Cable Distribution Process
    - Computer connected to wall jack using straight-through patch cable (copper or fiber)
    - Wall jack terminates cable into punch down block
    - Cable runs through walls, ceilings, or raised floor, across cable trays to intermediate distribution frame
    - Cable terminated into patch panel's punch down block

- Another patch cable connects patch panel to open port on edge switch in intermediate distribution frame
- For fiber instead of copper, switch, patch panel, and wall jack replaced with fiber counterparts
- Process breaks up long cable run into multiple pieces for flexibility and ease of repair
- Troubleshooting and repair facilitated by multiple connection points, avoiding full cable reruns for minor issues

- **Wiring a Network Demonstration**

- **Testing a Network Demonstration**

- **Power Distribution Systems**
  - Power Distribution Systems
    - Crucial for consistent and reliable power delivery
  - *Uninterruptible Power Supply (UPS)*
    - An electrical apparatus that provides emergency power during main power failures
    - Offers surge protection and line conditioning
    - Typically lasts 15 to 30 minutes
    - Installed at the bottom of each rack in data centers

- ■ Some data centers use larger UPS systems supporting multiple racks or the entire facility
- ○ *Power Distribution Unit (PDU)*
    - ■ A specialized device that distributes electric power to network components and computing equipment
    - ■ Advanced power strips with power monitoring and control features
    - ■ May be rack-mounted or in large cabinets for rows of servers
    - ■ Provides surge protection but not full protection against complete power loss
- ○ *Generators*
    - ■ Installed outside data centers for longer-term power during outages
    - ■ Powered by diesel, gasoline, or propane
    - ■ Paired with UPS or battery backup for seamless power transition
    - ■ Automatic transfer switch shifts power between UPS and generator
- ○ Power Load Management
    - ■ Critical for preventing circuit overloads and ensuring efficient power usage
    - ■ Careful calculation and monitoring of power loads on circuits
    - ■ New equipment installations require assessing power impact and balancing loads across data center

- Voltage Considerations

  - *Voltage*

    - Electric potential difference crucial in power distribution

    - US standard – 120 volts

    - European standard – 230 volts

  - Equipment must match voltage standards to operate properly

  - Dual voltage equipment can operate on both standards

  - Mismatched voltage can damage or destroy equipment

- Key Considerations

  - Install UPS, PDU, and backup generator for comprehensive power management

  - Ensure seamless power transition and protection against outages for data center reliability

  - Consider power loads and voltage requirements before equipment installation

- **Heating, Ventilation, and Air (HVAC) Systems**

  - *Heating Ventilation and Air Conditioning (HVAC) system*

    - Technology designed for indoor environmental comfort that provides temperature control, humidity management, and airflow regulation

    - Important for hardware and networking devices

- ○ Temperature Control

  - ■ Crucial for electronic equipment, including computer networks and data centers

  - ■ Overheating can lead to hardware malfunctions and reduced efficiency

  - ■ Maintain a steady temperature for peak efficiency

    - ● Typically 68-77°F or 20-25°C

    - ● Check equipment manufacturer's recommendations for specific temperature set points

- ○ Humidity Levels

  - ■ *Humidity*

    - ● Refers to the concentration of water vapor in the air

  - ■ Too much humidity can cause condensation, leading to corrosion or electrical shorts

  - ■ Too little humidity can cause static buildup, potentially damaging sensitive electronics

  - ■ Maintain relative humidity level of 40-60%

- ○ Airflow Management

  - ■ Important for dissipating heat generated by equipment in data centers

  - ■ Proper airflow management is crucial to prevent overheating or system shutdowns

- *Port-side Exhaust and Intake (*"Hot/cold aisle" Configuration)
  - Strategic method of air distribution in which server racks are positioned in alternating rows with cold and hot air
  - Maximizes cooling efficiency
  - Reduces energy consumption
- Design Considerations
  - Plan data center layouts with HVAC factors in mind
  - Proper rack spacing and orientation for efficient airflow
  - Use raised floor systems to push cold air upward into racks and expel hot air
  - Configure ceiling plenums to return cooled air to the data center
- Integration of HVAC system is imperative for uninterrupted operation and optimal performance of network and data center equipment

- **Fire Suppression Systems**
  - Fire Suppression System
    - Crucial for data centers
  - *Wet Pipe System*
    - Most basic type of fire suppression system
    - Involves sprinkler system with pipes always containing water
    - Activation occurs when fire alarm triggers valve opening, releasing water

- ■ Common in traditional office buildings but poses risk of water damage to equipment
- ○ *Pre-action System*
  - ■ Aim to minimize accidental releases
  - ■ Requires both detector actuation (e.g., smoke detector) and sprinkler activation before water release
  - ■ Offers enhanced security similar to two-factor authentication for fire system
- ○ *Special Suppression System*
  - ■ Utilize clean agents like halon, carbon agent, or inert gas
  - ■ Displaces oxygen in the room, suffocating fire
  - ■ Presents suffocation risk to people
    - ● Requires alarms and supplemental oxygen for personnel
- ○ Safety Measures
  - ■ Install clean agent systems to prevent water damage to equipment
  - ■ Ensure systems are professionally installed and annually inspected
  - ■ Be prepared for potential fire incidents by having suppression systems ready for use
- ○ While hoping to avoid fire incidents, it's crucial to have properly installed and maintained fire suppression systems in data centers to mitigate risks effectively

Wireless Networks

Objectives:

- 1.5 - Compare and contrast transmission media and transceivers
- 2.3 - Given a scenario, select and configure wireless devices and technologies

- **Wireless Network Types**
    - Wireless Network
        - Revolutionize connectivity, offering flexibility and scalability
    - *Ad Hoc Network/Independent Basic Service Set (IBSS)*
        - Network where devices connect directly to each other rathe than through a central access point
        - Operates like peer-to-peer networks
        - Ideal for quick, temporary setups without relying on existing infrastructure
        - Enables direct file sharing between devices within range
    - *Infrastructure Networks*
        - More organized setup in which devices connect to a network via wireless access points (APs) into wired local area networks (LANs)

- ■ Configuration:
  - ● *Basic Service Set Identifier (BSSID)*
    - ○ A unique identifier which is, by default, set to the MAC address of the wireless AP
  - ● *Service Set Identifier (SSID)*
    - ○ Common alphanumeric name given to the network
- ■ Larger setup configurations:
  - ● May require multiple APs with an Extended Service Set (ESS)
  - ● *Extended Service Set (ESS)*
    - ○ Creates a larger network that shares the same SSID to allow for seamless connectivity
    - ○ SSID becomes ESSID (Extended Server Set Identifier)
- ○ *Point to Point Networks*
  - ■ Connects two distinct locations over longer distances using high-gain antennas
  - ■ Static in nature with fixed locations at each end
  - ■ Offers dedicated bandwidth, ideal for linking buildings or areas without feasible cabling options
- ○ *Mesh Networks*
  - ■ Versatile and resilient, with nodes connecting to multiple others, creating infinite paths for data

- Self-healing capability ensures stability by reconfiguring around broken pathways
- Suitable for large-scale deployments where laying cables is impractical or expensive
- Two types:
  - Uses ESS configuration that operates in infrastructure mode
  - Involves multi-network integration

○ Autonomous vs. Lightweight Access Points

- *Autonomous AP*
  - Standalone devices handling wireless functions independently
  - Useful in small setups where centralized controller is not necessary
- *Lightweight AP*
  - Managed centrally by a wireless controller, simpler and cheaper
  - Offloads processing to the centralized controller, facilitating easier management in large networks

○ Considerations in Choosing Wireless Network Types

- Performance, reliability, and ease of use vary based on the network type
- Assess specific environment requirements and tasks when selecting the appropriate type
- Each type has its advantages and ideal use cases, ranging from simplicity to robustness

- **Wireless Antennas**
  - *Antennas*
    - Dictate the directionality and range of the signal that is being transmitted
  - *Wireless Antennas*
    - Devices that are designed to send and receive radio frequency signals
    - Types:
      - *Omni-directional Antennas*
        - Designed to transmit and receive signals equally in all directions
        - Ideal for providing broad coverage with uniform signal strength
        - Commonly used in wireless access points, mobile hotspots, and public networks
      - *Uni-directional Antennas*
        - Focuses energy in a single direction for a concentrated signal beam
        - Best suited for directing signals towards specific areas or remote locations
        - Often used in point-to-point connections, linking distant buildings or areas

- *Yagi Antennas*
    - Specific type of directional antenna providing high signal gains
    - Utilizes a narrow beam for long-distance communication in a specific direction
    - Commonly used for remote areas connecting to cell towers or television transmitters
- Considerations in Antenna Selection
    - Tailor choice to specific needs of the wireless system
    - Factors include desired coverage area, signal range, and physical environment
    - Selection impacts network performance and user experience
- Benefits of Proper Antenna Selection
    - Ensures strong and reliable connectivity
    - Tailors network to user needs and spatial constraints
    - Enhances performance and efficiency of wireless communication system

- **Understanding Antennas**
    - Types of Antennas
        - *Omnidirectional Antenna*
            - Sends and receives data in all directions with equal power

- Commonly <u>embedded in devices</u> (wireless access points, cell phones, etc.)
- Used when the signal direction is unknown or needs to reach multiple devices
    - *Unidirectional Antenna*
        - Focuses power in a <u>single direction</u>
        - Useful for long-distance communication or when limiting signal bleed-over is important
        - Included variants:
            - Unidirectional left
            - Unidirectional right
    - *Parabolic Antenna*
        - Specialized unidirectional antenna with a <u>curved dish</u>
        - Often used for microwave signals and <u>satellite TV</u> to focus energy toward a specific point
    - *Yagi Antenna*
        - A <u>type of directional antenna</u> often used for point-to-point communication over long distances
        - Provides a focused, directional beam of signal
- Some devices allow changing antennas for different needs
- Larger antennas can increase signal range but require more power

- ○ Exam Preparation

  - ■ Understand when to use each type of antenna

  - ■ Know about patch antennas for building-to-building communication

  - ■ Recognize antenna types based on their characteristics (omnidirectional, unidirectional, parabolic, Yagi)

- **Wireless Frequencies**

  - ○ *Wireless Frequencies*

    - ■ Refer to different frequency bands used to transmit and receive radio waves in wireless networks

    - ■ Each frequency band has specific characteristics related to speed, coverage, and regulations to prevent interference

  - ○ 2.4 GHz Band

    - ■ Widely used since 1997

    - ■ Long-range and better penetration through solid objects

    - ■ Contains frequencies from 2.400 GHz to 2.495 GHz

    - ■ Divided into channels with overlapping, causing interference

      - ● Up to channel 11 to 14

      - ● *Channel*

        - ○ Physical medium through which wireless networks can send and receive data

- - ○ Channels that do not overlap that are advisable for use to avoid interference:
      - Channel 1
      - Channel 6
      - Channel 11
  - ○ 5 GHz Band
    - Offers faster data transfer speeds with shorter range compared to 2.4 GHz
    - Contains frequencies from 5.7 GHz to 5.875 GHz, providing up to 24 non-overlapping channels
    - *Channel Bonding*
      - Creates a wider channel by merging two or more neighboring channels into a single wider channel
      - Increases bandwidth but becomes more susceptibility to interference due to increased channel widths
  - ○ 6 GHz Band
    - Newest spectrum for wireless networking, offering more channels and bandwidth
    - Frequencies range from 5.925 GHz to 7.125 GHz, providing faster connections with less congestion
    - Allows for channels of 20, 40, 80, or 160 MHz in width, accommodating up to 59 channels.

- Government Regulations and Standards
  - Government allocates portions of the wireless spectrum for wireless networks, with regulations varying globally
  - 802.11h Standard
    - Developed to comply with European regulations
    - *Dynamic Frequency Selection (DFS)*
      - Requires devices to actively monitor the environment for radar signals
    - *Transmit Power Control (TPC)*
      - Allows devices to adjust their transmitting power to the minimum required for maintaining a good quality connection
  - *Band Steering*
    - Technology that optimizes the distribution of client devices across different frequency bands
    - Relevant for environments where two or more frequency bands are being utilized
    - Can result in more efficient use of available bandwidth
- Comparative Analysis of Frequency Bands
  - 2.4 GHz – slower speeds but greater coverage
  - 5 GHz – faster speeds with shorter range and increased susceptibility to interference with wider channels

■ 6 GHz – fastest speeds but shortest distances and less solid object penetration

- **802.11 Standards**
  - *IEEE 802.11 Standard*
    - Defines technologies for wireless local area network (WLAN) communication
    - Evolved over time to meet demands for faster data transfer speeds and more reliable networks
  - Wireless a (802.11a)
    - Frequency band – 5 GHz
    - Speed – up to 54 Mbps
    - Range – around 35 meters
    - Introduced in the late 1990s, mainly used by business users due to cost
  - Wireless b (802.11b)
    - Frequency band – 2.4 GHz
    - Speed – initially 11 Mbps
    - Range – about 140 meters
    - Developed to be cheaper and more accessible than Wireless a, leading to widespread adoption
  - Wireless g (802.11g)
    - Frequency band – 2.4 GHz

- ■ Speed – up to 54 Mbps

- ■ Range – around 140 meters

- ■ Offers similar speed and range as Wireless a but utilizes cheaper frequency bands

- ○ Wireless n (802.11n/Wi-Fi 4)

    - ■ Frequency band

        - ● 5 GHz

            - ○ Speed – up to 600 Mbps

            - ○ Range – about 35 meters

        - ● 2.4 GHz

            - ○ Speed – up to 300 Mbps

            - ○ Range – upt to 70 meters

    - ■ Introduced to meet demands for faster networking speeds

    - ■ *Multiple-Input Multiple-Output (MIMO)*

        - ● Technology that allows access point to use multiple antennas to send and receive data at faster speeds than it could with a single antenna

        - ● Acts like a hub

- ○ Wireless ac (802.11ac/Wi-Fi 5)

    - ■ Frequency band – 5 GHz

    - ■ Speed – up to 6.9 Gbps or more

    - ■ *Multiple-User Multiple-Input Multiple-Output (MU-MIMO)*

- Multipath wireless communication technology that allows multiple users to access the wireless network and access the access point at the same time
- Acts like a switch
○ Wireless ax (802.11ax/Wi-Fi 6)
  ■ Frequency band – <u>2.4 GHz, 5 GHz, and 6 GHz</u> (Wi-Fi 6e)
  ■ Speed – up to 9.6 Gbps
  ■ Utilizes MU-MIMO technology for enhanced simultaneous user access
  ■ Fully backwards compatible with previous standards
○ <u>Important Exam Points</u>
  ■ <u>Supported frequencies</u>
    ● 2.4 GHz – b, g, n, and ax
    ● 5 GHz – a, n, ac, or ax
    ● 6 GHz – ax
  ■ Higher speeds often come with reduced coverage distances for a single access point
  ■ Check considerations for compatibility and frequency bands in troubleshooting scenarios
  ■ Caution against relying on marketing materials for exam answers
  ■ Stick to official standards

- **Wireless Security**
  - Wireless networks
    - Offer convenience but pose security risks due to easy access within signal range
    - Proper authentication and encryption are crucial for network security
  - Authentication Mechanisms
    - *Pre-Shared Key (PSK)*
      - Shared key between access point and client devices, typically a string of characters
      - Challenges with Pre-Shared Key:
        - Scalability issues in large environments
        - Lack of individual user accountability
        - Not practical for large office settings due to shared key usage
    - *Enterprise Authentication*
      - Utilizes individual user credentials managed by an authentication server (e.g., RADIUS)
      - *802.1X Authentication System*
        - Most widely-used enterprise-grade authentication method
        - Relies on authentication server (e.g., RADIUS) for managing user credentials

- - ○ Provides individual user authentication and better security protocols
  - ○ Wireless Security and Encryption Options
    - ■ *Wired Equivalent Privacy (WEP)*
      - ● Original wireless security standard introduced in 1999, which is insecure due to weak encryption and vulnerabilities
      - ● Relies on a pre-shared key
        - ○ 40-bit
        - ○ 64-bit
        - ○ 128-bit
      - ● Utilizes the Rivest Cipher 4 (RC4) encryption mechanism, which is weak
      - ● *Initialization Vector (IV)*
        - ○ 24-bit sent in plain text
        - ○ Vulnerability in WEP allows attackers to reverse engineer encryption keys
      - ● Capture of enough initialization vectors enables attackers to crack WEP encryption in a few minutes using tools like Aircrack-ng.
    - ■ *Wi-Fi Protected Access (WPA)*
      - ● Developed as a replacement for WEP to address IV vulnerabilities
      - ● Utilizes Temporal Key Integrity Protocol (TKIP) instead of Initialization Vectors (IV) to enhance security

- ○ *Temporal Key Integrity Protocol (TKIP)*
    - ■ A new type of vector that uses a longer 48-bit vector compared to WEP's IV
- Employs RC4 encryption like WEP but introduces additional features for enhanced security
    - ○ *Message Integrity Check (MIC)*
        - ■ Integrity checking to prevent On-path attacks
        - ■ Hashes data before transmission to verify integrity during transfer
    - ○ *Enterprise Mode*
        - ■ Function for individual authentication using unique usernames and passwords via an authentication server (e.g., RADIUS)
        - ■ Stronger encryption methods
        - ■ Better scalability
        - ■ Centralized key management
- ■ *Wi-Fi Protected Access 2 (WPA2)*
    - Replaced WPA due to vulnerabilities, introduced in 2004 as part of the 802.11i standard
    - Offers stronger integrity checking, better encryption, and improved authentication

- *CCMP*
  - Countermode with Cipher Blockchaining Message Authentication Code Protocol for enhanced security
  - Combines message integrity checks with comprehensive encryption protocols for confidentiality and integrity assurance
- *Advanced Encryption Standard (AES)*
  - Replaced the less secure RC4 encryption algorithm
  - 128-bit
    - Most WPA2 networks use for security and confidentiality
  - 192-bit
  - 256-bit
- Personal mode – with pre-shared key, common in home or small office networks
- Enterprise mode – preferred for larger environments, utilizing centralized authentication servers for user validation

- *Wi-Fi Protected Access 3 (WPA3)*
  - Introduced in 2018, improves upon WPA2 with enhanced features
  - *Simultaneous Authentication of Equals (SAE)*
    - Security protocol designed to enhance the handshake process used in wifi authentication

- ○ Replaces pre-shared key methods with a more secure authentication mechanism based on the Dragonfly key exchange
- ○ Ensures secure initial key exchange between client and access point, preventing interception by attackers
- ○ Slows down brute force attacks by requiring active interaction with the access point for each password attempt
- ○ Offers forward secrecy, ensuring past communications remain securely encrypted if a session key is compromised

- ■ *Wi-Fi Protected Setup (WPS)*
  - ● Simplifies secure network setup using a PIN or push button
  - ● Vulnerable to brute force attacks due to PIN vulnerability
  - ● Recommended to disable WPS for higher security

- ○ Key Tips for Exam
  - ■ Open networks – no security measures
  - ■ WEP – Initialization Vector (IV) vulnerabilities
  - ■ WPA – linked with TKIP and RC4 encryption
  - ■ WPA2 – uses CCMP for integrity and AES for encryption
  - ■ WPA3 – introduces SAE and dragonfly key exchange
  - ■ WPS – involves push-button configuration but should be disabled for security

■ Pre-shared key – personal mode authentication

■ Enterprise mode – individual user authentication via centralized server (e.g., RADIUS with 802.1X)

● **Understanding Wireless Security: Demonstration**

● **When Wireless Security Fails: Demonstration**

● **Captive Portals**
  ○ *Captive Portals*
    ■ Captive portals are webpages used in modern wireless networks for guest access
    ■ Commonly found in public networks like hotels, airports, coffee shops, and business guest networks
    ■ Functions by intercepting user's network connection then redirecting to a special webpage
      ● Authentication – verify user's access rights through login credentials
      ● Policy acceptance – users agree to terms of service or usage policies
      ● Data collection – collect user data like email addresses for marketing

- ○ Usage Scenarios

  - ■ Guest networks

    - ● Separate access points for visitors without access to the main network

  - ■ Enhance security

    - ● Control network access and track usage

  - ■ Branding opportunity

    - ● Customize login page with business logo and information

- ○ Design Considerations

  - ■ User experience

    - ● Ensure easy navigation and clear instructions

  - ■ Compliance

    - ● Comply with data protection laws (e.g., GDPR)

  - ■ Compatibility testing

    - ● Ensure functionality across various devices and browsers

- ○ Key Points

  - ■ Crucial for public and guest wireless networks

  - ■ Balances user access and network security

  - ■ Enhances user experience and aids in legal compliance

  - ■ Requires careful consideration of design, security, and compliance aspects

Ethernet Switching

Objectives:

- 1.2 - Compare and contrast networking appliances, applications, and functions
- 2.2 - Given a scenario, configure switching technologies and features
- 4.3 - Given a scenario, apply network security features, defense techniques, and solutions

- **Ethernet Fundamentals**
  - Introduction to Ethernet
    - Early computer networks lacked standardization, leading to various competing technologies
    - Ethernet emerged as the dominant protocol for Layer 2 communication in local area networks (LANs)
  - Evolution of Ethernet
    - Originally, Ethernet used coaxial cables with BNC connectors and vampire tabs (10Base2 and 10Base5)
    - Transitioned to 10Base-T Ethernet
      - Utilizes twisted pair cables (Cat 3)
      - 10 Megabits per second (Mbps) speed, significant at the time (1980s)
      - Covers distance of up to 100 meters only

- ○ Deterministic vs. Contention-based Access

  - ■ *Deterministic Access*

    - ● Organized and orderly access (e.g., Token Ring)

  - ■ *Contention-based Access*

    - ● Chaotic, but more efficient use of bandwidth (e.g., Ethernet)

- ○ *Carrier Sense Multiple Access with Collision Detection (CSMA/CD)*

  - ■ Allows devices to detect collisions and manage network access

  - ■ *Carrier Sensing (CS)*

    - ● Devices listen for existing transmissions

    - ● *Carrier*

      - ○ Refers to the signal that carries information or data in electronics

  - ■ *Multiple Access (MA)*

    - ● Many devices can access the network simultaneously

  - ■ *Collision Detection (CD)*

    - ● Devices detect and handle collisions

    - ● *Random Back-off Timer*

      - ○ Devices involved in collisions pause, then select random back-off times before retransmitting

      - ○ Allows two devices to attempt to retransmit again when the timer hits zero

      - ○ Avoids simultaneous retransmissions, reducing collisions

- ○ *Collision Domain*

    - ■ Area where collisions can occur

- ○ Ethernet Switches

    - ■ Break networks into smaller collision domains, improving efficiency

    - ■ Each switch port is its collision domain, allowing full-duplex communication

- ○ Key Takeaways

    - ■ Ethernet is the primary Layer 2 protocol for modern networks

    - ■ Switches are preferred over hubs for efficient network management

- **Network Devices**

    - ○ Hubs

        - ■ Layer 1 device

        - ■ Known as multi-port repeaters

        - ■ Types:

            - ● Passive – repeats signal without amplification

            - ● Active – boosts signal to overcome cable length limitations

            - ● Smart – active hub with enhanced features like SNMP for remote configuration

        - ■ Connect collision domains, making them bigger

    - ○ Bridges

        - ■ Layer 2 device

- Analyzes source MAC addresses to populate MAC address table

- Makes forwarding decisions based on destination MAC addresses

- Breaks up collision domains and adds security and efficiency to networks

○ Switches

- Layer 2 device

- Modern alternative to hubs, known as multiport bridge

- Each port acts as a separate collision domain

- Learns MAC addresses and makes forwarding decisions based on MAC
  tables

- Efficiently manages traffic, reduces collisions, and improves security

- Full duplex support allows simultaneous communication without
  interference

○ Routers

- Layer 3 device

- Operate based on IP addresses

- Connect dissimilar networks and makes routing decisions

- Separates broadcast domains, enhances network efficiency

- Support various interface types for versatile connectivity

○ Layer 3 Switches (Multilayer Switches)

- Combine functions of switches and routers

- Operate at Layer 3 like routers, with each port as a broadcast domain

- ■ Efficient for internal networks but less effective for large-scale routing operations
  - ○ Exam Tips
    - ■ Switches – Layer 2 devices focused on MAC addresses unless specified as multilayer or Layer 3 switches
    - ■ Routers – considered Layer 3 devices focused on IP addresses
    - ■ If the exam question mentions multilayer or Layer 3 switch, treat it like a router

- **Understanding Network Devices: Demonstration**

- **Virtual Local Area Network (VLAN)**
  - ○ *Virtual Local Area Network (VLAN)*
    - ■ Logical subdivision of a network that <u>segments it into separate broadcast domains</u>
    - ■ Unlike traditional LANs, VLANs group hosts together regardless of physical connections
    - ■ Achieved through software rather than hardware and cabling
    - ■ Benefits:
      - ● Flexibility in network configuration
      - ● Efficient resource allocation and management

- ○ Traditional LAN vs. VLAN

  - ■ Before VLANs, separate network segments required additional routers, cables, and switches

  - ■ VLANs reduce hardware requirements by allowing different logical networks to share the same physical hardware

- ○ How VLANs Work

  - ■ Operate at Layer 2 (Data Link Layer) of the OSI model

  - ■ Switches tag each data frame with a VLAN identifier (ID) as it passes through, defining its VLAN

  - ■ *Tags*

    - ● Used to determine the path of frames, ensuring they stay within their VLAN

- ○ <u>Reasons for Using VLANs</u>

  - ■ Enhanced Security

    - ● Isolate sensitive data, reduce data breach risks

  - ■ Improved Performance

    - ● Reduce broadcast domain size, decrease unnecessary traffic

  - ■ Increased Management

    - ● Easier policy implementation, troubleshooting

  - ■ Cost Efficiency

    - ● Utilize existing infrastructure more effectively, reduce hardware requirements

- ○ <u>VLAN Database</u>
    - ■ Contains VLAN configurations for switches
        - ● Identifier
        - ● Name
        - ● MTU size
    - ■ Cisco Switch
        - ● VLAN.DAT
            - ○ Ensures consistent VLAN configurations and easy deployment across the network
- ○ *Switch Virtual Interface (SVI)*
    - ■ Virtual interface on a switch providing Layer 3 processing for VLANs
    - ■ Allows routing between VLANs without the need for a separate router
    - ■ Enhances network efficiency by minimizing additional routing devices

- **VLAN Configuration**
    - ○ Virtual Local Area Network (VLAN)
        - ■ Offers flexibility, performance, and security in network design
        - ■ Proper configuration is essential
    - ○ *802.1Q Tagging*
        - ■ Refers to IEEE standard that facilitates the management of multiple VLANs on a single network
        - ■ Essential for VLAN configurations

■ Inserts VLAN tags into Ethernet frames

● Tags contain VLAN identifiers (VIDs) for switch identification and forwarding

● *Trunking*

○ Transmission of traffic from different VLANs across the same physical network infrastructure while keeping that traffic from each VLAN separate and secure

○ *Native VLAN*

■ One VLAN on a trunk port that does not get tagged with VID

■ Default VLAN for untagged frames

■ Used for devices that do not support VLAN tagging

■ Should be consistently configured across interconnected switches to avoid misrouting

○ *Voice VLAN*

■ Dedicated VLAN for voice traffic (VoIP)

■ Ensures quality and reliability of voice communications by segregating voice traffic

■ Enables the application of quality of service (QoS) policies for better voice call quality

○ *Link Aggregation*

■ Also known as port channeling/bonding, <u>combines multiple network connections into a single logical link</u>

- Enhances bandwidth capacity and provides redundancy for network availability
- Commonly used for trunking lines between switches and for high-speed connectivity in data centers
  - *Speed and Duplex Configurations*
    - Settings that determine the <u>rate</u> at which data is transmitted and the <u>mode of communication</u> between the network devices
    - *Speed*
      - Refers to the rate of data transfer (Mbps or Gbps)
    - *Duplex*
      - Refers to how data is sent
      - Half duplex
        - Device can either send or receive data, but cannot do both at the same time
      - Full duplex
        - Allows device to send and receive data simultaneously
    - Misconfigurations can significantly impact network performance and throughput
  - Configuration Best Practices
    - *Auto-negotiation*
      - commonly used when devices automatically select the highest performance settings that they have in common

■ Consider manual configurations for specific requirements

● **Understanding VLANs Demonstration**

● **Spanning Tree Protocol (STP)**
  ○ *Spanning Tree Protocol (STP)*
    ■ Additional Ethernet feature for preventing loops in network traffic
    ■ Known as 802.1d
  ○ Importance of STP
    ■ Enables redundant links between switches
    ■ Prevents broadcast storms and ensures network availability
  ○ Network Without STP
    ■ Can lead to switching loops and broadcast storms
      ● *Broadcast Storm*
        ○ Multiple copies of frames being forwarded back and forth which then consumes the network
  ○ STP Functionality
    ■ Uses a root bridge and non-root bridges
      ● *Root bridge*
        ○ Where a switch is elected to act as a reference point for the entire spanning tree
        ○ Elects root bridge based on lowest Bridge ID (BID)

- - - ■ *Bridge ID (BID)*
      - Made up of a priority value and a MAC address, with the lowest value being considered the root bridge
    - *Non-root bridge*
      - Every other switch on the STP topology
  - STP Port Types
    - Root port
      - Every non-root port has a single root port, closest to root bridge in terms of cost
      - If cost is determined based on cable types:
        - The lowest port number on the switch will be chosen
        - Faster cables – lower cost
        - Slower cables – higher cost
    - Designated port
      - On every network segment, closest to root bridge in terms of cost
      - All ports on root bridge
    - Non-designated port
      - Blocks traffic to prevent loops
  - STP Port States
    - Blocking
      - Stops forwarding frames

- - - ■ Listening

        - Learns MAC addresses but does not forward frames

    - ■ Learning

        - Processes BPDU and determines role in spanning tree

    - ■ Forwarding

        - Forwards frames as designated or root port

  - ○ Link Cost

    - ■ Associated with link speed

        - Lower speed – Higher cost

        - Higher speed – Lower cost

- **Network Access Control**

  - ○ *Network Access Control (NAC)*

    - ■ A method for increasing the security of a given network by inspecting devices as they try to connect to the network to determine if they're secure enough to be granted access

  - ○ NAC Process

    - ■ Devices present themselves for inspection when connecting to the network

    - ■ Devices are isolated and inspected based on NAC configurations

- ■ Inspection process:
  - ● *Port Security*
    - ○ Secures physical network ports to prevent unauthorized access
    - ○ Limits the number of devices that can connect to a network switch or hub
    - ○ Can be configured to allow specific MAC addresses or a set of specified MAC addresses
  - ● *MAC Filtering*
    - ○ Controls access to the network based on devices' unique MAC addresses
    - ○ Maintains a list of approved MAC addresses
      - ■ Allow listing
        - ● Only approved MAC addresses allowed
      - ■ Block listing
        - ● All devices allowed except those on the list
- ■ *802.1X Authentication*
  - ● Provides an authentication framework for networks
  - ● Ensures only authenticated users can access network services
  - ● Encapsulates the Extensible Authentication Protocol (EAP) within networks frames to enable more robust authentication mechanisms

- Three components
    - Supplicant – user device
    - Authenticator – network device
    - Authentication server – authenticates user device
  - Implementation
    - Can be used in conjunction with port security, MAC filtering, and 802.1X authentication
    - Persistent agent
      - For company-provided computers
    - Non-persistent agents
      - For personally owned devices
      - Use captive portals
    - Devices that fail inspection are either denied access or placed in a quarantine zone for further remediation
  - Advanced NAC Features
    - Time-based Access Control
      - Limits network access based on specified hours
    - Location-based Access Control
      - Verifies the physical location of the device
    - Role-based Access Control
      - Grants permissions based on user roles

- Rule-based Access Control

- Grants or denies access based on predefined rules

○ Benefits

- Strengthen network security by ensuring only authenticated devices can access the network

- Provide a scalable solution for modern and diverse network infrastructures

- **Maximum Transmission Unit**

  ○ *Maximum Transmission Unit (MTU)*

    - Refers to the largest size of a frame that can be set over a network

    - Measured in bytes, dictates data transmission capacity

    - Analogous to maximum load capacity for frames within a network

  ○ Impact of MTU on Network Performance

    - Properly configured MTU ensures optimal data packet and frame size

      - Enhances network performance and efficiency

    - MTU too high – packet loss and retransmission

    - MTU too low – increased overhead and slow network

  ○ MTU Configuration

    - Wired Ethernet

      - Standard MTU size is 1500 bytes for efficiency and compatibility

- Wireless Networks

  - <u>Smaller MTU size</u> due to instability and higher error rates

- VPN and PPPoE Connections

  - <u>Require smaller MTU</u> due to encapsulation overhead

  - Recommended size – <u>1400 to 1420 bytes</u>

- *Jumbo Frames*

  - Frames exceeding standard 1500 bytes

  - Typically configured at <u>9000 bytes</u>

  - Beneficial for high bandwidth applications but require careful configuration

  - Challenges and considerations:

    - Not all network equipment supports jumbo frames

    - Fragmentation may occur if encountering smaller MTU devices

    - Limited support in traditional network troubleshooting tools

    - Consistent configuration across all network devices necessary

IP Addressing

Objectives:

- 1.5 - Compare and contrast transmission media and transceivers

- 1.7 - Given a scenario, use appropriate IPv4 network addressing

- 1.8 - Summarize evolving use cases for modern network environments

- **Introduction**

    - *Internet Protocol (IP) Address*

        - An assigned numerical label that is used to identify Internet communicating devices on a computer network

        - Used in Layer 3 addressing

            - Between two different networks or subnets

- **IPv4 Addressing**

    - *Internet Protocol version 4 (IPv4) Addressing*

        - <u>Most common</u> type of IP addressing used in networks

    - IPv4 Address

        - Decimal representations of a 32 bit binary number

        - Written in Dotted-decimal Notation which is a series of four decimal numbers separated by dots

- *Octets*
  - Refers to the four decimal numbers, individually
  - IPv4 address consists of four octets, each representing 8 bits of a binary number, totaling 32 bits
  - Decimal numbers ranging from 0 to 255,
- *Network and Host Portion*
  - Portions of IPv4 that is determined by a subnet mask
  - *Subnet Mask*
    - Contains continuous strings of ones (1) and zeros (0)
  - Network portion – 1
  - Host portion – 0
- Classes of IPv4 Addresses
  - <u>IP addresses are classified into classes</u> depending on the first octet in their address
  - A
    - First octet – 1 to 127
    - Default subnet mask – 255.0.0.0
  - B
    - First octet – 128 to 191
    - Default subnet mask – 255.255.0.0
  - C
    - First octet – 192 to 223

- - - Default subnet mask – 255.255.255.0
  - ■ D
    - - First octet – 224 to 239
    - - No default subnet mask
    - - Reserved for multicast routing
      - ○ *Multicast Address*
        - ■ A logical identifier for a group of hosts
  - ■ E
    - - First octet – 240 to 255
    - - No default subnet mask
    - - Reserved for experimental use in terms of research and development
- ○ *Subnetting*
  - ■ The process of dividing a larger network into smaller subnetworks
  - ■ *Classful Subnet Mask*
    - - <u>Uses default masks</u> associated with specific address classes
  - ■ *Classless Subnet Mask*
    - - <u>Uses any subnet mask that is not the default</u> for a specific address class

- *Classless Inter-Domain Routing (CIDR)*
    - The process of borrowing bits from the host portion to expand the network portion, allowing for smaller subnetworks (Classless Subnet Mask)
- *CIDR Notation*
    - Combined notation of IP addresses and subnet masks (e.g., IP/subnet)
    - Default CIDR notations for IP address classes to be considered classful:
        - A – /8
        - B – /16
        - C – /24

- **IPv4 Address Types**
    - Public IPV4 Address
        - Also known as routable IP address
        - Unique identifier assigned to devices on the internet
        - Must be leased or purchased from Internet Service Providers (ISPs)
        - Globally, managed by Internet Corporation for Assigned Names and Numbers (ICANN)

- *Regional Internet Registries (RIRs)*
    - Responsible for managing public IP addresses for different regions
    - ARIN – North America
    - LACNIC – Latin America
    - AFNIC – Africa
    - APNIC – Asia Pacific
    - RIPE – Europe
- Private IPV4 Address
    - Non-internet routable IP address used within local networks
    - Allows communication between devices within the network without using a public IP address
    - Can be used by anyone at any time, but only within their own LANs
    - *Network Address Translation (NAT)*
        - Method used to translate private IP addresses into public IP addresses and vice versa
        - Facilitates communication between local and public networks
        - Helps conserve global IP address space
    - *Request for Comments (RFCs)*
        - A formal publication from the Internet Engineering Task Force (IETF)

- Authored by individuals or groups of computer scientists who want to document new technologies or standards that they are proposing
- RFC 1918
  - Defines ranges for the private IP addresses
  - Private IP Ranges
    - Class A – 10.x.x.x (e.g., 10.0.0.0 - 10.255.255.255)
    - Class B – 172.16.x.x to 172.31.x.x (e.g., 172.16.0.0 - 172.31.255.255)
    - Class C – 192.168.x.x (e.g., 192.168.0.0 - 192.168.255.255)
  - *Loopback Address (Local Host)*
    - Specialized IP address assigned as 127.0.0.1
    - Used for any higher level protocol can send data back to the host itself without going out to a switch or router
      - Internal testing and troubleshooting
    - Entire 127.x.x.x range reserved for loopback purposes
      - Almost always written as 127.0.0.1
      - Other IP addresses inside 127.x.x.x are wasted as part of loopback or local host range
    - Local Host – the human readable name for the IP address 127.x.x.1

- ○ Automatic Private IP Address (APIPA)

  - ■ Dynamically assigned by OS <u>when DHCP server is unavailable</u>

  - ■ Range – 169.254.0.0 to 169.254.255.255 (<u>169.254.x.x</u>)

  - ■ Used as a<u> fallback for network configurations</u>

  - ■ <u>Indicates a DHCP issue</u> if assigned to a device

  - ■ *Dynamic Host Configuration Protocol (DHCP)*

    - ● Assigns dynamic IP addresses to devices

    - ● Process – DORA

      - ○ Discovery

      - ○ Offer

      - ○ Request

      - ○ Acknowledgment

- ○ <u>Exam Tips</u>

  - ■ Understand distinctions between public and private IP addresses

  - ■ Memorize ranges for private IP addresses (RFC 1918)

  - ■ Be aware of loopback/local host, and APIPA addresses

  - ■ Recognize DHCP issues indicated by APIPA addresses

- **IPv4 Data Flows**

  - ○ *Unicast*

    - ■ Data from single source to single destination

    - ■ Two-way conversation between sender and receiver

- ○ *Multicast*

    - ■ Data from single source to multiple specific destinations

    - ■ Sender communicates with a specific group of receivers

- ○ *Broadcast*

    - ■ Data from single source to all sources on a destination network

    - ■ Sender addresses all devices on the network

- ○ Multicast vs. Broadcast

    - ■ Broadcast – everyone receives the message

    - ■ Multicast – only those who have opted into the multicast group receive the message

- ● **Assigning IPv4 Addresses**

    - ○ *Static Assignment*

        - ■ Manually inputting IP address, subnet mask, default gateway, and DNS server

        - ■ Prone to errors, time-consuming, especially in large networks

    - ○ *Dynamic Assignment*

        - ■ Provides quicker, easier, and less error-prone method

        - ■ Commonly used for large or small networks

        - ■ Utilizes DHCP (Dynamic Host Configuration Protocol) for automatic assignment

- ○ <u>Components of a Fully Configured Client</u>

    - ■ IP address

    - ■ Subnet mask

    - ■ Default gateway (often the router's IP)

    - ■ DNS server (or WINS server in Windows domains)

        - ● *DNS (Domain Name System)*

            - ○ Converts domain names to IP addresses for internet communication

            - ○ Acts like an internet phone book

        - ● *WINS (Windows Internet Name Service)*

            - ○ Identifies NetBIOS systems on a TCP/IP network and converts those NetBIOS names to IP addresses

            - ○ Works similar to DNS but within Windows domain environment

- ○ Methods of Dynamic Assignment

    - ■ *BOOTP (Bootstrap Protocol)*

        - ● Older and least used method, which is originally for diskless Unix workstations

        - ● Dynamically assigns IP addresses and allows a workstation to load a copy of the boot image over the network

        - ● Uses static database of IP and MAC addresses

- *DHCP (Dynamic Host Configuration Protocol)*
  - <u>Modern replacement for BOOTP</u>
  - <u>Dynamically assigns IPs</u> based on assignable scope and allows configuration of numerous options with it
  - <u>Gives all of the variables including the components of a fully configured client</u>
- *APIPA (Automatic Private Internet Protocol Addressing)*
  - Used if DHCP fails
  - Assigns self-assigned IPs
  - Allows a quick configuration of a LAN without the need for a DHCP server
  - Uses private IP addresses that cannot be routed outside LAN
  - Cannot communicate with non-APIPA devices
- ZeroConf
  - Newer technology based on APIPA, providing the same features and some new ones
  - Features:
    - Assigns IPv4 link local addresses
    - Utilizes MDNS (Multicast Domain Name Service) for name resolution without DNS
    - Enables service discovery on the network

- Implementations:
    - Apple Products
        - Known as Bonjour
        - Used for service discovery
    - Microsoft Windows
        - LLMNR (Link Local Multicast Name Resolution)
        - Extends APIPA for name resolution and service discovery
    - Linux
        - Implemented using SystemD, specifically the SystemD Resolved background service

- **Computer Mathematics**
    - Number Systems
        - Computers use binary (base-2) numbering
        - Humans typically use decimal (base-10) numbering
    - Binary to Decimal Conversion
        - Binary numbers are converted to decimal by summing the powers of 2 for each digit

- ■ Example: Converting 10010110 to decimal

    - ● Each digit represents a power of 2, starting from 2^0

        - ○ Table:

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

    - ● 1 indicates presence and 0 indicates absence

    - ● Sum up the values of all positions with 1

        - ○ 128+16+4+2 = 150 – decimal

- ○ Decimal to Binary Conversion

    - ■ Decimal numbers are converted to binary by repeatedly dividing by 2 and noting remainders

    - ■ Example: Converting 167 to binary

        - ● Subtract highest power of 2 possible, repeating until remainder is 0

        - ● Each subtraction corresponds to placing a 1 or 0 in the binary representation

            - ○ 167-128 = 39 – 1

            - ○ 39-64 = x – 0

            - ○ 39-32 = 7 – 1

- ○ 7-16 = x – 0
- ○ 7-8 = x – 0
- ○ 7-4 = 3 – 1
- ○ 3-2 = 1 – 1
- ○ 1-1 = 0 – 1
- ○ Table:

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

- • 10100111 – binary of 167
- ○ Conversion Verification
    - ■ To ensure accuracy, check the result by reversing the conversion process
    - ■ Add up the decimal values corresponding to the 1s in the binary representation
    - ■ Verify that the sum matches the original decimal number
    - ■ Example: 10100111 – binary of 167
        - • 128+32+4+2+1 = 167

- **Subnetting**
  - *Subnetting*
    - Involves dividing a large network into smaller networks for better management and optimization
    - It's crucial for efficient use of IP addresses, both public and private
  - *Subnet Masks*
    - Modify network sizes by borrowing bits from the host portion and adding them to the network portion
    - Default classful subnet masks are rarely optimal for network sizes, so custom subnet masks are used for better efficiency
  - Subnetting Formulas
    - Number of Subnets
      - 2^S
      - S is the number of borrowed bits
    - Assignable IP Addresses per Subnet
      - $2^h - 2$
      - h is the number of host bits
      - "– 2" represents network ID (first) and broadcast ID (last) that need to be taken away when calculating the number of usable IPs
  - Classful vs. Subnetted Networks
    - Classful networks (e.g., /8, /16, /24) have fixed sizes

- - Subnetted networks allow flexibility in network size by borrowing bits from the host portion
  - *CIDR (Classless Inter-Domain Routing) Notation*
    - Provides a shorthand for expressing subnet masks
    - Consolidates multiple subnets under a single route for more efficient routing
  - *Variable Length Subnet Mask (VLSM)*
    - Allows subnets of various sizes to be used within a larger network
    - Enhances flexibility in subnetting by accommodating different network requirements
  - Exam Tips
    - Memorize the chart correlating subnet mask notation (/24, /25, etc.) with the number of subnets and assignable IP addresses
    - Helps quickly answer subnetting questions by understanding the relationship between subnet size and IP allocation
    - Practice subnetting problems, especially in the Class C range (/24 to /30)
    - Familiarize yourself with CIDR notation and subnetting calculations to excel in subnetting questions on exams

- **Subnetting Practice**
  - *Subnetting*
    - Involves dividing a larger network into smaller, manageable sub-networks

- CIDR Notation

    - Commonly used to represent subnets

    - Expressed as IP address followed by a slash and a number indicating the subnet mask length

- Memory Aid

    - <u>Memorize a subnetting chart for quick reference during exams</u>

    - <u>Utilize a "dump sheet" to jot down important information during the test</u>

- Problem Solving Approach

    - Begin by identifying the total number of IPs available in the given subnet

    - Determine the required subnet sizes for different departments

    - Remember to account for network address and broadcast address in each subnet

    - Consider rounding up department sizes to factors of 2 for efficient allocation

- Practice Problem 1

    - 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.

- Process:
    - Identify the number of users in each department: IT, instructors, sales, administration
    - Round up the department sizes to the nearest power of 2 (1, 2, 4, 8, 16, 32, 64, 128)
    - Account for network address and broadcast address in each subnet
        - For IT
            - 54 users
            - Round up to 64
            - CIDR notation: /26
        - For instructors
            - 32 users
            - Round up to 64
            - CIDR notation: /26
        - For sales
            - 5 users
            - Round up to 8

- - ■ CIDR notation: /29
  - ○ For administration
    - ■ 3 users
    - ■ Round up to 8
    - ■ CIDR notation: /29
- Calculate the remaining unused IPs by subtracting allocated IPs from the total (given as /24 in this case)
- Round down the remaining IPs to the nearest power of 2
- Determine CIDR notation for each subnet based on rounded values
- Assign CIDR notation to each department's subnet accordingly
  - ○ For unused
    - ■ 112 IPs left
    - ■ Round down to 64
    - ■ CIDR notation: /26
- Sales and administration both have 8 IPs → CIDR notation: /29 for both
- <u>Use the subnetting chart for quick reference</u>

- ○ Practice Problem 2

  - ■ How many assignable IP addresses exist in this network?

    172.16.1.0/27

    A. 30

    B. 32

    C. 14

    D. 64

  - ■ Explanation:

    - ● Total IPs for /27: 32

    - ● Assignable IPs (excluding network and broadcast): 30

- ○ Practice Problem 3

  - ■ How many assignable IP addresses exist in this network?

    192.168.1.0/28

    A. 30

    B. 16

    C. 14

    D. 64

  - ■ Explanation:

    - ● Total IPs for /28: 16

    - ● Assignable IPs: 16 - 2 = 14

- ○ General Tips
    - ■ Pay attention to whether the question asks for assignable, usable, or total IPs
    - ■ Use subnetting formulas ($2^h - 2$) if needed, where h represents the number of host bits
    - ■ Practice with a subnetting chart and understand how to apply CIDR notation effectively

- **Subnetting by Hand: Demonstration**

- **IPv6 Addressing**
    - ○ IPv4 Limitations
        - ■ Limited address space of only 32 bits of addressable space
        - ■ Approximately 4.3 billion addresses
        - ■ Address exhaustion due to waste and subnetting
    - ○ IPv6 Advantages
        - ■ 128-bit addresses
        - ■ 340 undecillion addresses
        - ■ Solved address exhaustion problem
    - ○ IPv6 Features
        - ■ No broadcasts
        - ■ No packet fragmentation

- - ■ Simplified header with only 5 fields

    - ■ No maximum transmission units (MTUs) for discovery

  - ○ IPv6 Address Notation

    - ■ <u>Hexadecimal Notation</u>

      - ● 16 possible characters

      - ● Represented in segments of 4 hexadecimal digits, separated by colons

      - ● 0-9, A-F

        - ○ F can represent 10-15

    - ■ <u>No more than 32 hexadecimal digits</u>

      - ● Use of shorthand notation to shorten addresses

        - ○ Four consecutive zeros can be represented by one zero

        - ○ Double colon (::) can summarize multiple segments that have just zeros but it can only be once within an address

        - ○ Eliminate leading zeros within segments

  - ○ Identifying IPv6 Addresses

    - ■ IPv4 – Dotted decimal notation (0-255)

    - ■ IPv6 – Hexadecimal digits (0-9, A-F) with colons, in groups of four

    - ■ MAC – always have 12 hexadecimal digits, separated by colons, and grouped in pairs of two

- ○ IPv6 Address Types
    - ■ A single interface can be assigned to multiple IPv6 addresses
        - ● Can be a mixture of address types
    - ■ *Unicast*
        - ● Identifies a single interface
            - ○ Globally routed unicast addresses
                - ■ Similar as in IPv4
                - ■ 2000-3999
                - ■ First segment in IPv6 address
            - ○ Link local addresses
                - ■ Like a private IP in IPv4 that can only be used in LAN
                - ■ Begins with FE80 as first segment
    - ■ *Multicast*
        - ● Identifies a group of interfaces
        - ● Starts with FF as the first two digits within the first segment
    - ■ *Anycast*
        - ● Identifies a set of interfaces
        - ● Allocated from unicast space
- ○ *Stateless Address Autoconfiguration (SLAAC)*
    - ■ An Auto-configuration that eliminates the need to obtain addresses or other configuration information from a central server

- Utilizes MAC addresses to create unique identifiers
- *Extended Unique Identifier (EUI)*
  - Allows a host to assign itself a unique 64-bit IPv6 interface identifier (EUI-64)
- DHCPv6 can also be used to assign addresses

○ *Neighbor Discovery Protocol (NDP)*
  - Used to determine Layer 2 addresses on the network
  - Functions:
    - Router solicitation
    - Router advertisement
    - Neighbor solicitation
    - Neighbor advertisement
    - Redirection
  - Simplifies network configuration and improves efficiency

- **IPv6 Data Flows**
  ○ Data Flows in IPv6
    - Unicast
      - Similar to IPv4, but uses IPv6 addresses
    - Multicast
      - Uses multicast groups like in IPv4 (e.g., FF00::A)

- Data travels from a single source (server) to multiple specific destination devices
  - *Anycast*
    - Unique to IPv6, replaces broadcast from IPv4
    - Allows one host to efficiently update router tables for a group of other hosts
    - IPv6 determines the closest gateway and sends packets as though it was a unicast communication
    - Routers in the group update their tables, improving efficiency

- **IPv4 and IPv6 Compatibility Requirements**
  - IPv6 was designed to be backward compatible with IPv4
  - Both protocols can co-exist on the same network to facilitate a smooth transition
  - *Dual Stack*
    - A network architecture that allows coexistence and simultaneous operation of IPv4 and IPv6 on the same network
    - Devices are configured to understand and process both IPv4 and IPv6 addresses
    - Enables gradual migration to IPv6 while ensuring compatibility and communication between both protocols

- Preference for IPv6 by default
  - With fallback to IPv4 if IPv6 is not available or supported by the destination
- *Tunneling*
  - Method that enables communication of one network protocol within another by encapsulating packets
  - Crucial for transitioning from IPv4 to IPv6, allowing IPv6 packets to traverse IPv4 infrastructure
  - Encapsulation
    - IPv6 packet will be encapsulated within IPv4 packet at the source or entry point
  - Decapsulation
    - Original IPv6 packet will be deencapsulated at the tunnel's endpoint, and delivered to its intended IPV six destination
    - Tunnel endpoints configuration
      - Static tunnels
      - Dynamic tunnels
  - Enables the secure and transparent transportation of data through an incompatible network
- *NAT64*
  - A network address translation mechanism allowing IPv6-only devices to communicate with IPv4 servers

- Crucial in environments where dual stack configuration is not feasible

- <u>Translates IPv6 addresses into IPv4 addresses and vice versa</u>, facilitating interoperability

- Helps conserve remaining IPv4 addresses by allowing multiple IPv6 devices to share a single IPv4 address

- Utilizes a NAT64 gateway at the edge of the IPv6 network to manage translations seamlessly

Routing

Objectives:

- 1.4 - Explain common networking ports, protocols, services, and traffic types
- 2.1 - Explain characteristics of routing technologies

- **Introduction**
  - *Router*
    - Forwards 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
    - Multlayer switches also perform routing functions
      - Exam Tip: Even if a multilayer switch is being used, it is functioning as a router, so it will be called a router on the exam
        - If the word Switch is used, they are referring to a Layer 2 Switch
        - If the word Multilayer Switch or Router, they are referring to the Layer 3 functionality of a router

- **Routing Fundamentals**
  - *Router*
    - Crucial for connecting subnets within a network or connecting internal and external networks
    - Routes traffic between different subnets or networks
    - Separates broadcast domains, unlike switches which maintain one broadcast domain
    - Layer 3 switches can function as routers, handling both Layer 2 forwarding and Layer 3 routing
      - In the exam, a multi-layer switch is treated as a router
  - For the exam
    - Switch – standard Layer 2 switch
    - Multi-layer switch (router) – Layer 3 device
  - Basic Router Functionality
    - Routers forward traffic between networks based on IP addresses
    - To connect two networks, routers use WAN connections like fiber, serial, satellite, or VPN links
    - When a packet needs to travel between networks, it is forwarded to the router (default gateway)
    - Routers use IP addresses (Layer 3) to route packets between networks
      - MAC addresses are used internally, but IP addresses are used at Layer 3 for communication between routers

- - Routers repackage data frames (Layer 2) as packets (Layer 3) for transmission over the WAN

  - Routers strip off the IP header and convert packets back to data frames for delivery to the destination device on the local network

  - Communication between devices on different networks involves routers forwarding packets based on IP addresses and switches delivering data frames based on MAC addresses

  - Routing becomes more complex when packets are sent over the internet, which is the world's largest WAN

- **Routing Tables**
  - Routing Table
    - Helps determine which route entry is the best fit for the network
    - Used to decide where packets need to go inside and outside of networks
    - Routing decisions are based on Layer 3 information and map to Layer 2
      - ARP Cache
        - Used by routers to map IP addresses to MAC addresses within a local area network
    - Kept by routers to determine the best route for routing traffic
    - Entries in a routing table contain a prefix
      - Longer prefixes indicate more specific networks
      - A longer prefix means fewer available IP addresses in that range

- ○ Routing Information Sources

    - ■ Directly Connected Route

        - ● Learned by a physical connection between routers

    - ■ Static routes

        - ● Configured manually by an administrator

        - ● 0.0.0.0/0

            - ○ Default static route to handle unknown destinations

    - ■ Dynamic route

        - ● Learned through dynamic routing protocols

        - ● Learned by exchanging informations automatically between routers based on the protocols

        - ● Dynamic Routing Protocols

            - ○ Negotiate based on factors like number of hops and link bandwidth

- ○ Preventing Routing Loops

    - ■ *Split Horizon*

        - ● Prevents a route learned on one interface from being advertised back out the same interface

    - ■ *Poison Reverse*

        - ● Advertises a route back out the same interface but with a high cost to prevent its use

- **Routing Protocols**
  - Dynamic Routing Protocols
    - Internal
      - *Interior Gateway Protocol (IGP)*
        - Operates within an autonomous system
    - External
      - *Exterior Gateway Protocol (EGP)*
        - Operates between autonomous systems on exterior networks
  - Routing Protocol Characteristics
    - Router Advertisement Method
      - Distance Vector
        - Sends full routing table to directly connected routers at regular intervals
        - *Convergence Time*
          - Time for all routers to update routing tables in response to topology changes
          - Slow
        - *Hold-down Timer*
          - Prevents updates for a specific period of time and speeds up convergence

- - *Hop Count*
    - Number of routers from the source router through which data must pass to reach the destination network
    - Used as metric for routing decisions
  - Link State
    - Requires all routers to know about the paths that all other routers can reach in the network
    - Faster convergence time compared to distance vector
    - Considers cost, including link speed, as metric for routing decisions
  - Hybrid
    - Combines aspects of both distance vector and link state protocols
- Routing Protocols
  - *RIP (Routing Information Protocol)*
    - An interior gateway protocol that is used internal to the networks
    - Oldest dynamic routing protocol
    - Uses distance vector and hop count
      - 15 max hops
    - Updates every 30 seconds
    - Easy to configure

- Runs over UDP
- *OSPF (Open Shortest Path First)*
    - Another interior gateway protocol
    - Uses link state and cost for routing decisions
        - Cost is based on link speed
    - Faster convergence than RIP
- *IS-IS (Intermediate System to Intermediate System)*
    - An interior gateway protocol similar to OSPF
    - Uses cost based on link speed for routing decisions
    - Functions like OSPF but not as widely popular
- *EIGRP (Enhanced Interior Gateway Routing Protocol)*
    - Advanced distance vector protocol
    - Hybrid of distance vector and link state
    - Uses bandwidth, delay, and cost for routing decisions
    - A Cisco-developed upgrade to OSPF that is popular in Cisco-only networks
- *BGP (Border Gateway Protocol)*
    - An external gateway protocol
    - Uses path vector and autonomous system hops for routing decisions
    - Backbone protocol of the internet
    - Slow convergence time

- **Route Selection**
  - *Route Selection*
    - Traffic across routers determines the path
  - Believability of a Route
    - *Administrative Distance (AD)*
      - An index of believability used by routers
      - Lower value – more believable
      - Administrative Distance of Routing Protocols (for exam understanding, not memorization)
        - Directly connected – 0 (most believable)
        - Static – 1
        - EIGRP – 90
        - OSPF – 110
        - RIP – 120
        - External EIGRP – 170
        - Unknown/Unbelievable – 255 (unreachable)
  - Metrics for Route Selection
    - Factors
      - Hop count
      - Believability
      - Reliability
      - Bandwidth

- Delay

- Costs

- Other metrics

■ Each protocol will use a different metric based on its programming to determine which route to use

■ <u>Lower numbers are better</u>

○ Summary Slide

■ <u>Useful for exam preparation and understanding protocol characteristics</u>

Routing Protocol	Type	Interior/Exterior
RIP	Distance vector	Interior
OSPF	Link state	Interior
EIGRP	Advanced distance vector	Interior
IS-IS	Link state	Interior
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 then translate from one protocol for redistribution as the other protocol.		

- **Address Translation**
  - IPv4 faced address exhaustion, prompting the development of address translation
  - *Address Translation*
    - Allows private IP addresses to be translated into public IP addresses for routing over public networks like the internet
  - *Network Address Translation (NAT)*
    - Conserves limited IPv4 addresses by translating private IPs into public IPs
    - *Dynamic NAT (DNAT)*
      - Automatically assigns IP addresses from a pool of IPs for one-to-one translation
    - *Static NAT (SNAT)*
      - Manually assigns private IPs to public IPs for one-to-one translation
      - Used as security feature
  - *Port Address Translation (PAT)*
    - Allows multiple devices to share a single public IP address by using different port numbers to differentiate traffic
    - Many-to-one translation
  - NAT IP Address Terminology
    - *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
- ○ Comparison of NAT and PAT
  - ■ NAT translates private IPs to public IPs for individual devices
  - ■ PAT uses port numbers to differentiate between multiple devices sharing a single public IP

- ● **Routing Redundancy Protocols**
  - ○ *Routing Redundancy Protocol*
    - ■ A network protocol that prevents disruptions in communication by automatically rerouting data traffic in case of path or device failure
  - ○ *First Hop Redundancy Protocol (FHRP)*
    - ■ Group of protocols ensuring network reliability by providing automatic failover to a backup router if the primary router fails
    - ■ Benefits
      - ● Reliability
        - ○ Ensures communications remain up even if a router fails

- Load Balancing
  - Distributes network traffic across multiple routers to prevent overload
- Seamless Transitions
  - Makes quick and seamless transitions from sending data to one router to another

- Components
  - *Virtual IP*
    - Represents one or more devices
    - Used as default gateway for devices in the network
  - *Subinterface*
    - Allows a single physical interface to be divided into multiple logical interfaces, improving network management and security

- Protocols
  - *Hot Standby Router Protocol (HSRP)*
    - Establishes a fault-tolerant default gateway for devices on a local network segment
    - Enables two or more riders to work together
      - Active router
        - Handles all the networks routing responsibilities

- - ■ Standby router

      - ● Designed to wait to take over when the active router fails

  - ○ *Preempting*

      - ■ Allows a higher priority router to take over as the active router

- ● *Virtual Router Redundancy Protocol (VRRP)*

  - ○ Functions similarly to HSRP but is an <u>open standard</u>

      - ■ Not tied to a specific vendor

  - ○ Enables multiple routers to act as a single virtual router

  - ○ Provides a simple and automatic election scheme

- ● *Gateway Load Balancing Protocol (GLBP)*

  - ○ <u>Adds load balancing capabilities</u>, allowing multiple routers to simultaneously forward packets to distribute traffic load

  - ○ Assigns different virtual MAC addresses to each group member for load balancing

  - ○ Automatically redirects traffic to other routers in the group if any fail

- ○ Importance

  - ■ Critical for network designs to ensure continuous network availability, <u>reliability, and efficiency</u> especially as networks are relied upon for global communications and entertainment

- **Understanding Routing: Demonstration**

- **Multicast Routing**
  - *Multicast Routing*
    - Sending traffic to a class D IP address (multicast group) to deliver messages to multiple recipients efficiently
    - Objective:
      - Send traffic out once and have all interested devices receive it, while others ignore it
  - Methods of Multicast Routing
    - *IGMP (Internet Group Management Protocol)*
      - Used by clients and routers to let the routers know which interfaces have multicast receivers
      - Allows clients to join multicast groups and receive messages
      - More about clients and servers together
      - IGMPv1
        - Caused unnecessary traffic due to periodic group queries
      - IGMPv2
        - Improved by allowing clients to send leave messages
      - IGMPv3
        - Added support for source-specific multicast

- *PIM (Protocol Independent Multicast)*
  - Enables multicast traffic routing between multicast-enabled routers
  - Forms multicast distribution trees
  - Focuses more on routing
  - PIM Dense Mode (PIM-DM)
    - Uses flood and prune behavior, causing network performance issues
      - Floods traffic initially, then prunes non-optimal routes
      - High network performance impact due to periodic flooding
    - Not commonly used in modern networks
  - PIM Sparse Mode (PIM-SM)
    - Uses shared distribution tree initially, then switches to optimal tree (Shortest Path Tree/SPT)
    - Lower impact on network performance
    - Preferred in modern networks for efficiency

- **Generic Routing Encapsulation**
  - *Generic Routing Encapsulation (GRE)*
    - A tunneling protocol used to encapsulate a wide variety of network layer protocols inside a virtual point-to-point link over an Internet Protocol network
    - GRE tunnels operate at Layer 3 or the network layer of the OSI model
    - Serves as a universal translator
      - Allows different protocols to communicate and traverse over a shared network infrastructure
      - Useful for connecting similar network topologies over a different intermediate network
  - Use Cases
    - Connecting branch offices securely and efficiently over the internet without expensive dedicated leased lines
    - Encapsulating protocols for tunneling without the additional overhead of encryption techniques inside a VPN, making it ideal for connecting heterogeneous networks
  - Comparison with VPN
    - GRE
      - Favored for its simplicity and efficiency in encapsulating multiple protocol types, making it lightweight compared to a full site-to-site VPN

- Preferred when the main objective is to encapsulate protocols for tunneling without the additional overhead created by encryption techniques
    - VPN
        - Could provide more robust security features, but with additional overhead due to encryption
- GRE also provides versatility and integration by allowing different network protocols to co-exist and collaborate in heterogeneous network environments
- GRE tunnels are set up and configured on network routers
- GRE tunnels can be used with additional encryption techniques for securing data over untrusted networks like the internet

Network Services

Objectives:

- 1.2 - Compare and contrast networking appliances, applications, and functions
- 3.4 - Given a scenario, implement IPv4 and IPv6 network services

- **Introduction**
  - *Network Service*
    - Function provided by the network infrastructure to support various types of communications and processes

- **Dynamic Host Configuration Protocol (DHCP)**
  - *Dynamic Host Configuration Protocol (DHCP)*
    - Automates the process of assigning IP addresses to devices on a network
    - Helps prevent configuration errors and IP conflicts by dynamically assigning IPs
  - *Scope*
    - A range of valid IP addresses available for assignment on a subnet
    - Devices automatically receive an IP address from the scope when joining the network
    - Administrators can exclude certain IPs or use reservations for specific devices

- ○ DHCP Lease

  - ■ DHCP leases IPs for a specific period (default is 24 hours)

  - ■ Longer lease times are common in corporate networks for stability and security

- ○ *DHCP Reservation*

  - ■ Excludes some IP addresses from being handed out to devices unless a certain condition is met

- ○ DHCP Process: DORA

  - ■ Discover

    - ● Device requests an IP address from the DHCP server

  - ■ Offer

    - ● DHCP server offers an IP address to the device

  - ■ Request

    - ● Device requests the offered IP address

  - ■ Acknowledge

    - ● DHCP server acknowledges the request and assigns the IP

- ○ DHCP Configuration

  - ■ DHCP assigns four key pieces of information to devices

    - ● IP address

    - ● Subnet mask

    - ● Default gateway IP

    - ● DNS server IP

- DHCP set up:
    - Dynamic assignment
        - DHCP servers do the configuration
    - Static assignment
        - Requires manual configuration of all four pieces of information
- An alternate configuration is used if DHCP fails
    - APIPA – default
    - Static IP
- DHCP Scope Options
    - DHCP servers can be configured with scope options
        - Subnet mask
        - Default gateway
        - DNS server
        - Lease time
- *DHCP Relay*
    - Any host that forwards DHCP packets between clients and servers
    - Useful when clients and servers are not on the same subnet
    - Avoids installing DHCP servers on every subnet
- UDP and IP Helper Address
    - DHCP operates using UDP
        - A fire-and-forget method of sending data

- *IP Helper Address*

    - Used to forward UDP broadcasts, ensuring DHCP requests reach the server

- If the DHCP client and server are on separate network segments, the client's network segment router must be configured with an IP helper address

    - This configuration enables the router to properly forward DHCP requests to the DHCP server

- **Understanding DHCP: Demonstration**

- **Stateless Address Autoconfiguration (SLAAC)**

    - *Stateless Address Auto Configuration (SLAAC)*

        - An integral component of the IPv6 network protocol, simplifying the network configuration process by allowing devices to autonomously assign their IP addresses

        - Created to reduce administrative overhead and foster self-sufficiency in network management

    - SLAAC Advantages

        - Enhances network efficiency

        - Eliminates potential for IP conflicts

        - Streamlines integration of new devices into networks

- ○ Operation
  - ■ Device Initiation
    - ● Device generates a temporary link-local address
  - ■ Router Solicitation
    - ● Device sends a message to identify local routers
  - ■ Router Advertisement
    - ● Routers respond with network prefix information
  - ■ Address Configuration
    - ● Device combines prefix with unique identifier to create IP address
  - ■ Neighbor Solicitation (Final check)
    - ● Device checks for address conflicts before settling on IP address
- ○ Real-World Analogy
  - ■ Similar to smart devices in a home autonomously finding their place on a network without manual assignment

- **Domain Name System (DNS)**
  - ○ *Domain Name System (DNS)*
    - ■ A protocol used to convert human-readable domain names (like example.com) into IP addresses (like 192.0.2.1) that computers use to identify each other on the network
    - ■ Helps users find websites using easy-to-remember domain names instead of numeric IP addresses

- ○ Functionality

    - ■ When a user's computer wants to access a website, it contacts a DNS server to resolve the domain name to an IP address

    - ■ DNS servers store mappings of domain names to IP addresses in records

- ○ *Fully Qualified Domain Name (FQDN)*

    - ■ A domain name that is under a top-level provider

        - ● .com – most common

        - ● .mil

        - ● .edu

        - ● .org

        - ● .net

- ○ <u>DNS is structured in a five-level hierarchy</u>

    - ■ *Root Level*

        - ● Highest level

        - ● Answers requests in the root zone

    - ■ Top-Level Domain (TLD)

        - ● Organizational hierarchies – .com, .net, .org, etc.

        - ● Geographical hierarchies – .uk (United Kingdom), .it (Italy), .fr (France), etc.

    - ■ *Second-Level Domain*

        - ● Tied directly below the top level domain (e.g., diontraining in diontraining.com)

- *Subdomain*
    - Server underneath second-level domain (e.g., www in www.diontraining.com)
- *Host*
    - Lowest and most detailed level
    - Refers to a specific machine within a domain
- *URL (Uniform Resource Locator)*
    - Specifies how to access a resource (e.g., a website) on the internet using a domain name and a protocol (e.g., https://www.diontraining.com)
    - Examples
        - Secure – https://
        - Insecure – http://
        - FTP – ftp://
- *Host File*
    - A simple text file that serves as the first point of contact when the device wants to seek out communication with other devices over the network
    - Can be used to manually map domain names to IP addresses, bypassing the need for DNS
    - Takes priority over DNS and has a closer proximity
    - Useful for testing and can be a security risk if not managed properly
    - Can be used as a temporary workaround for DNS issues

- ○ Security Implications

  - ■ DNS can be used maliciously to redirect users to fake websites for phishing attacks

  - ■ Manipulating the hosts file can also be a security risk if not done carefully

- **DNS Record Types**

  - ○ <u>DNS Record Types</u>

    - ■ *A Records (Address Records)*

      - ● <u>Link host names to IPv4 addresses</u>

    - ■ *AAAA Records (IPv6 Address Records)*

      - ● <u>Link host names to IPv6 addresses</u>

    - ■ *CNAME Records (Canonical Name Records)*

      - ● Used to <u>point a domain to another domain name or subdomain</u>

      - ● Example

        - ○ Setting multiple domains to resolve to the same site

      - ● <u>Cannot be used to point to an IP address</u>

    - ■ *MX Records (Mail Exchange Records)*

      - ● <u>Direct emails </u>to a mail server using SMTP over port 25

      - ● Point to another domain, not an IP address

      - ● Include priority values to determine preferred servers

        - ○ The lower the number, the higher the priority

- ○ To load balance email across multiple servers, set their priorities to be the same value
- ■ *SOA Records (Start of Authority Records)*
  - ● <u>Store important domain information</u> like update times and administrators
  - ● Critical for DNS server zone transfers
    - ○ *Zone Transfer*
      - ■ Process of sending DNS records data from the primary nameserver to a secondary nameserver
      - ■ Uses TCP
- ■ *PTR Records (Pointer Records)*
  - ● <u>Correlate an IP address with a domain name</u>
  - ● Opposite of A Records
  - ● *Reverse DNS lookup*
    - ○ Determines what the domain name is for a given IP address
    - ○ Query is made against PTR records
    - ○ *Forward Lookup*
      - ■ Uses DNS to find the IP address for a given domain name

- Helpful in proving that a domain is not associated with spam, troubleshooting email deliverability issues, or creating better logging by converting IP addresses back into domain names
- Always stored under .arpa top-level domain
    - Versed as ".in-addr.arpa"
    - *Advanced Research Projects Agency Network (ARPAnet)*
        - First top-level domain that was defined for what would become the Internet

- *TXT Records (Text Records)*
    - Add text into the DNS
    - Store human-readable or machine-readable data
    - Used for domain ownership verification and email spam prevention

- *NS Records (Nameserver Records)*
    - Indicate the authoritative DNS name server for a domain
    - Necessary for DNS hierarchy and record management
    - *Nameserver*
        - Type of DNS server that stores the DNS records for a given domain
        - There are often more than one nameserver for domain
            - Primary
            - Secondary

- Internal and External DNS

  - Internal DNS

    - For private networks, cloud instances, etc.

  - External DNS

    - For publicly accessible domain names

- *TTL (Time to Live)*

  - Specifies how long a DNS resolver should cache a query before requesting a new one

    - *DNS Resolver/DNS Cache*

      - Makes local copy of every DNS entry it resolves as the user connects to websites

      - Helps in speeding up DNS lookups and managing server load

- *Recursive Lookup*

  - DNS resolver keeps querying DNS servers until it finds the IP for a domain

  - Used for finding IPs for domain names

- *Iterative Lookup*

  - DNS server tells the resolver to query the next DNS server until it finds the IP

  - Resolver is responsible for hunting down the IP

- **Securing DNS**
  - *Domain Name System (DNS)*
    - Redirects network devices from domain names to associated IP addresses
    - Critical for network security
      - If compromised, can redirect requests to malicious servers
  - *DNS Security Extensions (DNSSEC)*
    - Provides a digital seal for DNS data to ensure it hasn't been tampered with
    - Uses cryptographic signatures verified against a chain of trust
    - Prevents successful exploitation even if DNS records are falsified
    - Does not encrypt DNS data
  - *DNS over HTTPS (DoH)*
    - Encrypts DNS queries sent through HTTPS
    - Blends DNS queries with HTTPS traffic for increased privacy and security
  - *DNS over TLS (DoT)*
    - Encapsulates DNS traffic in a Transport Layer Security (TLS) tunnel
    - Encrypts DNS data for privacy, preventing eavesdropping on queries
  - Privacy and Integrity
    - *DNS Snooping*
      - An attacker monitors DNS queries to infer what websites a user is visiting

- Prevented by both DoH and DoT, ensuring online activities remain private
  - Trust and Integrity
    - Implementing DNSSEC, DoH, and DoT safeguards trust in the digital ecosystem
  - Implementation Considerations
    - Collaborative Effort
      - Requires involvement of website owners, ISPs, and organizations
    - Balancing Act
      - Implementing DoH may shift DNS resolution control to third-party providers, requiring careful consideration
  - Overall Objective
    - While protecting data, also aim to preserve trust and reliability in networks and the internet

- **Understanding DNS: Demonstration**

- **Network Time Protocol (NTP)**
  - *Network Time Protocol (NTP)*
    - Used for synchronization of clocks between different computer systems
    - Sends data using UDP packets on port 123
    - NTP version 4 (2010) – most current version

- Synchronizes clocks to within a few milliseconds of Coordinated Universal Time (UTC)
- Components
    - Stratum
        - Hierarchical system of time sources
        - Stratum 0
            - Most precise timekeeping devices like atomic clocks
            - Reference clock
        - Stratum 1
            - Where first NTP servers in the hierarchy are going to start at
            - Computers synchronized to within a few microseconds of the attached stratum 0 devices
            - Considered primary time servers
        - Stratum 2
            - Connected and synchronized to stratum 1 servers
            - Often configured to query multiple stratum 1 servers
        - Stratum 3
            - Synchronized upward back to stratum 1 and 2 servers

- ○ The hierarchy continues with each stratum adding more delay and becoming further from stratum 0
- ○ Stratum 15 – maximum limit
- ○ Stratum 16
    - ■ Indicates unsynchronized devices
  - ● Clients
  - ● Servers
- ■ In enterprise networks, a time server is connected, and client software is installed on workstations to interface with the server
- ■ NTP service on domain controllers acts as the time source for workstations
- ○ *Precision Time Protocol (PTP)*
  - ■ Used to synchronize clocks throughout the computer network
  - ■ Achieves clock accuracy in the sub-microsecond range
  - ■ Ideal for networks requiring precise timekeeping
    - ● Financial trading
    - ● Industrial automation systems
  - ■ Uses a primary-secondary architecture for clock synchronization
    - ● Primary clocks send precise time messages
    - ● Secondary clocks adjust to align with the primary clock

- ○ *Network Time Security Protocol (NTS)*
    - An extension of NTP developed to provide cryptographic <u>security for time synchronization</u>
    - Uses TLS and AEAD to ensure secure time synchronization
    - Authenticates the time source and the integrity of received time to prevent malicious tampering

- **Quality of Service (QoS)**
    - ○ *Quality of Service (QoS)*
        - Enables strategic optimization of network performance based on different types of traffic
        - Purpose
            - Ensure proper delivery of voice, data, and video content over converged networks
        - Benefits
            - Optimize network performance
            - Efficiently utilize bandwidth
            - Ensure service availability
            - Save costs
    - ○ QoS Components
        - Categorization
            - Identify and categorize traffic types (e.g., web, voice, video, email)

- Prioritization
  - Assign priority levels to different types of traffic
- Bandwidth Management
  - Determine and allocate required bandwidth for each traffic type
- Traffic Dropping
  - Identify and drop lower-priority traffic during congestion to maintain quality for higher-priority traffic
- QoS Categories
  - *Delay*
    - Time taken for a packet to travel from source to destination
      - Measured in milliseconds
    - Critical for real-time traffic like voice and video
  - *Jitter*
    - Uneven arrival of packets
    - Particularly detrimental to voice over IP (VoIP) traffic
  - *Drops*
    - Occur during network congestion
      - Leads to packet loss
    - More critical for UDP-based traffic like VoIP
- *Effective Bandwidth*
  - The lowest bandwidth among the links in a network path, which determines the actual data rate

■ Limits the overall throughput of the network, impacting user experience and application performance

- **QoS Categorization**
  - ○ Purpose of QoS
    - ■ Categorize traffic into buckets
    - ■ Apply policies based on traffic categories
    - ■ Prioritize traffic based on categories
  - ○ Traffic Prioritization
    - ■ High priority for real-time traffic like VoIP to avoid delays and ensure quality
    - ■ Low priority for non-mission-critical data like web browsing or email
    - ■ Documentation and Communication
      - ● Document and share QoS policies with users
      - ● Help users understand the policies to avoid confusion and reporting of issues
  - ○ Mechanisms of Traffic Categorization
    - ■ Best Effort
      - ● No QoS
      - ● First in, first out
      - ● No reordering or shaping

- Integrated Services (IntServ)
  - Hard QoS
  - Strict bandwidth reservations for different traffic types
- Differentiated Services (DiffServ)
  - Soft QoS
  - Traffic marked for different priorities
  - Allows for flexible allocation
- Comparison of QoS Approaches
  - Best Effort
    - Least efficient, no strict policies.
  - DiffServ (Soft QoS)
    - Better than Best Effort but less efficient than IntServ
  - IntServ (Hard QoS)
    - Strict policies, highest level of service for critical traffic
- Implementation of QoS
  - Classification and marking
  - Congestion management and avoidance
  - Policing and shaping
  - Link efficiency

- **QoS Mechanisms**
  - ○ Traffic Categorization
    - ■ Classification
      - ● Determines traffic categories based on type (e.g., email protocols)
      - ● Analyzes packet headers, packet type, and ports
      - ● Helps prioritize services without altering packet bits
    - ■ Marking
      - ● Alters bits within frames, cells, or packets
      - ● Indicate how to handle traffic
      - ● Uses Type of Service (ToS) header
        - ○ IP precedence
        - ○ DSCP
    - ■ Congestion Management
      - ● *Queuing*
        - ○ Buffers extra traffic when devices receive data faster than they can transmit
        - ○ Empties the packets in specified sequence and amount using one of three mechanisms:
          - ■ Weighted Fair Queuing
          - ■ Low-latency Queuing
          - ■ Weighted Round-robin

- Congestion Avoidance
  - *RED (Random Early Detection)*
    - Prevents buffer overflow by dropping packets based on priority
    - Discards lower priority packets first to avoid congestion
- Policing and Shaping
  - *Policing*
    - Discards packets that exceed configured rate limits
    - Results in retransmissions, creating more bandwidth
    - Good for very high speed interfaces
  - *Shaping*
    - Delays traffic from exceeding rate limits by buffering
    - Holds packets in the buffer and releases them when space is available
- Link Efficiency
  - *Compression*
    - Reduces packet size, conserving bandwidth
    - Utilizes protocols like CRTP (Compressed RTP) for VoIP to reduce header size significantly
  - *LFI (Link Fragmentation and Interleaving)*
    - Fragments big packets and interleaves smaller packets to utilize slower links efficiently

- Prevents voice latency by interleaving smaller voice packets between larger data packets

Wide Area Networks (WANs)

Objective 1.5: Compare and contrast transmission media and transceivers

- **Introduction**
  - Computer networking over time
    - Pareto Principle (80-20 rule) in early networking
      - 80% of traffic stays within the LAN
      - 20% of traffic goes out to the WAN
    - Pareto Principle (80-20 rule) in current networking
      - 80% of traffic goes out to the WAN
      - 20% of traffic stays within the LAN

- **Fiber Optic Connections**
  - *Fiber Optic Connections*
    - Backbone of hyper-connected lifestyles in homes and small offices
    - Various forms categorized by proximity to end user premises
  - Key Terms
    - *FTTH (Fiber to the Home)*
      - Direct fiber optic connection to individual residences
      - Highest speed and reliability due to entire connection being fiber optic

- Ideal for demanding users like home offices, gamers, and streaming enthusiasts
  - *FTTC (Fiber to the Curb/ Cabinet)*
    - Fiber optic cables run to curbside or nearby cabinet
    - Uses traditional copper cable for the final connection
    - Offers a balance between cost and performance
    - Common in urban setups
  - *FTTN (Fiber to the Node/Neighborhood)*
    - Extends fiber optic connection to a central point in an area
    - Copper cables branch out from the node to individual locations
    - Allows leveraging existing copper infrastructure for improved speeds
  - *FTTB (Fiber to the Building/Basement)*
    - Fiber optic cables reach building's main communication room or basement
    - Connection to individual units/offices within the building is usually done through copper cabling
    - Common in multi-dwelling units where high-speed fiber is brought close to users but not directly into each unit
- Speed and Reliability Comparison
  - <u>Highest speed and reliability</u>
    - <u>FTTH</u>

- FTTB
  - Slower but still faster than entirely copper-based networks
    - FTTC
    - FTTN
  - Marketers may use the term "fiber" even for slower connections like FTTC or FTTN, so understanding the specific type is important for choosing the best connection

- **Cable (DOCSIS) Connections**
  - DOCSIS Overview
    - A prevalent technology that brings high-speed internet through TV cable lines
    - Uses (HFC) network
  - *HFC (Hybrid Fiber Coaxial)*
    - Network acts as a high-capacity highway for data transmission
    - Combines fiber optic and coaxial cables
      - Fiber optic cables
        - Transmit data from service provider to distribution points
      - Coaxial cables
        - Deliver data to homes/offices

- *DOCSIS (Data Over Cable Service Interface Specification)*
  - Standardizes data transmission over HFC networks for consistent, reliable, high-speed internet access
  - Ensures cable modems speak the same language, regardless of location or service provider
  - Frequency Ranges
    - *Upstream*
      - Data that is sent out
      - 5-42 MHz
    - *Downstream*
      - Data that is received
      - 50-860 MHz
  - Asynchronous Speeds
    - Cable modems are usually asynchronous, providing high download speeds but slower upload speeds
  - Advantages
    - Utilizes existing cable TV infrastructure, making rollout cost-effective and quick
    - Offers higher speeds compared to DSL, a popular alternative in the late 1990s and early 2000s

- ○ DOCSIS Evolution

  - ■ Evolved over versions (e.g., DOCSIS 1.0 to latest) for faster speeds (up to 1-5 Gbps), better performance, and improved security

  - ■ Ensures safe and swift data transmission for activities like streaming, video conferencing, and online gaming

- **Digital Subscriber Line (DSL) Connections**

  - ○ *Digital Subscriber Line (DSL)*

    - ■ A family of technologies that provide internet access by transmitting digital data over the wires of a local telephone network

  - ○ Types of DSL

    - ■ *Asymmetric DSL (ADSL)*

      - ● Different speeds for download and upload

        - ○ Maximum download speed – about 8 Mbps

        - ○ Upload speed – 1.544 Mbps

      - ● Suitable for users who download more than they upload

    - ■ *Symmetric DSL (SDSL)*

      - ● Provides equal upload and download speeds

      - ● Offers dedicated access but at a slower overall speed compared to ADSL

- *Very High Bit-Rate DSL (VDSL)*
  - Offers very high speeds
    - Downloads – up to 50 Mbps
    - Uploads around 10 Mbps
  - Limited by distance from the DSLAM (Digital Subscriber Line Access Multiplexer)
    - *DSLAM (Digital Subscriber Line Access Multiplexer)*
      - Point of presence that is owned by the telephone company
      - Within 4,000 ft range for VDSL
      - 4,000 ft to 18,000 ft for ADSL
- Popularity and Usage
  - DSL was popular in the late 1990s and early 2000s due to its affordability and ability to provide high-speed data to small offices and home office environments
  - ADSL was popular with home users and received significant funding from telecommunication companies, leading to speed increases over time
  - DSL is still used in some remote areas, but cable modems and fiber optics have become more common in larger city environments
- Future Trends
  - Traditional copper phone lines, over which DSL operates, are being phased out in favor of fiber optic connections and Voice over IP services

- **Satellite Connections**
  - *Satellite Internet Access*
    - Method of utilizing communication satellites in space to connect users to the internet
    - Ideal for remote areas where cable, cellular, or fiber is unavailable
  - Usage
    - Home Users
      - Can use commercial services like HughesNet or Starlink
      - Requires a satellite dish installed on the roof
    - Mobile Users
      - Ideal for users on the go, like those in RVs, trucks, or traveling internationally, providing internet access via satellite modems
  - Advantages
    - Availability
      - Accessible in remote areas where other services are unavailable
    - Global Coverage
      - Can be accessed almost anywhere with a clear line of sight to the satellite
    - Decent Speed
      - Provides relatively fast internet service, allowing activities like streaming movies

- ○ Drawbacks

    - ■ Slower speed compared to fiber, microwave links, or cable modems

    - ■ <u>More expensive than other types of internet service</u>

    - ■ High latency due to geosynchronous satellites located around 22,000 miles above the earth

- ○ Recent Developments

    - ■ Companies like SpaceX with Starlink are revolutionizing satellite internet by deploying satellites in <u>low earth orbit</u>

        - ● Reduces latency to around 25-35 milliseconds

    - ■ Starlink's approach involves launching thousands of satellites at closer distances (340 miles) to the earth

        - ● Offers lower latency and higher speeds compared to traditional geosynchronous satellites

- ○ <u>Key Points</u>

    - ■ Satellite internet tends to be <u>more expensive</u>

    - ■ Commonly used in <u>remote or mobile environments</u>

    - ■ Opt for systems using <u>low earth orbit for lower latency and higher speeds</u>, such as Starlink

- **Cellular Connections**
  - Cellular Connections Overview
    - Includes smartphones, tablets, dedicated cellular modems, wireless access points, and fixed cellular services
    - Encompasses a wide range of technologies, from 2G to 5G
  - Generations (G) of Cellular Technology
    - 1G (1980s)
      - Frequency – 30 KHz
      - Speed – 2 Kbps
      - Voice calls-focused, with limited data capabilities
    - 2G (Late 1990s)
      - Frequency – 1,800 MHz
      - Speed – 14.4-64 Kbps (Similar to dial-up)
      - Ran over digital network that used multiplexing
      - Allowed data usage (low -speed) in addition to phone calls
        - SMS and text messaging
        - International roaming conference calls
    - 3G
      - Frequency – 1.6-2 GHz
      - Speed – 144 Kbps to 2 Mbps

- Technologies:
  - *WCDMA (Wideband Code Division Multiple Access)*
    - Used by the UMTS (Universal Mobile Telephone System) standard
    - Slowest (2 Mbps)
  - *HSPA (High Speed Packet Access)*
    - Referred to as 3.5G
    - Speed up to 14.4 Mbps
  - *HSPA+ (High Speed Packet Access Evolution)*
    - Referred to as 3.75G
    - Speed up to 50 Mbps
- 4G
  - Frequency – 2-8 GHz
  - Speed – 100 Mbps to 1 Gbps
  - Introduced MIMO (Multiple Input, Multiple Output) technology
  - Often called 4G LTE (Long Term Evolution)
- 5G (2019)
  - Frequency –
  - Speed – up to 10 Gbps
  - Three Frequency Bands
    - Low Band
      - 600-850 MHz

- - - ■ Speeds of 30-250 Mbps (<u>low speed</u>)
      - ■ <u>Long-range coverage</u>
    - ○ <u>Mid Band</u>
      - ■ 2.5-3.7 GHz
      - ■ Speeds of 100-900 Mbps
      - ■ <u>Good balance of coverage and speed</u>
      - ■ <u>Most used</u>
    - ○ <u>High Band</u>
      - ■ 25-39 GHz
      - ■ <u>Speeds in the gigabit range, but very short-range coverage</u>
    - ○ <u>Upward band means faster speed but decreasing coverage area</u>
  - ■ <u>Higher G means newer standard and faster speeds</u>
- ○ Cellular Technologies
  - ■ Determined by which area users live or which cellular provider users will use in a particular country
  - ■ GSM vs. CDMA
    - ● *GSM (Global System for Mobile Communications)*
      - ○ Converts voice to digital data
      - ○ Uses time division for efficiency
      - ○ More widely supported across the globe

- - - ○ GSM phones use SIM cards
    - *CDMA (Code Division Multiple Access)*
      - ○ Uses code division to split channels
      - ○ More flexible and powerful than GSM
      - ○ Mostly used in 3G and beyond
      - ○ CDMA phones are configured to the provider
  - Considerations for Cellular Devices
    - Network Compatibility
      - ○ Check the cellular technology (GSM or CDMA) supported by your provider and region
    - Modern smartphones support eSIMs for easy switching between providers

- **Microwave Connections**
  - *Microwave Link*
    - Communication system that uses radio waves in the microwave frequency band to transmit information between two fixed locations
    - Frequency range
      - 300 MHz to 300 GHz
      - UHF (Ultra High Frequency) range
      - SHF (Super High Frequency) range
      - EHF (Extremely High Frequency) range

- - Commonly used in large college campuses and small businesses for network connections
  - Line of Sight connection
    - Requires antennas to have a direct line of sight, limiting the distance to around 40 miles (64 kilometers) due to the curvature of the earth
    - Requires professional installation with antennas mounted on the roof of buildings
  - Originally marketed as WiMAX (Worldwide Interoperability for Microwave Access)
    - IEEE 802.16 standard for microwave access
    - Offers faster speeds than cellular and DSL services
    - Expensive
    - Complex installation
      - Internet service providers often place antennas on tall buildings for better coverage
    - Wireless Fixed Location Service
      - Requires larger antennas and radios compared to traditional modems
    - WiMAX and microwave connections are losing popularity for consumer internet due to the rise of 4G and 5G cellular technology
    - Still used for internal network connections in business parks or campuses

- **Leased Line Connections**
  - *Leased Lines*
    - Fixed bandwidth that has symmetric data connections reserved for subscribers' exclusive use
    - <u>Premier choice for businesses and organizations that require a dedicated, reliable, and high performance internet connection</u>
    - Ideal solution for uncompromising communications infrastructure
    - Often referred to as Dedicated Leased Line
      - Continuous connection between two points that are set up by a telecommunications provider
  - Benefits
    - Symmetric Nature
      - Upload and download speeds are identical
      - Critical for businesses requiring high upload speeds
    - Bandwidth options
      - 2 Mbps to 10 Gbps
      - Allows tailored connectivity
    - Reliability
      - Guarantees consistent speeds and high levels of service and security

- Service Level Agreements (SLAs)
    - Providers often offer SLAs with guaranteed uptimes exceeding 99.9%, ensuring swift repair and recovery
    - Gives high level of availability
    - Security
        - Fewer routers and switches reduce exposure to cyber attacks
        - Ideal for handling sensitive information
    - Cost
        - Generally more expensive than shared services like DSL or cable
        - Justified by the benefits, especially for businesses with critical communication needs
    - Applications
        - Can be used to create wide area networks (WANs)
- Primarily used by businesses where connectivity is a critical component of their operational backbone
- Offer unmatched speed, reliability, and security, making them a strategic investment for businesses needing robust communication capabilities

- **MPLS Connections**
    - *Multiprotocol Label Switching (MPLS)*
        - Technique that is leveraged by service providers to enhance network efficiency and flexibility

- ■ Streamlines and speeds up data traffic flow
- ■ <u>"Label Routing"</u>
- ○ *Label Switching*
  - ■ MPLS routers forward packets based on short path labels rather than lengthy IP headers and routing tables
  - ■ Label Assignment
    - ● Ingress router assigns a short, fixed-length identifier (label) to the packet
    - ● The label encapsulates the packet's forwarding information
  - ■ Label Switching
    - ● Core routers in the MPLS network forward packets based on labels
    - ● Routers use labels to look up forwarding tables and determine the next hop
    - ● Avoids complex route lookups
  - ■ Label Removal
    - ● Egress router (exit point of the MPLS network) removes the label
    - ● The packet is forwarded based on its original IP header
- ○ MPLS operates like an expressway, getting on or off at certain points, not at every router
- ○ Protocol Agnostic Nature
  - ■ MPLS can carry various types of data (e.g., Ethernet frames, ATM cells) because it treats them all the same way

- ■ This versatility makes MPLS ideal for integrating diverse network types and services
  - ○ Quality of Service (QoS)
    - ■ MPLS can enforce traffic engineering, allowing service providers to define explicit paths for different types of traffic
    - ■ Ensures optimal use of network resources and can prioritize high-priority data packets
  - ○ Reliability and Redundancy
    - ■ Offers mechanisms for automatic and rapid rerouting of traffic in case of link or node failure
    - ■ Minimizes downtime and ensures continuous data flow, enhancing service continuity and performance
  - ○ End User Impact
    - ■ Improves service quality, reliability, and performance for end users
    - ■ Operates quietly behind the scenes but plays a crucial role in shaping efficient, robust, and agile networks
    - ■ Goes beyond traditional IP routing, offering more streamlined and dynamic ways of handling data traffic using labeling

- **Understanding WAN Connections: Demonstration**

Cloud and the Datacenter

Objectives:

- 1.3 - Summarize cloud concepts and connectivity options
- 1.8 - Summarize evolving use cases for modern network environments

- **Cloud Computing**
    - <u>Cloud Computing Characteristics</u>
        - *High Availability*
            - Refers to services experiencing minimal downtime in the cloud
            - Services are highly reliable and fault-tolerant
            - Measured in uptime percentage (e.g., five nines means 99.999% uptime)
        - *Scalability*
            - Ability to increase system capacity at a linear rate or less than a linear rate
            - Can accommodate increasing numbers of users or things in the system
            - *Vertical Scaling*
                - Scale up
                - Increasing the power of the existing resources in the working environment

- *Horizontal scaling*

    - Scale out

    - Adding additional resources, like additional servers, to help handle the extra load being experienced

- *Rapid Elasticity*

    - Ability to rapidly scale up or down based on demand

    - Achieved through automation and orchestration of virtual machines

    - Enables handling changes in demand in real time

- *Metered Utilization*

    - Pay-per-use model for cloud services

    - Charges based on actual usage of services

    - Offers cost efficiency and flexibility in resource allocation

    - Metered Service

        - Consumption basis – exact amount used

    - Measured Service

        - Based on a certain amount of quantity upfront

- *Shared Resources*

    - Ability to use virtual machines on shared physical servers

    - Minimizes costs by efficiently utilizing hardware resources

    - Pooling of resources across the cloud provider's data center

- ■ *File Synchronization*
  - ● Ability to synchronize files across multiple locations
  - ● Facilitates collaboration and remote work
  - ● Ensures consistent access to files across devices and locations

- ● **Cloud Service Models**
  - ○ Cloud Deployment Options
    - ■ On-premise Solution
      - ● Offers security but are costly and require a dedicated support team
      - ● Confidentiality is better ensured, where physical and logical access can be controlled
    - ■ Hosted Solution
      - ● Third-party service providers provide hardware and facilities, often in a multi-tenancy environment, reducing costs and resource requirements
      - ● Multi-tenancy solutions may expose residual data to other tenants as server capacity expands or contracts
      - ● Understanding the hosting provider's authentication, redundancy, fault tolerance, and data storage location is crucial

- ○ Cloud Service Models
    - ■ *Software as a Service (SaaS)*
        - Provider offers a <u>complete solution</u>, including hardware, software, and application access
        - Examples
            - ○ Office 365
            - ○ Google Workspace
            - ○ TurboTax
            - ○ QuickBooks Online
    - ■ *Platform as a Service (PaaS)*
        - Provider offers hardware and operating system software, allowing <u>customization</u> of applications
        - Useful for developing web applications without managing underlying infrastructure
        - Includes <u>middleware and runtime</u>
    - ■ *Infrastructure as a Service (IaaS)*
        - Provides IT resources like servers, load balancers, and storage area network components
        - Offers dynamic allocation of resources without long-term hardware commitments
        - Focuses <u>mostly on hardwares</u>

- ○ Exam Tip

    - ■ If a service includes more than IaaS but less than SaaS, it's likely PaaS

- **Cloud Deployment Models**

    - ○ Cloud Computing Trends

        - ■ Increased availability

        - ■ Higher resiliency

        - ■ Unlimited elasticity

    - ○ Despite its advantages, cloud computing introduces unique security challenges

    - ○ Types of Cloud Deployment Models

        - ■ *Public Cloud*

            - Resources provided over the internet by a service provider (e.g., Google Drive, Microsoft Azure)

            - Cost-effective and efficient for quick service acquisition

        - ■ Private Cloud

            - Organization creates and manages its own cloud environment

            - Offers higher security but can be more costly

        - ■ Hybrid Cloud

            - Combines private and public cloud resources

            - Requires strict data hosting rules for security

- Community Cloud

  - Resources and costs shared among multiple organizations with common service needs

  - Challenges include varying security controls among organizations

- Multi-Tenancy

  - Same resources used by multiple organizations for efficiency

  - Security concerns include shared vulnerabilities

- Single-Tenancy

  - Single organization assigned to a resource

  - Less efficient and more expensive than multi-tenancy

- Choosing a Cloud Model depends on:

  - Security needs

  - Cost restrictions

  - Risk tolerance

- **Using Cloud Computing: Demonstration**

- **Cloud Connectivity**

  - Connectivity Options for Cloud-based Solutions

    - Focusing on connecting enterprise networks to public cloud service providers (CSPs)

- Ensuring network clients can access resources from anywhere, just as they could on-premise

- ■ Virtual Private Network (VPN)
    - Establishes secure connections between on-premise network, remote offices, client devices, and cloud provider's network
    - Often created as a site-to-site VPN between edge router and cloud provider's network
    - Uses traditional IPsec VPN for encrypted connection over the public internet
    - Provides a managed, highly available, and elastic solution for extending the network

- ■ Private Direct Connection
    - Allows extending on-premise network into cloud provider's network
    - Bypasses the internet, providing a secure and dedicated connection
    - Uses dedicated lease line or similar WAN connection
    - Supports faster speeds and better performance compared to VPNs

- ○ Trade-offs
    - ■ VPN
        - Offers cost-effective connectivity

- ■ Private Direct Connections
    - ● Offer better performance and redundancy
    - ● More expensive
- ○ <u>Choose between VPNs and private direct connections based on performance needs and cost considerations</u>

- **Cloud Security**
    - ○ *Cloud Security*
        - ■ Involves protecting cloud-based resources from unauthorized access and attacks
    - ○ <u>*Virtual Private Cloud (VPC)*</u>
        - ■ Used to provision <u>a logically isolated section of a cloud provider's infrastructure</u>
        - ■ Allows launching resources inside a defined virtual network
        - ■ <u>Part of the larger concept of Infrastructure as Code (IAC)</u>
            - ● *Infrastructure as Code (IAC)*
                - ○ Includes the provisioning of architecture where the deployment of resources is performed by scripted automation and orchestration
        - ■ <u>Key Components</u>
            - ● *Subnet*
                - ○ A range within a VPC for allocating instances

- ○ Can be public or private
- *Route Tables*
  - ○ Contain rules (routes) for directing network traffic within a VPC
  - ○ Associated with each subnet
- *Internet Gateway*
  - ○ Enables communication between VPC instances and the public internet
  - ○ Horizontally scalable, redundant, and highly available
- *Network Access Translation (NAT) Gateway*
  - ○ Enables private subnet instances to connect to the internet, but prevents the internet from initiating a connection with those instances in he VPC
- *Network Access Control List (ACL)*
  - ○ Subnet-level firewalls for controlling inbound and outbound traffic
  - ○ Operates like stateless firewall
    - ■ Each rule for inbound or outbound traffic is evaluated independently
  - ○ May be used to supplement Security Groups but not to replace them

- *Security Groups*
    - Instance-level firewalls for controlling inbound and outbound traffic
    - Operate like stateful firewall
    - Newly created security group has no inbound rule and has allow outbound rule by default
- *VPC Peering*
    - Network connection between two VPCs for private traffic routing
- *VPC Endpoints*
    - Allow private connectivity to services within a cloud provider without using the internet
- *VPN Connections*
    - Connect VPCs to remote networks or other VPCs
- Advantages of VPCs
    - Allow mixing products from different vendors
    - Speed up network development
    - Added layers of automation and policy management
    - Enables fully automated deployments
        - Critical for high-velocity or high-availability architectures and disaster recovery

- ■ Challenges of VPCs
  - ● Risk of being a single point of failure if connectivity is lost
  - ● Centralized nature can make them a potential target for attackers, requiring proper security measures

- **Network Virtualization**
  - ○ *Network Function Virtualization (NFV)*
    - ■ A concept that transforms traditional, hardware-dependent network services into software-based virtual functions, enhancing agility and flexibility in telecommunications
  - ○ Traditional Network Services vs. NFV Solution
    - ● Historically, services like routing, firewalling, load balancing, and intrusion detection were performed by dedicated hardware appliances
      - ○ Limit scalability and deployment speed
      - ○ Increase costs
    - ■ NFV Solution
      - ● Extracts network functions from hardware, deploying them as software applications known as Virtual Network Functions (VNFs)
        - ○ Allows for greater flexibility
        - ○ Faster response

- ○ Components of NFV
    - ■ *NFV Infrastructure (NFVI)*
        - ● Includes hardware and virtual resources for deploying, managing, and executing VNFs
    - ■ Management and Network Orchestration (MANO)
        - ● Oversees lifecycle management of VNFs
        - ● Orchestrates resources across NFVI for efficient deployment and scaling
    - ■ *Virtual Network Functions (VNFs)*
        - ● Software implementations of network functions traditionally bound to hardware appliances
        - ● Instantiated on NFVI, and can be chained together for full-scale network services
- ○ Benefits of NFV
    - ■ Flexibility and rapid deployments
        - ● Enables rapid scaling of network services without physical hardware installations
    - ■ Cost Efficiency
        - ● Reduces capital expenditures by utilizing commercial off-the-shelf server technology
            - ○ Eliminates the need for hardware replacements with software upgrades

- ○ Challenges of NFV

  - ■ Security Concerns

    - ● Transitioning to NFV raises security challenges

  - ■ Management Complexity

    - ● Managing and orchestrating virtualized functions can be complex

  - ■ Skills Requirement

    - ● Skilled personnel proficient in virtualization technologies are needed

- **Software-Defined Network (SDN)**

  - ○ *Software Defined Networking (SDN)*

    - ■ An approach to networking that <u>uses software-based controllers or APIs</u> to communicate with underlying hardware infrastructure and direct traffic on a network

    - ■ A part of Infrastructure as Code (IaC)

      - ● *Infrastructure as Code (IaC)*

        - ○ Includes provisioning of architectures in which deployment of resources is performed by scripted automation and orchestration

  - ○ <u>Control Plane</u>

    - ■ Responsible for routing signals to and from a router

    - ■ <u>Makes decisions</u> on traffic prioritization and security

- ○ Data Plane

    - ■ Carries user traffic on the network

    - ■ Performs actual switching and routing

- ○ Management Plane

    - ■ Administers routers and switches

    - ■ Monitors traffic conditions

    - ■ Manages network configurations

- ○ Setting up SDN

    - ■ SDN application is used to define the policy decisions

        - ● Occurs in management plane

        - ● Deployed and operate within control plane

        - ● Traffic is moved by the data plane across the network

- ○ Advantages of SDN

    - ■ Flexibility

        - ● SDNs allow mixing and matching of products from different vendors using common API calls

    - ■ Increased Choices

        - ● Provides organizations with increased choices in network development, adding speed and agility to network establishment

        - ●

    - ■ Automation

        - ● Enables automation of network provisioning

- - Scalability
    - Facilitates fully automated deployment of networks
    - Critical for high velocity or high availability architectures
  - Security
    - Security data is easier to collect, making detection of different traffic patterns in the network unchallenging
- Disadvantages
  - Loss of Connectivity
    - Loss of connectivity to the SDN controller can lead to network downtime
  - Centralized Controller
    - Vulnerable to attacks targeting the singular controller
- Types of SDN
  - *Open SDN*
    - Uses open source technologies like OpenFlow, OpFlex, and OpenStack
  - *Hybrid SDN*
    - Combines traditional networking protocols with SDN technologies
  - *SDN Overlay*
    - Creates layers of network abstraction for virtualized network layers on top of physical networks

- ○ Security Benefits

  - ■ Logical Isolation

    - ● Provides additional security and logical isolation in the network

  - ■ Zero Trust

    - ● Allows implementing zero-trust security models using SDN overlay

- **Software-Defined Wide Area Network (SD-WAN)**

  - ○ *Software-Defined Wide Area Network (SD-WAN)*

    - ■ <u>A virtualized approach to managing and optimizing wide area network connections</u>

    - ■ <u>Used to efficiently route traffic between remote sites, data centers, and cloud environments</u>

  - ○ Benefits of SD-WAN

    - ■ Provides agility, security, and efficiency in network infrastructures

    - ■ Allows enterprises to leverage any combination of transport services

    - ■ Enables the creation of virtualized network architectures using various network transport types

    - ■ Extracts control from underlying hardware, making it a software-based architecture

  - ○ How SD-WAN Works

    - ■ Uses a centralized control function to securely and intelligently redirect traffic

- Can layer over multiple types of network transport, such as MPLS, cellular, microwave, or broadband internet services

- Identifies network applications used by end-users and routes data across the WAN accordingly

○ Comparison with Traditional WAN

- Unlike traditional WAN architectures, SD-WAN offers dynamic and efficient routing

- Provides improvements in visibility, performance, and manageability from a centralized point

- Addresses the inefficiencies of traditional star topologies, improving user experience and productivity

○ Use Cases

- Ideal for large enterprises with geographically dispersed branch offices

- Particularly useful for enterprises moving towards cloud-based environments (IaaS, PaaS, SaaS)

- Helps increase performance for end-users and reduce bottlenecks caused by traditional WAN architectures

○ Future Considerations

- Important for enterprises to consider SD-WAN as work environments become more geographically dispersed

- Not just about keeping pace with digital transformation, but also about anticipating future challenges and capitalizing on opportunities

- ○ Security and Career Advancement

    - ■ <u>Elevates organizational security posture</u>

    - ■ <u>Helps in migrating more heavily into cloud-based environments</u>, aiding in career advancement

- **Virtual Extensible Local Area Network (VXLAN)**

    - ○ *Virtual Extensible Local Area Networks (VXLAN)*

        - ■ A network virtualization technology that <u>addresses limitations of traditional networks by creating larger, more agile virtual networks</u>

        - ■ <u>A network overlay technology that encapsulates Ethernet frames within UDP packets</u>

        - ■ <u>Extends layer 2 networks over layer 3 infrastructure, enabling virtualized networks across physical networks</u>

        - ■ Scalability

            - ● VXLAN uses a 24-bit VXLAN Network Identifier (VNI), supporting over 16 million virtual networks, compared to the 4,096 limit of traditional VLANs

    - ○ Components

        - ■ *VXLAN Tunnel Endpoints (VTEPs)*

            - ● Entities that encapsulate and de-encapsulate Ethernet frames into VXLAN packets

            - ● Typically implemented in hypervisors or physical network switches

- ■ *VXLAN Segments*
    - ● Layer 2 networks overlaid onto layer 3 networks, identified by the unique 24-bit VXLAN Network Identifier (VNI)
- ○ Benefits
    - ■ Scalability
        - ● Supports up to 16 million virtual networks
    - ■ Flexibility
        - ● Can traverse layer 3 networks without changes to the underlying network
    - ■ Improved Utilization
        - ● Optimizes network traffic flows within and across data centers
- ○ Real-World Use
    - ■ Facilitates communication between virtual machines across different servers in data centers
    - ■ Especially useful when servers are spread across multiple locations
- ○ Challenges
    - ■ Configuration Complexity
        - ● Requires understanding of layer 2 and layer 3 networking, as well as network overlays
    - ■ Latency and Packet Size
        - ● Encapsulation and decapsulation processes can introduce latency and increase packet size

- Multicast Support

  - Requires multicast support within the underlying network for broadcasting and unknown unicast traffic

  ○ Simplification

  - Deployment can be simplified with management and orchestration tools that automate configuration and management, especially in cloud-based networks

  ○ Conclusion

  - <u>VXLAN is a significant advancement in network virtualization, providing extensible, scalable, and efficient virtual networks</u> over existing architectures, essential for designing and managing advanced network solutions in modern distributed networks

- **SASE and SSE**

  ○ SASE and SSE Overview

  - <u>SASE and SSE are network security architectures blending traditional network services with comprehensive security functions</u>

  - They represent an evolution from a decentralized security model to a unified cloud-centric approach

- ○ *Secure Access Service Edge (SASE)*
    - ■ Consolidates wide area networking (WANs) and security functions into a single cloud-native service for secure, seamless user access regardless of physical location
    - ■ Key Feature
        - ● Utilizes Software-Defined Networking (SDN) for security and networking services from the cloud, offering flexibility, scalability, and cost efficiency
    - ■ SASE Security Services
        - ● Firewalls
        - ● VPNs
        - ● Zero-trust network access
        - ● Cloud Access Security Brokers (CASBs)
        - ● Delivered through common policy and management platforms for networking goals
    - ■ SASE Benefits
        - ● Addresses challenges of securing and connecting distributed users and data across branch offices, remote workers, and cloud environments
        - ● Provides secure, fast, and reliable access to cloud-based resources for users and devices

- Cloud Provider Solutions

  - AWS

    - Offers Virtual Private Cloud (VPC) for secure network infrastructure

      - Enables creation of virtual networks in the cloud and connected to on-premise data centers or other AWS services

  - Azure

    - *Azure Virtual WAN*

      - Provides secure global and efficient connectivity between branch offices, data centers, and Azure resources

    - *Azure ExpressRoute*

      - Enables creation of a dedicated, private connection between an Azure data center and an on-premise network infrastructure

  - Google Cloud Platform

    - *Google Cloud Interconnect*

      - Allows connection of an on-premise infrastructure to the Google cloud platform (GCP) over a dedicated private connection

- ○ *Google Cloud VPN*
    - ■ Allows secure connection of an on-premise infrastructure to a virtual private cloud network through an IP sec VPN tunnel
- ○ *Security Service Edge (SSE)*
    - ■ A key subset of SASE that focuses exclusively on security services for protecting access between users, devices, and the cloud
    - ■ Key Technologies
        - ● *Secure Web Gateways*
            - ○ Inspect and filter unwanted software and malware from web and internet traffic
        - ● *Cloud Access Security Brokers (CASBs)*
            - ○ Monitor and control data shared with cloud applications for visibility, compliance, and threat protection
        - ● *Zero-Trust Network Access (ZTNA)*
            - ○ Treats every access attempt as untrusted, granting access based on user/device identity and context
    - ■ SSE Benefits
        - ● Provides comprehensive and adaptable security measures for a cloud-centric world

- Reduces attack surface and mitigates internal threats through

  strict access controls

Network Security Fundamentals

Objectives:

- 4.1 - Explain the importance of basic network security concepts
- 4.3 - Given a scenario, apply network security features, defense techniques, and solutions

- **The CIA Triad**
    - *CIA Triad*
        - Fundamental to network security comprising Confidentiality, Integrity, and Availability
    - *Confidentiality*
        - Ensures data privacy using encryption and authentication
        - *Symmetric Encryption*
            - Both sender and receiver use the same key for encryption and decryption
            - Fast but challenging for key management
        - *Asymmetric Encryption*
            - Involves a key pair
                - Public key – known to everyone
                - Private key – known only to the owner

- Sender uses the receiver's public key to encrypt the data, ensuring confidentiality
- In e-commerce, asymmetric keys are used to exchange a symmetric key for secure communication.
    - <u>Key exchange</u> process
        - Client requests a secure website using HTTPS
        - Server provides its public key with a digital certificate
        - Client encrypts a random number with the server's public key and sends it back
        - Server decrypts the number using its private key
        - Both parties use the random number as a symmetric key for secure communication
- *Integrity*
    - Verifies data is not modified in transit or storage, preventing spoofing and unauthorized data changes
    - *Hashing*
        - Algorithm creates a unique fingerprint for data, allowing verification of data integrity

- ○ *Availability*

    - ■ Ensures data accessibility

    - ■ Can be achieved through redundant network design and components

    - ■ Threats to Availability

        - ● Network floods

        - ● Hardware failures

        - ● Power outages

        - ● Other disruptions

- **Threats and Vulnerabilities**

    - ○ Risk exists where threats and vulnerabilities intersect within networks

    - ○ Understanding the different threats and vulnerabilities can add protection mechanisms to help mitigate risks

    - ○ *Threat*

        - ■ <u>Person or event</u> that has the potential to negatively impact valuable resources

            - ● Hackers

            - ● Hurricanes

    - ○ *Vulnerability*

        - ■ <u>Weakness in system design, implementation, or lack of preventive mechanisms</u>

- - ■ <u>Usually within the user's control</u>
      - Running outdated software
      - Insufficient battery backup
  - *Risk*
    - Occurs when a threat exploits a vulnerability
    - No risk if no threat targets a vulnerability or if no vulnerability exists
  - Types of Threats
    - *Internal Threat*
      - Originates from within the organization
        - Malicious employee
        - Unknowing end user
    - *External Threat*
      - Originates from outside the organization
        - Hackers
        - Environmental events
  - Types of Vulnerabilities
    - *Environmental Vulnerabilities*
      - Weaknesses in the surrounding area affecting services
        - Hurricanes
        - Earthquakes

- *Physical Vulnerabilities*
  - Weaknesses in the building infrastructure
    - Unlocked doors
    - Misconfigured systems
- *Operational Vulnerabilities*
  - Weaknesses in policies and procedures
    - Poorly enforced policies
- *Technical Vulnerabilities*
  - System-specific weaknesses
    - Misconfigurations
    - Outdated hardware
    - Malicious softwares
  - *Common Vulnerabilities and Exposures (CVEs)*
    - List of publicly disclosed vulnerabilities – known vulnerabilities
    - Provides details on vulnerabilities and affected software
  - *Zero-Day Vulnerabilities*
    - Newly discovered vulnerabilities
    - Exploited before a patch is available
- *Exploiting Vulnerability*
  - Taking advantage of a vulnerability as a threat actor

- ■ *Exploit*

  - ● Software code that takes advantage of a vulnerability

- ■ Prevention

  - ● Keep systems updated with latest patches

  - ● Use up-to-date anti-malware software

- ● **Risk Management**

  - ○ *Risk Management*

    - ■ Involves identifying, evaluating, and prioritizing risks

    - ■ Aims to allocate resources to minimize, monitor, and control the probability or impact of vulnerabilities being exploited by threats

  - ○ *Risk Assessment*

    - ■ Process to identify potential hazards and analyze their likelihood and consequences

    - ■ Determines an organization's tolerance for such events occurring

  - ○ Types of Risk Assessments

    - ■ *Security Risk Assessment*

      - ● Identifies, assesses, and implements key security controls within an application, system, or network

      - ● *Threat Assessment*

        - ○ Focuses on identifying different threats that may harm systems or networks

- ○ *MITRE ATT&CK Framework*
    - ■ A knowledge base of adversary tactics and techniques, derived from real-world observations
    - ■ Allows administrators or analysts to understand the methods used by threats to harm networks
    - ■ Helps identify where to focus resources for better protection
- ● *Vulnerability Assessment*
    - ○ Identifies, quantifies, and prioritizes risks and vulnerabilities
    - ○ Uses vulnerability scanner tools
        - ■ Nessus
        - ■ QualysGuard
        - ■ OpenVAS
- ● *Penetration Test*
    - ○ Attempts to exploit vulnerabilities within the system or network for evaluation of an IT infrastructure security
    - ○ Validates the effectiveness of defensive mechanisms and adherence to security policies
- ● *Posture Assessment*
    - ○ Assesses an organization's attack surface to understand its cyber risk posture and exposure to threats

- ○ Includes four main steps:
    - ■ Defining mission-critical components
    - ■ Identifying strengths, weaknesses , and security issues
    - ■ Strengthening security position
    - ■ Staying in control
- ■ *Business Risk Assessment*
    - ● Identifies, understands, and evaluates potential hazards in the workplace
    - ● *Process Assessment*
        - ○ Examines processes used by an organization against a set of criteria to determine their capability to perform within quality, cost, and schedule goals
    - ● *Vendor Assessment*
        - ○ Evaluates a prospective vendor to determine if they can effectively meet the business's obligations and needs regarding the product
        - ○ Importance
            - ■ Ensures vendors and suppliers implement and maintain appropriate security controls.
            - ■ Mitigates the threat of supply chain vulnerabilities, such as counterfeit devices with malware

- **Audits and Compliance**
    - Audits and Compliance
        - Critical for ensuring data integrity, confidentiality, and availability
        - Organizations span across geographical borders, subject to various laws and regulations
    - *Data Locality*
        - Refers to geographic location where data is stored and processed
        - Influenced by legal and regulatory requirements
            - Every country has its own laws governing data protection, privacy, and sovereignty
    - *Payment Card Industry Data Security Standard (PCI DSS)*
        - Security standards for companies handling credit card information
        - Not a law but a contractual requirement for handling cardholder data
    - *General Data Protection Regulation (GDPR)*
        - European Union (EU) regulation focusing on data protection and privacy
        - Applies to all organizations operating within the EU or offering goods/services to individuals inside the EU
        - Provides individuals with greater control over their personal data
            - Right to be informed
            - Right of access
            - Right to rectification
            - Right to erasure

- Right to restrict processing
- Implementation and Compliance
  - Implement continuous monitoring and auditing programs
  - Regular audits to ensure compliance with relevant standards and regulations
  - Employee training on auditing and compliance processes
    - Also includes implications of non-compliance
      - Potential legal and financial penalties
  - Develop clear policies and procedures for data handling, access control, and incident response

- **Device Hardening**
  - *Device Hardening*
    - Refers to ensuring that a device has had any unnecessary application or port disabled or removed from the host
    - Process of securing a host system by reducing its attack surface
    - Key Practices
      - Run only necessary services
      - Install monitoring software for malware protection
      - Establish a maintenance schedule for system patching
    - Applies to endpoint devices, servers, network infrastructure, and mobile devices

- Endpoint Security Software

  - Install anti-malware, antivirus, spam filters, host-based firewalls, and log collection agents

  - Enhances security posture and threat detection capabilities

- Specialized Hardware

  - Manufacturers add secure hardware like UEFI, TPM, and HSM

  - Aids in securing devices, especially as networks become more de-perimeterized

- Host Hardening Practices

  - Ensure all software is patched and up-to-date

  - Ensure that device is properly configured

  - Remove unnecessary applications.

  - Block unnecessary ports and services

  - Control external storage devices tightly

  - Disable unneeded accounts

  - Rename default accounts

  - Change default passwords

- Additional Host Hardening Practices

  - Configure standardized OS baselines

  - Implement allow and deny lists for applications

  - Use security and group policies

  - Restrict command line interface and peripheral device usage

- ○ Balancing Security and Usability

    - ■ Open the least amount of ports

    - ■ Run the least amount of services needed

- ○ Network Interfaces

    - ■ Disable unneeded network connections

    - ■ Consider wired, wireless, and management LAN interfaces

- ○ Services

    - ■ Disable unused services (e.g., CUPS daemon for print server)

- ○ Ports

    - ■ Close ports not needed for services

    - ■ Use host-based firewalls for further hardening

- ○ Disk Encryption

    - ■ Enable full disk encryption or use self-encrypting drives

    - ■ Protects data at rest from unauthorized access

- ○ Account Review

    - ■ Disable or delete unused accounts

    - ■ Follow the rule of thumb

        - ● Disable, delete, or block anything unused or unneeded

- ○ Consideration of Device Lifecycle

    - ■ *End of Life (EOL)*

        - ● Date when a manufacturer will no longer sell a given product

- ■ *End of Support (EOS)*
  - ● Last date that a manufacturer will support a given product
- ■ <u>Ensure devices are always using supported and up-to-date software to prevent vulnerabilities</u>

- ● **Understanding Device Hardening: Demonstration**

- ● **Physical Security**
  - ○ Physical Security in Networking
    - ■ Importance of Physical Security
      - ● Protecting networking equipment is crucial to prevent unauthorized access and tampering
  - ○ *Detection Mechanisms*
    - ■ Refer to security controls that are used during an event to find out whether or not something malicious may have happened
    - ■ Cameras
      - ● Used to monitor entrances, exits, and critical areas
      - ● Types
        - ○ Wired
          - ■ Allows the device to be physically cabled from the camera to a central monitoring station

- ○ Wireless

    - ■ No physical cables

    - ■ Susceptible to interference

- ○ Outdoor

    - ■ Should be able to withstand elements

- ○ Indoor

    - ■ Monitors things contained inside the building

    - ■ Lighter, cheaper, and easier to install

- ○ PTZ (Pan, Tilt, Zoom) Camera

- ○ *Infrared Camera*

    - ■ Displays images based on the amount of heat in the room

- ○ *Ultrasonic Camera*

    - ■ Uses sound-based detection

- ○ *Prevention Mechanisms*

    - ■ Controls that are put in place to prevent things from happening

    - ■ Access Control Hardware

        - ● Controls access to secure areas

        - ● Badge Readers

            - ○ Rely on either a magnetic strip, a chip card, or RFID

        - ● Biometric Readers

            - ○ Fingerprint, retina scans, or voice prints

- **Two-factor authentication can be added for more secure data center**
- Access Control Vestibules
  - Area between two doorways for authentication
  - Used in high-security facilities
  - Example
    - Turnstiles
- Smart Lockers
  - Used to store personal electronic devices
  - Can be accessed using employee badges
- Locking Racks and Cabinets
  - Protect networking equipment from tampering
  - Controlled by a key custodian
  - Standard server and networking equipment rack
    - 48 units high
    - 50 inches deep
    - 20 inches wide
- Employee Training
  - Crucial for preventing security breaches
  - Provides awareness of security policies and procedures
  - Reduces vulnerabilities caused by misconfiguration or user error
  - Offers a high return on investment for companies of all sizes

- **Honeypots and Active Defense**
  - *Active Defense*
    - Practice of responding to threats by destroying or deceiving the threat actor's capabilities
    - Involves having an engagement with the adversary
  - *Honeypot*
    - A host or server set up to attract attackers, allowing organizations to observe and learn from their attack methods
    - A form of active defense, designed to lure attackers away from critical network components
    - Can be a single host or part of a larger network (Honeynet), enticing attackers with seemingly valuable information
  - Active Defense Strategies
    - *Attribution*
      - Involves identifying and publishing an attacker's methods, techniques, and tactics for threat intelligence
      - Helps security researchers and organizations understand and counteract specific threats
    - *Annoyance Strategies*
      - Use techniques like obfuscation to waste attackers' time and resources

- Examples
  - Bogus DNS entries
  - Decoy directories on web servers
  - Port triggering and spoofing
- Hack Back
  - Involves offensive techniques to identify and degrade attackers' capabilities
  - Legally and ethically complex, often discouraged due to legal and reputational risks
- Legal Considerations
  - Active defense strategies, especially hack back, have significant legal implications
  - Understand and comply with local laws and regulations before considering these strategies

Network Attacks

Objective 4.2: Summarize various types of attacks and their impact to the network

- **Dos and DDos Attacks**
  - *Denial of Service (DoS) Attack*
    - Occurs when one machine overwhelms a victim system with continuous service requests
    - Leads to resource exhaustion, causing the victim system to crash
    - *TCP SYN Flood*
      - Involves initiating multiple TCP sessions without completing them
      - TCP Handshake – in a normal scenario, involves SYN, SYN/ACK, and ACK packets
      - Attack Process – attacker sends SYN packets, victim reserves resources, but attacker ignores subsequent SYN/ACK packets, leading to half-open connections and resource exhaustion
      - Attacker often spoofs source IP during the three-way handshake to flood the server
    - *SMURF Attack (ICMP Flood)*
      - Utilizes ICMP traffic instead of TCP traffic

- Attacker sends ping to subnet broadcast address with a spoofed source IP, causing all devices on the subnet to respond to the victim server
- Attack can be intensified by sending multiple requests to different subnets, leading to resource exhaustion
- *Distributed Denial of Service (DDoS) Attack*
  - Involves multiple machines simultaneously overwhelming a single server
  - *Botnet*
    - Collection of compromised computers under the control of a Command and Control (C2) server
  - *Zombie*
    - Individually compromised computers within a botnet
  - C2 server controls all zombies, allowing coordinated attacks
- Preventing DDoS Attacks
  - Cloud Challenge – cloud-based resources can horizontally scale to handle increased demand
  - Cost Consideration – despite scaling, organizations may face substantial costs for illegitimate traffic during DDoS attacks
  - Prevention Importance – emphasizes the need to implement preventive measures to avoid financial and operational consequences

- **MAC Flooding**
  - *MAC Flooding*
    - A network attack technique aimed at compromising a switch's security by overflowing its MAC table
  - Normal Switch Operation
    - Utilizes MAC tables to associate MAC addresses with switchports for efficient data forwarding
  - Attack Implications
    - Data Snooping
      - Attackers are enabled to capture sensitive data by forcing the switch into hub mode
    - Disruption of Services
      - Network performance is degraded and may lead to Denial-of-Service attacks
    - Bypassing Security Measures
      - MAC flooding allows attackers to circumvent MAC address filtering and gain unauthorized network access
  - Execution of MAC Flooding
    - Attackers use specialized tools to flood the switch with random MAC addresses, forcing it into fail-safe mode
  - Detection and Prevention
    - Implement anomaly-based intrusion detection systems (IDS)

- Employ network monitoring tools

- Configure port security

- Set MAC address limits per switchport

- Use VLANs to segregate network traffic and limit the impact of MAC flooding attacks

- **Address Resolution Protocol (ARP) Attacks**
  - *Address Resolution Protocol (ARP)*
    - Used to map IP addresses to MAC addresses on a local area network
  - *ARP Spoofing*
    - Occurs when an attacker sends falsified ARP messages, linking their MAC address with a legitimate IP
    - Goals are to intercept, modify, or stop data-in-transit, and initiate on-path attacks
  - *ARP Poisoning*
    - Corrupts ARP cache by associating attacker's MAC with IP addresses of LAN devices
    - Enables alteration of network traffic flow, interception, session hijacking, or DoS attacks
  - Difference between ARP Spoofing and ARP Poisoning
    - ARP Spoofing – Targets single host's traffic
    - ARP Poisoning – Affects all hosts in a LAN

- ○ Motivations for ARP Attacks

  - ■ Data Interception

  - ■ On-Path Attack

  - ■ Network Disruptions

- ○ Techniques for ARP Attacks

  - ■ Scanning network for IP-MAC pairs and sending fake ARP responses

  - ■ Conducting ARP poisoning via ARP flood

- ○ Detection and Prevention

  - ■ Use ARP monitoring tools to detect unusual ARP traffic patterns

  - ■ Alert network administrators

  - ■ Configure intrusion detection systems to identify ARP spoofing or poisoning activities

  - ■ Implement preventive measures

    - ● Static ARP entries

    - ● Dynamic ARP inspection

    - ● Network segmentation

    - ● VPNs or encryption technologies

- **VLAN Hopping**

  - ○ *Virtual Local Area Network(VLAN)*

    - ■ Segregates broadcast domains at Layer 2 of the OSI model, enhancing network security

- Commonly utilized in intranets and local area networks to partition and secure network segments
  - *VLAN Hopping*
    - Exploits misconfigurations to gain unauthorized access to different VLAN
    - *Double Tagging*
      - Attacker exploits trunk port vulnerabilities to direct traffic to another VLAN
        - Inner tag
          - Contains the true destination
        - Outer tag
          - Denotes the native VLAN
        - Purpose of VLAN Hopping
          - Blind attacks
            - Commands are sent to the victim, but the attacker or pen tester does not get to see any of the responses
          - Denial of Service (DoS) or Stress Testing
            - Does not always require response data, facilitating various attack scenarios
        - Prevention Measures
          - Change the default configuration of the native VLAN from VLAN ID 1 to another identifier

■ Avoid adding user devices to the native VLAN

■ *Switch Spoofing*

● Attackers use Dynamic Trunking Protocol (DTP) to negotiate trunk ports

● Disabling dynamic switch port modes helps prevent switch spoofing attacks

■ *MAC Table Overflow*

● Overloading CAM tables can cause switches to act like hubs, exposing traffic from other VLANs

● Flood the switch's CAM table with MAC addresses to induce this behavior

○ By grasping these key concepts and preventive measures, you can better understand and mitigate VLAN hopping vulnerabilities

● **Domain Name System (DNS) Attacks**

○ *Domain Name System (DNS)*

■ Fundamental internet component translating domain names to IP addresses

○ *DNS Cache Poisoning*

■ Corrupting DNS resolver cache with false information to redirect traffic

- Mitigations:
  - Utilize Domain Name System Security Extensions (DNSSEC) to add a digital signature
  - Implement secure network configurations and firewalls
- *DNS Amplification Attacks*
  - Overwhelm target system with DNS response traffic
  - Limit size of DNS responses or rate limit DNS response traffic for mitigation
- *DNS Tunneling*
  - Involves using the DNS protocol to encapsulate non-DNS traffic (such as HTTP or SSH, over port 53) to attempt to bypass firewall rules
  - Can be used for command and control or data exfiltration
  - Mitigation involves regularly monitoring of DNS logs to analyze for any signs of unusual patterns of behavior
- *Domain Hijacking*
  - Unauthorized change of domain registration
  - Can lead to redirection to malicious websites
  - Mitigations:
    - Conduct regular updates
    - Ensure that registration account information is secure
    - Use domain registry lock services

- ○ *DNS Zone Transfer Attacks*

    - ■ Pretend to be authorized system to get entire DNS zone data

    - ■ Expose sensitive network infrastructure information

- ○ DNS attacks exploit vulnerabilities to disrupt services, steal information, or redirect traffic

- **On-path Attack**

    - ○ *On-Path Attack*

        - ■ An attack where the penetration tester places their workstation between two hosts to capture, monitor, and relay communications

        - ■ Captures authorization packets, allowing the attacker to take over the authorized session between client and server

        - ■ Methods of On-Path Attack

            - ● ARP Poisoning

            - ● DNS Poisoning

            - ● Rogue Wireless Access Point

            - ● Rogue Hub/Switch

    - ○ *Replay Attack*

        - ■ Occurs when an attacker captures valid data and repeats it either immediately or with a delay

- ■ Example
    - ● Capturing authentication handshake to gain access to network resources
- ○ *Relay Attack*
    - ■ An attack where the attacker becomes a proxy between two hosts, intercepting and potentially modifying communications
    - ■ Example:
        - ● Modifying transaction details in online banking to divert funds
- ○ Challenges with Encryption
    - ■ SSL/TLS Encryption poses difficulty in intercepting and cracking communications
    - ■ Techniques to overcome challenges with encryption:
        - ● *SSL Stripping*
            - ○ Redirecting HTTPS requests to HTTP to capture unencrypted data
        - ● Downgrade Attack
            - ○ An attack that persuades client or server to adopt lower security modes
            - ○ Convinces systems to abandon higher security modes in favor of lower ones

- ○ Example:
    - ■ Allowing encryption at lower levels (e.g., SSL 2.0) to facilitate easier interception
  - ○ Not limited to SSL/TLS
    - ■ Applicable to any encryption or protection mechanism like WiFi, VPNs, etc.

- **Rogue Device and Attacks**
  - ○ *Rogue Devices*
    - ■ Unauthorized devices or services on a network that allows unauthorized individuals to connect to that network
    - ■ Identified by MAC address and IP address
    - ■ Use digital certificates for authentication and encryption (IPsec, HTTPS) to authorize devices
  - ○ *Rogue System Detection*
    - ■ Process of identifying and removing machines on the network that are not supposed to be there
  - ○ Types of Rogue Systems
    - ■ *Network Taps*
      - ● Physical device that is attached to cabling to record packets passing over the network segment

- ■ *Wireless Access Points (WAPs)*
  - ● Devices that can be connected to the network and extend the physical network into the wireless spectrum
  - ● Types of Rogue Access Points
    - ○ Connected to a network
      - ■ Allows adversaries to convert radio signals into physical network access
    - ○ Evil Twin
      - ■ Attacker sets up own access point with his own internet connection, masquerading as legitimate network
  - ● Scanning airwaves to identify and remove rogue devices is crucial
  - ● Tools like Wi-Fi Pineapple enable easy creation of rogue access points, posing significant threats to unsuspecting users
- ■ *Servers*
  - ● Set up as honeypots to harvest data
- ■ *Wired/Wireless Clients*
  - ● Personal devices connected to network
  - ● Bring Your Own Device Policy
    - ○ Personal devices are not considered as rogue devices unless they are used to do things that are unauthorized

- ■ *Unauthorized Software*

    - ● Installed without permission

- ■ *Virtual Machines*

    - ● Created within highly virtualized environments

- ■ *Smart Appliances*

    - ● Vulnerabilities in internet-connected devices

- ○ Detection and Removal

    - ■ *Visual Inspection*

        - ● Checking ports and switches for rogue devices

    - ■ *Network Mapping and Host Discovery*

        - ● Use enumeration scanners to identify hosts

    - ■ *Wireless Monitoring*

        - ● Detect unknown SSIDs within range

    - ■ *Packet Sniffing and Traffic Flows*

        - ● Identify unauthorized protocols and peer-to-peer communication

    - ■ *NAC and Intrusion Detection*

        - ● Use automated network scanning for prevention and detection

- ○ Mitigation

    - ■ Use digital certificates and encryption for authentication

    - ■ Perform regular inventories to detect additional or rogue devices

    - ■ Implement network access control (NAC) and intrusion detection systems (IDS) for automated scanning and defense

- ○ <u>Key Points</u>
    - ■ Rogue devices can compromise network security
    - ■ Detection and removal are crucial for network integrity

- **Social Engineering Attacks**
    - ○ *Social Engineering*
        - ■ Any attempt to manipulate users into revealing confidential information or performing actions detrimental to the user or system security
        - ■ Focus
            - ● <u>Exploiting human vulnerabilities</u> to bypass technical controls
    - ○ Types of Social Engineering Attacks
        - ■ *Phishing*
            - ● Sending deceptive emails to trick users into revealing sensitive information
            - ● Example
                - ○ Fake PayPal email requesting account information
            - ● Effectiveness
                - ○ High, even with obvious signs of phishing
            - ● Variants
                - ○ Phishing – most broad type, does not target any particular person
                - ○ Spear phishing – more targeted form

- ○ Whaling – targets key executives
- ■ *Tailgating*
  - ● Unauthorized entry into secure areas by following an authorized person
  - ● Prevention
    - ○ Train employees to shut doors behind them
- ■ *Piggybacking*
  - ● Gaining entry to a secure area with an employee's consent
  - ● Example
    - ○ Asking someone to hold the door open with hands full
- ■ *Shoulder Surfing*
  - ● Gaining authentication information by direct observation
  - ● Example
    - ○ Watching someone type their password
- ■ *Eavesdropping*
  - ● Listening in on conversations to gather sensitive information
  - ● Example
    - ○ Overhearing business discussions to gain insights
- ■ *Dumpster Diving*
  - ● Scavenging for personal or confidential information in trash or recycling

- Prevention

    - Shred paperwork before disposal or use locked trash cans

- **Understanding Phishing Attacks: Demonstration**

- **Malware Attacks**

    - *Malware*

        - Short-hand term for malicious software

        - Designed to infiltrate a computer system and possibly damage it without the user's knowledge or consent

    - Malware Types

        - *Virus*

            - Malicious code that <u>infects a computer when run</u>

        - *Worm*

            - <u>Self-replicating malware that spreads without user interaction</u>

            - Exploits security vulnerabilities in OS, protocols, or applications

            - Notable Examples

                - Nimda (2001) – infected the entire internet in 22 minutes

                - Conficker (2009) – infected 9-15 million machines, creating a botnet

        - *Trojan Horse*

            - Malware disguised as legitimate software

- *Remote Access Trojan (RAT)*
  - A common type of Trojan that provides the attacker with remote control of a victim's system
- *Ransomware*
  - Malware that restricts access until a ransom is paid
  - Encrypts files or changes passwords, demanding payment for access
  - Notable Example
  - SamSam (2018) – cost Atlanta over $17 million to fix
- *Spyware*
  - Malware that gathers information without consent
  - Types
    - Adware – for advertising
    - Keylogger – captures keystrokes
- *Rootkit*
  - Malware that gains administrative control without detection
  - Difficult to detect, often requires booting from an external device
- Prevention and Best Practices
  - Always check files for malware before downloading or installing
  - Keep software up to date to patch vulnerabilities
  - Use reputable antivirus software and firewalls
  - Educate users about safe browsing and downloading practices

- **Understanding Malware Attacks: Demonstration**

Logical Security

Objectives:

- 1.4 - Explain common networking ports, protocols, services, and traffic types
- 4.1 - Explain the importance of basic network security concepts
- 4.3 - Given a scenario, apply network security features, defense techniques, and solutions

- **Identity and Access Management (IAM)**
  - *Identity and Access Management (IAM)*
    - Security process for identification, authentication, and authorization of users, computers, and entities
    - Provides access to organizational assets like networks, operating systems, and applications
  - Unique Subjects in IAM
    - *Personnel*
      - Employees with user accounts and access to the system
    - *Endpoints*
      - Devices (desktops, laptops, tablets, cell phones) used to access the network

- **■ *Servers***
    - **●** Machines for machine communication, containing mission-critical systems and encryption
- **■ *Software***
    - **●** Applications requiring IAM, often using digital certificates
- **■ *Roles***
    - **●** Define permissions based on the function an asset fulfills, applicable to personnel, endpoints, servers, and software
    - **●** In Windows
        - **○** People are assigned to different groups then permissions are given to those groups
- **○** IAM Systems and tools
    - **■** Directory services and repositories
    - **■** Access management tools
    - **■** Auditing and reporting systems
- **○** IAM Tasks
    - **■** Account Creation and Deprovisioning
        - **●** Provisioning new accounts and disabling/deleting existing accounts
    - **■** Account Management
        - **●** Resetting passwords
        - **●** Updating digital certificates

- Managing permissions
  - Account Auditing
    - Reviewing account activity to ensure legitimacy
  - Evaluating Identity-based Threats
    - Identifying and mitigating threats to IAM systems
  - Maintaining Compliance
    - Ensuring the system meets security requirements and standards
- IAM Risks
  - Biggest risk is the risk caused by accounts
    - *User Accounts*
      - Standard accounts with basic permissions
      - Least risky
    - *Privileged Accounts*
      - Administrator, root, or superuser accounts with elevated permissions, requiring additional auditing
    - *Shared Accounts*
      - Used in small office environments, posing a risk due to shared passwords and lack of individual accountability
      - Not recommended

- **Multifactor Authentication (MFA)**
  - *Multifactor Authentication (MFA)*
    - Means authenticating or proving identity using more than one method
    - At least two methods are required for MFA
  - Categories
    - *Something You Know*
      - A knowledge factor
        - Username
        - Password
        - PIN
        - Answers to personal questions
      - *Two-factor Authentication (2FA)*
        - A combination of two MFA categories
        - Use 2FA to increase security
        - A common misconception is that a username and password constitute 2FA
          - Both are from the knowledge factor, making it a single factor
    - Passwords
      - Weaknesses of Passwords
        - Unchanged default credentials
        - Common passwords

- - ■ Weak or short passwords
  - ○ Attacks Against Passwords
    - ■ *Dictionary Attack*
      - ● Guessing the password using every word or phrase in a dictionary, including variations like substituting symbols for letters
    - ■ *Brute Force Attack*
      - ● Trying every possible combination until the correct password is found
    - ■ *Hybrid Attack*
      - ● A combination of dictionary and brute force methods, using keywords related to the individual's life
  - ○ Prevention of password attacks
    - ■ Password Length and Complexity
      - ● Longer and more complex passwords are harder to crack
        - ○ Uppercase
        - ○ Lowercase
        - ○ Numbers
        - ○ Special characters

- - ○ At least 12 characters long for good security

    - ■ *Something You Have*
        - A possession factor
            - ○ Smart card
            - ○ RSA key fob
            - ○ RFID tag

    - ■ *Something You Are*
        - An inherence factor
            - ○ Fingerprints
            - ○ Retina scans
            - ○ Voiceprints
        - Often used in high-security environments

    - ■ *Something You Do*
        - An action factor
            - ○ The way a person signs his/her name, draws a pattern, or says a catchphrase

    - ■ *Somewhere You Are*
        - A location factor
            - ○ *Geotagging*
                - ■ Used to authenticate based on the current GPS location of a device

- ○ *Geofencing*

  - ■ Used to track devices and receive alerts if they enter or leave a predefined area

  - ● Used to ensure that devices are in an authorized location for authentication

- **Authentication Methods**

  - ○ *Authentication*

    - ■ The process of determining whether someone or something is who/what they claim to be

  - ○ *Local Authentication*

    - ■ Username/password verification stored locally

    - ■ Example

      - ● Personal laptop login

  - ○ *LDAP (Lightweight Directory Access Protocol)*

    - ■ Centralized client/object database

    - ■ Contains a hierarchal organization of the users, groups, servers, and systems in the network

    - ■ Port

      - ● 389 – plain text

      - ● 636 – secure

- ■ Platforms
  - ● Unix
  - ● Linux
  - ● Mac
  - ● Windows
- ■ Example
  - ● Validating user/password over the network
- ○ *Kerberos*
  - ■ Windows domain authentication/authorization
  - ■ *Mutual authentication*
    - ● User verifies server, server verifies user
  - ■ *Key Distribution Center (KDC)*
    - ● Issues tickets for authentication and ticket granting
    - ● Tickets
      - ○ Ticket Granting Ticket (TGT)
      - ○ Service ticket/session key
  - ■ Port 88
  - ■ Example
    - ● Windows domain environment
- ○ *SSO (Single Sign-On)*
  - ■ Single login for multiple resources

- Works by creating trust relationships between various applications and resources
- Benefit
  - Simplifies access, reduces password management
- Drawback
  - Compromised credentials give access to all resources
  - MFA can help keeping secure access
- Example
  - Using Google account to log in to various services

○ *SAML (Security Assertion Markup Language)*

- XML-based authentication data exchange
- Usage
  - SSO or federated identity management
- Roles
  - Service provider
  - User agent (e.g., web browser)
  - Identity provider
- Example
  - Using Google as an identity provider to access a website

○ *RADIUS (Remote Authentication Dial-In User Service)*

- Centralized administration for authentication

- Usage
  - Dial-up
  - VPN
  - Wireless authentication
- Protocol
  - UDP
    - Port 1812 – for authentication
    - Port 1813 – for accounting
- A cross-platform standard

○ *TACACS+ (Terminal Access Controller Access-Control System Plus)*

- Cisco proprietary authentication/authorization
- Usage
  - 802.1X network authenticator
- Protocol
  - TCP (slower than RADIUS)
- Benefits
  - Can provide some additional security features
  - Can be used to independently conduct authentication, authorization, and accounting processes
  - Supports all major network protocols
    - Requires Cisco devices

- ○ *Time-Based Authentication*
    - ■ A security mechanism that will generate temporary dynamic password or token that is valid for a short period of time
    - ■ Most often implemented as TOTP (Time-Based One-Time Passwords)
    - ■ Part of MFA
    - ■ Benefit
        - ● Enhances security, resistant to replay attacks
    - ■ Implementation
        - ● Software (Google Authenticator)
        - ● Hardware (RSA Key fob)

- **Security Principles**
    - ○ *Least Privilege*
        - ■ Users should use the lowest level of permissions necessary to complete job functions
        - ■ Administrators should only use elevated privileges when necessary
        - ■ Applies to user accounts, system designs, and network configurations
    - ○ Role-based Access
        - ■ Methods of Access Control
            - ● *Discretionary Access Control (DAC)*
                - ○ Access control method where owners of resources determine access permissions

- ○ Owners assign permissions to files or folders they create
- ○ Challenges
  - ■ Ensuring every object has an owner
  - ■ Owners set appropriate permissions
- ● *Mandatory Access Control (MAC)*
  - ○ Access control policy where the computer system determines access
  - ○ Uses data labels to assign trust levels to subjects and objects
  - ○ Commonly used in military systems for highly classified information
  - ○ *Need-to-Know Principle*
    - ■ Users must have both the necessary clearance level and a need to know to access information
    - ■ Ensures access is restricted to only those who require it for their job functions
- ● *Role-Based Access Control (RBAC)*
  - ○ Access control model based on defining roles for job functions
  - ○ Permissions are assigned to roles, and users are assigned to roles

○ Users inherit permissions based on their role, simplifying access control management

○ *Role-Based Groups*

■ Grouping users based on their job functions

■ Assigning permissions to groups rather than individual users

■ Facilitates access control based on job roles, improving security and manageability

■ *Power Users*

● A user group with permissions between regular users and administrators

● Can perform certain administrative tasks like adding printers or changing the system time

● Illustrates the concept of assigning permissions based on job functions

- **Encryption**
  - ○ *Data Encryption*
    - ■ A fundamental method for securing data

- Encoding information and allowing access only with the correct security key

- *Unencrypted Data (Cleartext/Plaintext)*

  - Easily accessible and viewable format

  - Stored, transmitted, and processed in an unprotected format

- *Encrypted Data (Ciphertext)*

  - Scrambled up and unreadable without the proper decryption key

- Benefits of Encryption

  - Mitigates risks associated with access control failures

  - Even if access controls are bypassed, encrypted data remains unreadable

- *Data State*

  - Location of data within a processing system

  - <u>Data can exist in only one of three states</u>

    - *Data at Rest*

      - Data stored on memory, hard drives, or storage devices

      - Vulnerable without encryption

      - Types of encryption to support the confidentiality

        - Full disk encryption

        - Folder encryption

        - File encryption

        - Database encryption

- *Data in Transit/Motion*
    - Data moving between systems or within a system
    - Examples of encryption usage
        - TLS/SSL for web server communication
        - IPsec for VPN connections
        - WPA2 with AES for wireless connections
- *Data in Use/Processing*
    - Data being read into memory or processed by the CPU
    - Active data held in RAM, CPU caches, or registers
    - Involves encryption and integrity checks to protect data during processing
- <u>Data Moves constantly between these different states continually</u>
- <u>Data security must address protection during each state transition</u>

- **Internet Protocol Security (IPSec)**
    - *Internet Protocol Security (IPsec)*
        - A secure network protocol suite that provides authentication and encryption of data packets to create a secure encrypted communication path between two computers over an internet protocol network
        - Widely used for VPNs (virtual private networks)

- Functions
  - Confidentiality
    - Achieved through data encryption
  - Integrity
    - Ensured by hashing data before transmission and verifying upon receipt
  - Authentication
    - Each party verifies their identity
  - Anti-replay
    - Prevents duplicate packet transmission and attacks involving captured and resent packets
- Five Main Steps
  - Key Exchange Request
    - Initiates the VPN connection
  - IKE Phase 1
    - Authenticates parties and establishes a secure channel for negotiation
    - Utilizes Diffie-Hellman key exchange to create a shared secret key for establishing secure tunnels
    - Modes
      - Main Mode

- ■ Conducts three two-way exchanges between the peers, from the initiator to the receiver
  - 1 – Agree on algorithms and hashes
  - 2 – Use Diffie-Hellman key exchange to generate shared secret key
  - 3 – Verify identities
- ○ Aggressive Mode
  - ■ Fewer exchanges for faster initial connection
  - ■ Less secure
- ■ IKE Phase 2
  - Negotiates security association parameters and establishes the secure tunnel
  - Quick Mode
    - Only occurs after IKE already established the secure tunnel in Phase 1
- ■ Data Transfer
  - Allows data transfer over the secure tunnel using negotiated parameters
- ■ IPSec Tunnel Termination
  - Occurs when security associations are terminated through mutual agreement or due to timeout

- ○ *Diffie-Hellman Key Exchange*

    - ■ Allows two systems that do not know each other to be able to exchange keys and trust each other

- ○ Data Transfer Modes

    - ■ <u>Transport Mode</u>

        - Uses original IP header

        - <u>Suitable for client-to-site VPNs</u>

    - ■ <u>Tunneling Mode</u>

        - Encapsulates the entire packet

        - <u>Suitable for site-to-site VPNs</u>

- ○ Security Protocols

    - ■ *Authentication Header (AH)*

        - Provides data integrity and origin authentication, but not confidentiality

    - ■ *Encapsulating Security Payload (ESP)*

        - Provides authentication, integrity, replay protection, and confidentiality of the data

- ○ Client-to-Site VPNs

    - ■ Typically use transport mode with AH for integrity and ESP for encryption of data

○ Site-to-Site VPNs

■ Typically use tunneling mode with both AH and ESP for integrity, encryption, and protection of entire packets

● **Public Key Infrastructure (PKI)**

○ *Public Key Infrastructure (PKI)*

■ A system of hardware, software, policies, procedures, and people that is based on asymmetric encryption

■ Used for secure data transfer, authentication, and encrypted communications over networks

■ Creates a secure connection from end to end

■ Asymmetric Encryption

● Uses public and private keys for encryption and decryption

● Public key is used to encrypt data, private key is used to decrypt data

● Ensures confidentiality and authenticity of data

● Process

○ 1 – Browser requests server's public key from Certificate Authority

○ 2 – Browser encrypts shared secret key with server's public key

- ○ 3 – Encrypted key is sent to server, which decrypts it with its private key
- ○ 4 – AES is used to create a secure tunnel for data transfer
- Benefits
  - ○ Ensures confidentiality of data
  - ○ Provides authentication of servers
  - ○ Facilitates secure communication over networks
- ○ Relation to Public Key Cryptography
  - ■ _Public Key Cryptography_
    - <u>Encryption and decryption process that is just one small part of the overall PKI</u>
  - ■ PKI uses public key cryptography for its functions
  - ■ <u>PKI encompasses the entire system of managing digital keys and certificates</u>
- ○ Components of PKI
  - ■ _Certificate Authority (CA)_
    - A trusted third party that issues digital certificates and maintains trust between CAs worldwide
  - ■ _Key Escrow_
    - Secure storage of cryptographic keys, allowing retrieval in cases of key loss or legal investigations

- Challenges

  - ○ Security concerns with key escrow

  - ○ Need for strong regulations and security measures to protect keys

- ○ Conclusion

  - ■ PKI is crucial for secure communication and data exchange on the internet

  - ■ Understanding PKI components and processes is essential for network security

- **Digital Certificates**

  - ○ *Digital Certificate*

    - ■ A digitally signed electronic document that binds a public key with a user's identity

    - ■ Used for users, servers, workstations, or devices

  - ○ *X.509 Protocol*

    - ■ Standard for digital certificates within PKI

      - ● Contains owner/user information and certificate authority details

  - ○ *Wildcard Certificate*

    - ■ Allows multiple subdomains to use the same public key certificate

    - ■ Useful for managing subdomains off a main web domain

- ■ Certificate Revocation
    - ● If a server using a wildcard certificate is compromised, the certificate needs to be revoked, affecting all subdomain servers
- ■ Reissuing Process
    - ● Reissuing a new certificate is quick
    - ● Having one wildcard certificate allows quick reissuance and deployment to all servers
- ■ Multiple Domains
    - ● <u>For organizations with multiple websites on different domains, using a wildcard certificate isn't suitable</u>
- ■ *Subject Alternate Name (SAN) Field*
    - ● Certificate that specifies what additional domains and IP addresses will be supported
    - ● Used to cover multiple domains with one certificate
    - ● Modify the SAN field in the digital certificate
- ■ Wildcard vs. SAN Field
    - ● <u>Use a SAN field for different domains</u>
    - ● <u>Use a wildcard certificate for subdomains of the same domain</u>
- ○ Single-Sided and Dual-Sided Certificates
    - ■ *Single-Sided Certificate*
        - ● Authenticates only the server to the user
        - ● Requires no certificate from the user

- *Dual-Sided Certificate*
  - Requires both server and user to validate each other using certificates
  - Offers higher security but requiring more processing power
- *Self-Signed Certificate*
  - Signed by the entity it certifies
  - Lacks external verification and trust
  - Suitable for closed or non-production systems
- *Third-Party Certificate*
  - Issued by a trusted certificate authority (CA), embedded in major web browsers and operating systems
  - Offers a higher level of trust and security
- *Root of Trust*
  - Validates certificates in a chain from a trusted root certificate authority, ensuring trustworthiness
- *Certificate Authority (CA)*
  - Issues digital certificates
    - Contains CA details, serial number, issue/expiry dates, and version
- *Registration Authority (RA)*
  - Processes certificate requests from users
  - Forwards requests to the CA for digital certificate creation

- ○ *Certificate Signing Request (CSR)*

  - ■ Contains entity details and public key

  - ■ A vital component in the process of obtaining a digital certificate from a CA

- ○ *Certificate Revocation List (CRL)*

  - ■ Maintained by CAs, lists revoked digital certificates to prevent their use

- ○ *Key Escrow Agents*

  - ■ Securely hold copies of user's private keys in case of key loss

- ○ *Key Recovery Agents*

  - ■ Specialized software to restore lost or corrupted keys

- ○ Trust and Security

  - ■ Central to digital certificates, compromised root certificate authorities can lead to certificate revocation and reissuance

- ● **Understanding Digital Certificates: Demonstration**

- ● **Key Management**

  - ○ *Key Management*

    - ■ Involves generating, exchanging, storing, and using encryption keys securely

  - ○ Importance of Strong Keys

    - ■ A strong key is essential for encryption

- Weak passwords can compromise the confidentiality of files even with strong encryption algorithms
- ○ Secure Key Exchange
  - Asymmetric methods are often used to encrypt symmetric keys for secure transmission
    - Diffie Hellman algorithm is an example used in VPN, SSL, TLS connections, etc
- ○ Secure Storage
  - Keys must be securely stored when not in use, similar to passwords
  - Leaving keys vulnerable can lead to unauthorized decryption of files
- ○ Regular Key Rotation
  - Keys should be changed periodically to enhance security
  - Regular rotation resets the clock on potential attacks, increasing confidentiality

Network Segmentation

Objectives:

- 1.2 - Compare and contrast networking appliances, applications, and functions
- 1.8 - Summarize evolving use cases for modern network environments
- 3.5 - Compare and contrast network access and management methods
- 4.1 - Explain the importance of basic network security concepts
- 4.3 - Given a scenario, apply network security features, defense techniques, and solutions

- **Firewalls**
  - *Firewall*
    - Common network security device that acts as a barrier to networks
    - Uses a set of rules to define permitted or denied traffic
    - Types
      - Software/Hardware Based
      - Virtual/Physical devices
      - Host/Network Based
    - Functions
      - Performs Network Address Translation (NAT) or Port Address Translation (PAT)
      - Can use one public IP and many private IPs

- ○ Types of Firewalls
  - ■ *Packet Filtering Firewall*
    - ● Permits or denies traffic based on packet headers
    - ● Uses Access Control Lists (ACLs) for decision-making
    - ● Limited by rules and may not enable two-way communication effectively
  - ■ *Stateful Firewall*
    - ● Inspects traffic as part of a session
    - ● Allows incoming traffic that corresponds to outgoing requests
    - ● Can be exploited in phishing attacks due to session-based nature
      - ○ <u>Combine Packet Filtering and Stateful Firewalls for good security</u>
        - ■ Modern firewalls often support both packet filtering and stateful capabilities
  - ■ *Next-Generation Firewall (NGFW)*
    - ● Conducts deep packet inspection (DPI) for detailed traffic analysis
    - ● Operates at layers 5, 6, and 7 of the OSI model
    - ● Can be specific to web servers (web application firewall) or for entire networks
- ○ *Access Control Lists (ACLs)*
  - ■ Sets of rules assigned to routers or firewalls

- - ■ Permit or deny traffic based on IP/MAC address or port depending on device
      - Switch – MAC address
      - Router – IP address
      - Firewall – IP address or port
    - ■ Criteria
      - Source/destination IP
      - Source/destination port
      - Source/destination MAC
  - Exam Tip
    - ■ Study how to read ACLs
  - *Unified Threat Management (UTM) System*
    - ■ Combines firewall, router, intrusion detection/prevention, malware solutions, and other security devices
    - ■ Generally considered a border device with next-generation firewall capabilities
    - ■ Available as physical, virtual, or cloud solutions

- **Access Control List (ACL)**
  - *Access Control Lists (ACLs)*
    - ■ A list of permissions associated with a given system or network resource
    - ■ Can be applied to routers, layer three switches, or firewalls

- ■ Contain rules that are applied based on IP addresses, ports, or applications
- ■ Processed from top to bottom
  - ● Specific rules should be at the top
  - ● Generic rules should be at the bottom
- ○ Blocking Strategies
  - ■ Block incoming requests from internal or private loopback addresses, multicast IP ranges, and experimental ranges
  - ■ Block incoming requests from protocols that should only be used locally (e.g., ICMP, DHCP, OSPF, SMB)
  - ■ Configure IPv6 to block all traffic or allow only authorized hosts and ports
- ○ *Explicit Allow*
  - ■ Specified in ACLs using "permit" statements
  - ■ Each "permit" statement explicitly allows a specific type of traffic from a specific source to a specific destination
- ○ *Explicit Deny*
  - ■ Statement used to block specific types of traffic
  - ■ Created by changing the "permit" keyword to "deny" in an ACL rule
- ○ *Implicit Deny*
  - ■ Statement that is automatically applied at the end of an ACL if no explicit deny statements are present
  - ■ Blocks all traffic that is not explicitly permitted by "permit" statements

- ○ Impact on Security

    - ■ Explicit allow statements ensure that only specified traffic is allowed, increasing security by minimizing unintended access

    - ■ Explicit deny statements allow for precise control over which traffic is blocked

    - ■ Implicit deny provides a default block for all traffic not explicitly permitted, adding an extra layer of security

- ○ *Role-Based Access Control*

    - ■ Defines privileges and responsibilities of administrative users

    - ■ Users are grouped based on roles or job functions

    - ■ Permissions are assigned based on roles (e.g., configuring firewalls, adding/removing users)

- ○ Exam Tips:

    - ■ CompTIA exams are device-agnostic

        - ● Do not focus on specific brands or models of devices

    - ■ Focus on understanding the concepts and principles behind firewall configurations, rather than memorizing specific device configurations

    - ■ Practice reading and interpreting firewall configurations from different vendors to prepare for the exam's broad scope

    - ■ Understand the difference between explicit allow, explicit deny, and implicit deny, as they are fundamental concepts in ACL configuration and network security

- **Segmentation Zones**
    - Segmentation Zones
        - *Trusted Zone*
            - Local Area Network (LAN), also known as the Inside Zone
            - Represents the corporate intranet
        - *Untrusted Zone*
            - Includes the internet and other external networks
            - Traffic from the internet to the trusted zone is typically blocked, except for responses to specific requests from the inside
        - *Screened Subnet*
            - A semi-trusted zone between the trusted and untrusted zones
            - Contains devices like web servers and email servers
            - Has restricted access from the untrusted zone and is not fully trusted by the internal network
            - Screened Subnet to Trusted Zone
                - Traffic from internal to the screened subnet is allowed, but traffic is restricted
                - Return traffic from screened subnet devices is allowed
            - Screened Subnet to Untrusted Zone
                - Screened subnet devices can access the internet freely
                - Certain inbound ports need to be open for services like email and web hosting

- Provides a choke point for network security measures, enhancing protection for hosted servers
    - Firewalls
    - Intrusion detection systems (IDS)
    - Intrusion prevention systems (IPS)
    - Unified threat management (UTM) systems
- Functionality
- Allows hosted servers like email and web servers to be accessible from both internal and external networks
- Without the screened subnet, servers hosted inside the network would be inaccessible or less useful to external users

- **Jumpbox**
    - *Internet Facing Hosts*
        - Hosts or servers that accept inbound connections from the internet
        - Example
            - Web server on a screen subnet
    - *Screen Subnet*
        - A segment isolated from the private network by firewalls
        - Set up to accept connections from the internet over designated ports
        - Purpose
            - Keeps forward-facing servers out of the internal network

- Security
  - Semi-trusted zone
    - Invisible to the outside network except for forward-facing servers
- Content of Screen Subnet
  - Internet facing servers like email, web servers
  - Communication servers, proxy servers, and remote access servers
  - Public services or extranet capabilities
  - Security Measures
    - Harden devices in the screen subnet
    - Use intrusion detection systems
    - Consider all devices in the screen subnet as untrusted
    - Protect against pivoting attacks from the screen subnet to the internal network
  - *Bastion Host*
    - A host or server in the screen subnet that is not configured with services that run on the local network
    - Example
      - Email server
      - Web server
      - Remote access server

- - *Jumpbox*
    - A hardened server that provides access to other hosts within the screen subnet
    - Purpose
      - Control access to the screen subnet from the internal network
    - Security
      - Should be heavily hardened and protected
    - Management of Jumpbox
      - Can be a physical PC or a virtual machine
      - Should have only the minimum required software
      - Fully hardened and secured to protect against unauthorized access

- **Understanding Firewalls: Demonstration**

- **Content Filtering**
  - *Content Filtering*
    - A network management practice that involves restricting access to certain content, websites, or applications based on specific criteria to conserve network bandwidth, comply with legal or organizational policies, or prevent exposure to inappropriate or harmful content

- ○ Techniques
  - ■ *URL Filtering*
    - ● Blocks access to specific websites based on their URL
    - ● Common in organizational settings to prevent access to non-work-related or inappropriate sites
  - ■ *Keyword Filtering*
    - ● Scans webpages for specific keywords or phrases and blocks them
    - ● Useful for blocking specific content without blocking entire websites
    - ● Can lead to over-blocking if not configured carefully
  - ■ *Protocol or Port Filtering*
    - ● Blocks certain types of network traffic based on the protocol or port they use
    - ● Example
      - ○ Blocking specific ports can prevent the use of certain file sharing applications or services
- ○ *Proxy Servers*
  - ■ Act as intermediaries between a user's device and the internet
  - ■ Manage internet traffic and can be used for various purposes, including content filtering

- ■ Types
  - ● *Web Proxy*
    - ○ Retrieves web pages from the internet and can be used to bypass content filters
  - ● *Reverse Proxy*
    - ○ Manages incoming internet traffic to an organization, load balancing, improving security, and performance
  - ● *Transparent Proxy*
    - ○ Monitors and filters internet traffic, blocking access to specific websites or content types, and enforcing company policies
- ■ Benefits
  - ● Filter out malicious traffic and prevent unauthorized access, improving cybersecurity
  - ● Hide user's IP address, preserving anonymity and privacy
  - ● Block access to specific websites or content types, enforcing company policies
  - ● Cache frequently accessed resources, improving performance

- **Internet of Things (IoT)**
  - *Internet of Things (IoT)*
    - refers to a global network of appliances and personal devices equipped with sensors, software, and network connectivity to report state and configuration data
  - Types of IoT Devices
    - *Building and Home Automation Systems*
      - Manage lighting, HVAC, water, and security systems
    - *IP Video Systems*
      - Provide remote collaboration using video teleconference suites
    - *Audio Visual Systems*
      - Stream live video productions and control multiple displays
    - *Physical Access Control Systems*
      - Determine access into secure areas
        - Proximity readers
        - Access control systems
        - Biometric readers
    - *Scientific and Industrial Equipment*
      - Found in hospitals, factories, and laboratories
      - Allows centralized monitoring and management

- ○ <u>Best Practices</u>
  - ■ Segregation
    - ● Place IoT devices on their own network, physically or logically separated from the business network
  - ■ Security
    - ● Ensure devices are properly security enabled and receive security patches
  - ■ Power
    - ● Provide power using Power over Ethernet (PoE) or battery power supply
- ○ Categories of IoT Components
  - ■ *Hub and Control System*
    - ● Central point of communication for automation and control.
  - ■ *Smart Devices*
    - ● Endpoints that connect to the hub for automation
  - ■ *Wearables*
    - ● IoT devices that are designed as accessories that can be worn, such as smart watches and fitness trackers
  - ■ *Sensors*
    - ● Measure various parameters like temperature, sound, motion, etc.

- ○ Security Considerations

    - ■ Understand endpoints

        - ● Each new device brings new vulnerabilities, so understand and secure them

    - ■ Track and manage devices

        - ● Carefully manage device connections and configurations

    - ■ Patch vulnerabilities

        - ● Apply patches when available, and manage residual risks

    - ■ Conduct tests and evaluations

        - ● Evaluate devices using penetration testing techniques

    - ■ Change default credentials

        - ● Change default usernames and passwords before deployment

    - ■ Use encryption

        - ● Encrypt data sent and received by IoT devices

    - ■ Segment IoT devices

        - ● Place IoT devices in their own VLAN and subnet to prevent interference

- ● **SCADA and ICS**

    - ○ *Information Technology (IT)*

        - ■ Focuses on standard computers, servers, networks, and cloud platforms

- ○ *Operational Technology (OT)*
  - ■ A communications network that is designed to implement an industrial control system, rather than traditional business and data networking systems
  - ■ <u>Deals with controlling machinery and processes in the physical world</u>
- ○ *Industrial Control System (ICS)*
  - ■ Provides workflow and process automation by controlling machinery using embedded devices
  - ■ Heavily used to control real world devices
  - ■ Interconnected ICSs can form a Distributed Control System (DCS)
  - ■ <u>Prioritizes availability and integrity over confidentiality</u> (CIA triad in OT)
    - ● Unlike the CIA triad in IT where confidentiality is often more emphasized
  - ■ *Fieldbus*
    - ● A communication technology used in OT to link Programmable Logic Controllers (PLCs) together
  - ■ *Programmable Logic Controllers (PLCs)*
    - ● Digital computers used in industrial settings for automation and are programmed using Human Machine Interfaces (HMIs)

■ *Human Machine Interfaces (HMIs)*

- A local control panel or a piece of software running on a regular computer that will act as the input to the PLCs and the output for the entire system

○ *Supervisory Control and Data Acquisition(SCADA)*

■ A type of ICS used to manage large-scale, multi-site devices and equipment spread over a geographic region

■ Network made up of interconnected ICS/DCS plants using wide area network (WAN) connections, such as cellular, microwave, satellite, fiber, or VPN based WAN

■ Often operated with software running on ordinary systems like Windows or Linux

- **Bring Your Own Device (BYOD)**
  - ○ *Bring Your Own Device (BYOD) Policy*
    - ■ Policy allowing employees to use their personal devices (laptops, tablets, phones) for work purposes
    - ■ Security Issues
      - Introducing vulnerabilities from personal devices, potential for malware transfer to work network

- Data Ownership
  - Concerns about who owns the data on personal devices, distinguishing between personal and business data
- *Storage Segmentation*
  - Separating personal and company data on the same device
  - Can be achieved technologically or procedurally
- *Mobile Device Management (MDM)*
  - Centralized software for remote administration and configuration, updating devices, enforcing policies
- *Choose Your Own Device (CYOD)*
  - Employees choose from a selection of supported devices, organization provides and manages the device
  - Benefits of CYOD
    - Allows for installation of MDM, enforcing technical policies, preventing data loss, and controlling device features
- Considerations for Organizations
  - Security Policy
    - Organizations must decide on a mobile device security policy that suits their needs
  - Choose between BYOD and CYOD based on security, cost, and control considerations

- **Zero-trust and Architecture**
    - Concept of Zero Trust
        - Modern approach to cybersecurity due to sophisticated threats
        - Traditional strategies focused on strong perimeter defense like castle walls
            - Ineffective against modern threats due to de-perimeterization
            - *De-perimeterization*
                - Protect systems and data using encryption, secure protocols, and host-based protection
                - Allows cost reduction, global business transactions, and increased agility
                - Resulted from cloud migration, remote work, mobile tech, wireless networks, outsourcing
    - Zero Trust Principles
        - Trust nothing, verify everything
        - Verify every device, user, and transaction regardless of origin
        - Addresses threats from inside and outside networks
    - Zero Trust Architecture
        - *Control Plane*
            - Defines, manages, and enforces access policies

- Elements
    - *Adaptive Identity*
        - Real-time validation based on behavior, device, and location
    - *Threat Scope Reduction*
        - Limiting user access to minimize attack surface
    - *Policy-driven Access Control*
        - Enforcing access based on roles and responsibilities
    - *Secured Zones*
        - Isolated environments for sensitive data access
- *Data Plane*
    - Ensures execution of policies
    - Components
        - *Subject System*
            - Individual or entity seeking access
        - *Policy Engine*
            - Cross-references access requests with predefined policies
        - *Policy Administrator*
            - Establishes and manages access policies
        - *Policy Enforcement Point*
            - Executes access decisions

- ○ <u>Key Takeaways</u>

  - ■ Zero Trust assumes no user or system is trusted by default

  - ■ Requires continuous verification for access regardless of location or origin

  - ■ Complements traditional perimeter-based defenses

  - ■ Offers a roadmap for robust security in remote work, cloud computing, and diverse device environments

- **Virtual Private Network (VPN)**

  - ○ *Virtual Private Network (VPN)*

    - ■ Extends a private network across a public network, allowing users to send and receive data securely as if their devices were directly connected to the private network

    - ■ Uses tunneling protocols to establish a secure connection over the public internet

  - ○ Types of VPNs

    - ■ *Site-to-Site VPN*

      - ● Connects two offices or sites

      - ● Provides a cost-effective alternative to dedicated lease lines

    - ■ *Client-to-Site VPN*

      - ● Connects a single remote user to a corporate network, enabling remote work or telecommuting

- *Clientless VPN*
  - Creates a secure remote access VPN tunnel using a web browser, without requiring software or hardware clients
  - Tunneling protocols (HTTPS Connection)
    - *Secure Socket Layer (SSL)*
      - Provides cryptography and reliability using the upper layers of the OSI model (Layers 5, 6, and 7)
      - Outdated and less secure
    - *Transport Layer Security(TLS)*
      - Provides secure web browsing over HTTPS
      - More updated than SSL
    - Both SSL and TLS use TCP
      - Can slow down connection due to more overhead
      - *Datagram Transport Layer Security (DTLS)*
        - UDP version of TLS
        - Provides same level of security as TLS
        - Operates faster due to less overhead inside UDP protocol
        - An excellent choice for video streaming and voiceover IP over secure and encrypted tunnels

- ○ VPN Configuration for Site-to-Site and Client-to-Site
    - ■ *Full Tunnel*
        - ● Routes and encrypts all traffic through the VPN connection, making the remote user part of the headquarters network
    - ■ *Split Tunnel*
        - ● Divides traffic, routing and encrypting traffic bound for headquarters over the VPN while sending other traffic directly to the internet
        - ● Offers better performance but may be less secure
    - ■ Use full tunnel when connecting VPN over an untrusted network like wifi at a hotel or a coffee shop
- ○ Older VPN Protocols
    - ■ Layer 2 Tunneling Protocol (L2TP)
        - ● A very early VPN invented in the 80s and 90s
        - ● Lacks security features like encryption by default
        - ● Needs to be combined with an extra encryption layer for protection
    - ■ *Layer 2 Forwarding (L2F)*
        - ● Originally developed by Cisco
        - ● Provides a tunneling protocol fir the P2P protocol (PPP)
        - ● Lacks native security and encryption features

- - - *Point-to-Point Tunneling Protocol (PPTP)*
      - Supports dial-up networks
      - Lacks native security features except when used with Microsoft Windows
  - ○ Modern VPNs
    - *IP Security (IPsec)*
      - Provides authentication and encryption of packets to create a secure communication path between two computers
  - ○ <u>Tunneling protocols like SSL/TLS, L2TP, L2F, PPTP, and IPsec can be used to establish VPN connections</u>

- **Using VPN Connections: Demonstration**

- **Remote Access Management**
  - ○ *Telnet*
    - Operates on port 23
    - Sends text-based commands to remote devices
    - Sends data in plain text, so it is not secure for sensitive information
    - <u>Should never be used for secure devices like routers, switches, or firewalls</u>
  - ○ *Secure Shell (SSH)*
    - Operates on port 22
    - Encrypts data sent between client and server

- Provides better security compared to Telnet

- <u>Always use SSH for configuring networking devices</u>

○ *Remote Desktop Protocol (RDP)*

- Operates on port 3389

- Developed by Microsoft for graphical interface remote connections

- Useful for remotely accessing Windows servers or client machines

- Provides a Graphical User Interface (GUI) for remote control

- Uses tunneling to secure connections

○ *Remote Desktop Gateway (RDG)*

- A Windows server that creates secure connections to servers via RDP

- Uses SSL or TLS protocols to encrypt data

- Security features

  ● Creating encrypted tunnels like a VPN

  ● Controlling access to network resources based on permissions and group roles

  ● Maintaining and enforcing authorization policies

  ● Monitoring the status of the gateway and any RDP connections passing through that gateway

- Recommended for Windows 2008 or newer to protect RDP connections

○ *Virtual Network Computing (VNC)*

- Operates on port 5900

- ■ Designed for thin client architectures and Virtual Desktop Infrastructure (VDI)
- ■ Cross-platformed
  - ● Linux
  - ● OS X
  - ● Windows
- ■ Allows remote access with a graphical interface
- ○ *Virtual Desktop Infrastructure (VDI)*
  - ■ Hosts a desktop environment on a centralized server
  - ■ Runs a desktop image within a virtual machine for end-user access
  - ■ Also known as Desktop as a Service (DAS) in cloud computing
- ○ In-Band vs. Out-of-Band Management
  - ■ *In-Band Management*
    - ● Uses Telnet or SSH over the network
  - ■ *Out-of-band Management*
    - ● Uses a separate network for device configuration
    - ● Provides additional security by separating data networks from management networks
- ○ *Application Programming Interface (API)*
  - ■ Set of protocols and routines for building and interacting with software applications
  - ■ Acts as an intermediary between different systems for communication

- ■ Allows for automated administration, management, and monitoring of applications and services
- ■ Typically built using either Representational State Transfer (REST), or Simple Object Access Protocol (SOAP)
- ■ Allows for direct integration of different third-party applications

Networking Monitoring

Objectives:

- 1.2 - Compare and contrast networking appliances, applications, and functions
- 3.2 - Given a scenario, use network monitoring technologies

- **Intrusion Detection and Protection Systems (IDS/IPS)**
    - *Intrusion Detection System (IDS)*
        - Detects network threats
        - Passive device
        - Monitors network traffic, logs, and alerts
    - *Intrusion Prevention System (IPS)*
        - Detects network threats and responds to them
        - Active device
        - Operates in line, blocking offending traffic
    - *Snort*
        - Software-based IDS/IPS
        - Open-source and widely used
    - Challenges with IPS
        - False positives can lead to blocking legitimate traffic

- ○ Detection Methods

  - ■ *Signature-based*

    - ● Matches unique byte strings or patterns

  - ■ *Policy-based*

    - ● Relies on specific security policies

  - ■ Anomaly-based

    - ● *Statistical*

      - ○ Watches traffic patterns to build baseline

    - ● *Non-statistical*

      - ○ Administrator defines the baseline

- ○ Network-based vs. Host-based IDS/IPS

  - ■ Network-based – protects entire network

  - ■ Host-based – installed on individual hosts

  - ■ Combination of two can provide more protection to the network

- **Simple Network Management Protocol (SNMP)**

  - ○ *Simple Network Management Protocol (SNMP)*

    - ■ Internet protocol for collecting, organizing, and modifying information about managed devices on IP networks

    - ■ Can be used to change device behavior

  - ○ *Managed Devices*

    - ■ Devices communicating with an SNMP manager (MIB)

- ○ SNMP Architecture
    - ■ *SNMP Manager*
        - ● Any machine on the network that is running the SNMP protocol to collect and process information from the devices
    - ■ *SNMP Agents*
        - ● Network devices sending information to the manager
- ○ Message Types
    - ■ *Set*
        - ● Manager request to change variable values
    - ■ *Get*
        - ● Manager request to retrieve variable values
    - ■ *Trap*
        - ● Asynchronous notifications sent from agent to manager
        - ● Used for event/alarm notifications
        - ● Encoding methods:
            - ○ *Granular Trap*
                - ■ Each SNMP trap message is sent with a unique Object Identifier (OID)
            - ■ *Object Identifier (OID)*
                - ● Identifies a variable that can be read or set via SNMP

- Consolidated and stored in Management Information Base (MIB)
        - *Management Information Base (MIB)*
            - Describes the structure of the management data of a device subsystem using a hierarchical namespace
    - ○ *Verbose Trap*
        - SNMP traps may be configured to contain all the information about a given alert or event as a payload
- ○ SNMP Versions
    - SNMPv1
    - SNMPv2
        - Both v1 and v2 use community strings sent and stored in plain text, making them insecure
    - SNMPv3 – most secure
        - Integrity – hashing messages to prevent alteration
        - Authentication – validating message sources
        - Confidentiality – encryption using DES (Data Encryption Standard) or newer standards like 3DES and AES (Advanced Encryption Standard)
        - Groups SNMP components for increased security

- Allows different access privileges (read, write) for different group

- Enhances network protection and management

- **Network Sensors**
  - *Network Sensors*
    - Monitor device performance (e.g., routers, switches, firewalls)
  - *Temperature Sensor*
    - Reports device chassis temperature
    - Minor Threshold –indicates rising temperature
    - Major Threshold – signals dangerous conditions
    - Actions:
      - System messages
      - SNMP notification
      - *Load Shedding*
        - A device can turn off different functions to reduce temperature
    - Excessive heat reduces performance, lifespan, may cause failure
  - CPU Usage/Utilization
    - Normal range – 5% to 40%
    - High utilization
      - Possible causes:
        - Misconfiguration

- - - ○ Network attacks
  - ● Consequences:
    - ○ Packet drops
    - ○ Connection failure
- ○ Memory Utilization
  - ■ Thresholds:
    - ● Minor
    - ● Severe
    - ● Critical
  - ■ Normal operation – around 40%
  - ■ Busier times – 60% to 70%
  - ■ Peak times – Up to 80%
  - ■ Above 80%
    - ● Device capacity may have to be adjusted
    - ● Could indicate network attack
    - ● Implications:
      - ○ System hangs
      - ○ Crashes
- ○ Real-world Operation
  - ■ Monitoring deviations from baseline
  - ■ Alarms for abnormal metrics
  - ■ Investigation and resolution of issues

- **Packet Captures**
  - *Packet Capture*
    - Used to capture all data going to or from a network device
    - Packet Capture Columns
      - Number
        - Packet number in the capture sequence
      - Time
        - Elapsed time since starting the capture
      - IP Addresses
        - Source IP
        - Destination IP
      - Protocol
        - TCP, UDP, or other Layer 3 or 4 protocols
      - Length
        - Size of the packet
      - Info
        - Header information
  - Example Attacks
    - Packet Capture 1
      - Port Scan
        - SYN packets are sent to various ports to detect open ports

- Packet Capture 2
    - SYN Flood
        - Flood of SYN packets, without completing the three-way handshake, to overwhelm a server
- Packet Capture 3
    - Distributed Denial of Service (DDoS)
        - Multiple systems attacking the same server, shown by SYN flood attempts from different source IP addresses
- *Exam Focus*
    - Exam packet captures may contain 5, 10, 15, or 20 lines (snippets), highlighting specific attack types
    - Understanding attack types based on limited information is crucial (e.g., identifying a DDoS attack from multiple sources targeting the same server)
    - Remember to focus on the key elements of a packet capture and how they relate to different attack types, especially when information is limited

- **Network Flow Data**
    - *Flow Analysis*
        - Recording of metadata and statistics about network traffic using flow collector tools

- - - Do not capture the content of the network traffic like full packet capture but provide valuable metadata for monitoring
  - Benefits of Flow Analysis
    - Allows capturing traffic flow information instead of the content, saving storage space
    - Helps in identifying trends, patterns, and anomalies in network traffic for performance monitoring and security
  - Tools for Traffic Flow Analysis
    - *NetFlow*
      - Cisco-developed means of reporting network flow information to a structured database
      - Defines traffic flow based on packets that share the same characteristics
    - *Zeek*
      - A hybrid tool that passively monitors the network
      - Logs full packet captures when something of interest is detected based on configured parameters and rules
      - Normalizes data and stores them in tab-delimited or JSON formats
        - Allows compatibility with various cybersecurity and network monitoring tools for analysis

- ■ *Multi Router Traffic Grapher (MRTG)*
    - ● Creates graphs to show network traffic flows through network interfaces, aiding in visualizing traffic patterns
    - ● Can reveal abnormal traffic patterns that require further investigation
    - ● Incident Response
        - ○ Network sniffers can be deployed to investigate potential malicious activities, such as data exfiltration, based on abnormal traffic patterns
        - ○ Instant response and cleanup actions can be taken upon identifying suspicious activities to maintain network health and security

- **Log Aggregation with Syslog**
    - ○ Network Logging Overview
        - ■ Network devices generate logs containing information, events, warnings, alerts, and critical data
        - ■ For large networks, manual log review is impractical
    - ○ *System Logging Protocol (Syslog)*
        - ■ A protocol that is utilized to transmit logs to a central server, simplifying the process of collecting logs from all routers and switches
        - ■ Allows easier analysis and review from a single location

- ○ *Syslog Server*
  - ■ Centralized servers where logs from routers, switches, servers, and other devices are sent
  - ■ Can be standalone syslog servers or integrated
    - ● Security Information Management (SIM)
    - ● Security Event Management (SEM)
    - ● Security Information and Event Management (SIEM)
      - ○ Combines logging and analysis functionalities into one system
  - ■ A big collection of all the different logs from all the different servers and clients and network devices
- ○ Syslog Components
  - ■ Client
    - ● Sends log information to the syslog server
  - ■ Server
    - ● Receives and stores logs from clients
  - ■ Logs are sent over UDP using port 514
- ○ <u>Syslog Severity Levels</u>
  - ■ Eight levels, each level indicates the severity of the log message
    - ● 0 – Emergency
      - ○ The system has become unstable
      - ○ Most severe

- 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
  - Least severe
- Log Management
  - Administrators determine which levels to log and how long to keep logs
  - Limiting logs to levels 0-5 is common to conserve disk space
- Exam tip
  - Study and understand the eight different severity levels of syslog

- ○ Network Device Logs
    - ■ *Traffic Logs*
        - ● Contain information about traffic flows within the network
        - ● Useful for identifying abnormal traffic patterns and troubleshooting network issues
    - ■ *Audit Logs (or Audit Trails)*
        - ● Record sequence of events and changes on network devices
        - ● Useful for tracking configuration changes and identifying unauthorized modifications
- ○ Log Analysis
    - ■ Analyzing logs can reveal trends and anomalies that may indicate security breaches or network issues
    - ■ <u>Understanding normal network behavior is key to identifying abnormal activity</u>
- ○ Windows Logs
    - ■ *Application Logs*
        - ● Information about software running on Windows machines
        - ● Severity Levels
            - ○ Informational
            - ○ Warning
            - ○ Error

■ *Security Logs*

● Information about security-related events, such as login attempts

■ *System Logs*

● Information about the operating system itself

● Severity Levels

○ Informational

○ Warning

○ Error

● **Security Information and Event Management (SIEM)**

○ *Security Information and Event Management (SIEM)*

■ A security solution that provides real-time or near real-time analysis of security alerts generated by network hardware and applications

■ Helps maintain a strong security posture by collecting and analyzing logs, informational alerts, and events from various devices on the network

○ SIEM Functions

■ Log Collection

● Gather event records from sources throughout the network, usually using syslog

● Provides important forensic tools

● Helps address compliance reporting requirements

- Normalization
  - Map log messages from different systems into a common data model for analysis
- Correlation
  - Link logs and events from different systems or applications into a single data feed
  - Detects threats more efficiently
- Aggregation
  - Reduce event data volume by consolidating duplicate events into single records
- Reporting
  - Present correlated and aggregated event data in real-time monitoring dashboards or long-term summaries
- ○ SIEM Implementation
  - Software on a server
  - Hardware appliance
  - Outsourced managed service
- ○ Considerations for Effective SIEM Deployment
  - Log all relevant events and filter out irrelevant data
  - Establish and document the scope of events
  - Develop use cases to define threats
  - Plan incident responses for different scenarios

- - Establish a ticketing process to track flagged events

    - Schedule regular threat hunting

    - Provide auditors and analysts with an evidence trail

  - SIEM systems use the syslog protocol to collect data from network and client devices

    - Ports

      - Port 514 – UDP

      - Port 1468 – TCP

  - Exam Tip

    - Understand the purpose of SIEM, its reliance on the syslog protocol, and its functions in collecting, normalizing, correlating, and aggregating logging data for analysis

- **Understanding SIEMs: Demonstration**

- **Network Performance Metrics**

  - *Network Performance Monitoring*

    - Focuses on end-to-end monitoring of user experience, unlike traditional monitoring which focuses on specific points.

  - Key Metrics

    - *Latency*

      - Time taken for data to reach its destination and return

- Measured in milliseconds
- High latency
    - Slows down network performance
    - Especially noticeable in real-time applications like video conferencing or gaming

■ *Bandwidth*
- Maximum rate of data transfer across a network
- Measured in bits per second
- *Throughput*
    - The actual data transfer rate achieved
    - Often lower than the theoretical bandwidth due to network conditions

■ *Jitter*
- Variation in packet delay
- Particularly impactful for real-time applications
- Causes disruptions like voice speeding up or video freezing during conferences
- Managing Jitter
    - Implement Quality of Service (QoS) to prioritize voice and video traffic
    - Ensure network connections and devices can handle the data volume without congestion

- ○ Monitoring Responsibility
    - ■ As a network administrator, it is important to continuously monitor these metrics to ensure optimal network performance

- **Interface Statistics**
    - ○ *Interface*
        - ■ A physical or logical switch port on a router, switch, or firewall
        - ■ In, enterprise-level devices, each interface can generate its own statistics and maintains its own status
    - ○ *Interface Statistics*
        - ■ Provide detailed information about the status and performance of network interfaces
        - ■ Helps troubleshoot network connectivity issues and optimize network performance
    - ○ Key Elements of Interface Statistics
        - ■ *Link State*
            - ● Indicates whether the interface has a cable connected and a valid protocol for communication
            - ● "FastEthernet 0/0 is up, line protocol is up"
                - ○ Indicates the interface is physically connected and operational

■ *Speed and Duplex Status*

- Specifies the interface's speed and duplex mode

- Optimal settings for fast Ethernet

    ○ 100BaseTX/FX

        ■ 100 Mbps bandwidth

        ■ Full duplex

        ■ Using either copper or fiber cabling

■ *Send and Receive Traffic Statistics*

- Tracks the number of packets and bytes sent and received by the interface

■ *Cyclic Redundancy Check (CRC) Statistics*

- Counts the number of packets that failed the CRC check

- High CRC errors may indicate issues with cabling or electromagnetic interference

■ *Protocol Packet and Byte Counts*

- Provides detailed counts of packets and bytes for different protocols

- *Input and Output Errors*

    ○ Counts errors in received and transmitted packets, indicating potential issues with the interface or network

- Additional Information Based from Cisco Router for an Interface (F0/0)

    - MAC Address and IP Address

        - IP and MAC addresses assigned to the interface

    - MTU Size

        - Maximum Transmission Unit size of the interface

        - 1500 bytes – default for Ethernet

    - *Bandwidth*

        - Speed of the interface

        - 100,000 Kbps (100 Mbps) – fast Ethernet

    - *Reliability*

        - Indicates the reliability of the connection

        - 255/255 – best

    - *TxLoad*

        - Indicates how busy the router is transmitting frames over the connection and

        - Example

            - 1/255 – not busy

    - *RxLoad*

        - Show how busy the router is in terms receiving frames.

    - ARP Type

        - Indicates the ARP protocol being used

        - ARPA – for Ethernet

- ■ *Keep Alive*
    - ● Specifies the interval at which the router sends keep alive packets to check if connected devices are still online
    - ● 10 seconds – default
- ■ *Input queue*
    - ● Shows the number of packets in the input queue and its maximum size
- ■ *Drops*
    - ● Count dropped packets
- ■ *Flushes*
    - ● Count Selective Packet Discards (SPD)
    - ● When the router or switch starts shedding some load and dropping packets selectively
    - ● Selective Packet Discards (SPD)
        - ○ Drops low priority packets when CPU is busy to prioritize higher priority packets
- ■ Queuing Strategy
    - ● Specifies the queuing strategy
        - ○ First in, first out (FIFO) – default for Ethernet
- ■ *Output queue size*
    - ● Shows the current and maximum size of the output queue

- *Input and Output Rates*
  - Display the average rates at which packets are being received and transmitted

- *Packet Input and Output*
  - Counts the number of packets received and transmitted, along with the corresponding byte counts

- *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 received

- *Throttle*
  - Occurs when the interface fails to buffer the incoming packets
  - High number indicates quality of service issues

- *Input errors*
  - Counts frames received with errors

- *Frame*
  - Counts packets with CRC errors and a non-integer number of octets

- *Overrun*
  - Counts times when the interface was unable to receive traffic due to insufficient hardware buffer

- *Ignored*
  - Counts packets ignored due to low internal buffers
  - Rises drastically when connection is experiencing noise or a broadcast storm
- *Watchdog counter*
  - Counts times the watchdog timer has expired
  - Happens whenever a packet over 2048 bytes is received
- *Input Packets with Dribble Condition*
  - Counts frames slightly longer than the default frame size (MTU size, 1500 bytes) but not yet a giant (1518 bytes)
- *Packet Output Counter*
  - Number of packets that have been sent and the size of those transmissions in bytes
- *Underrun*
  - Counts times when sender operated faster than router can handle
  - Causes buffers or dropped packets
- Output Errors
  - Counts collisions and interface resets
  - Collision
    - 0 – full duplex
    - not zero indicates something is wrong

- *Unknown Protocol Drops*
    - Counts packets dropped when the device couldn't determine the protocol
- *Babble*
    - Counts any frame that are transmitted and larger than 1518 bytes
- *Late Collision*
    - Counts the number of collisions that occur after the interface has started transmitting its frame
    - 0 – full duplex
    - not zero – half duplex
- *Deferred*
    - Counts the number of frames that were transmitted successfully after waiting
    - 0 – full duplex
    - not zero – half duplex
- *Lost Carrier and No Carrier*
    - Counts times the carrier signal was lost or not present during transmission
- *Output Buffer Failure*
    - Number of times a packet was not output from the output hold queue due to shortage of shared memory

- ■ *Output Buffer Swapped Out*
  - ● Number of packets stored in the main memory when the queue is full
  - ● High number indicates busy time in the network
- ○ <u>Exam Tips</u>
  - ■ Focus Areas
    - ● Link state, speed and duplex status, traffic statistics, CRC errors, and common error types (e.g., giants, runts)
  - ■ Scenario-Based Questions
    - ● Be prepared to analyze interface statistics to troubleshoot network issues
  - ■ Sample Troubleshooting Using Interface Statistics
    - ● Slow Network Performance
      - ○ Check duplex settings and for excessive collisions or errors
    - ● CRC Errors
      - ○ Inspect cabling and connectors for damage or interference
    - ● Collisions
      - ○ Investigate network segments with multiple devices or network congestion
    - ● Input and Output Errors
      - ○ Look for issues with the interface or network configuration

Orchestration and Automation

Objective 1.8: Summarize evolving use cases for modern network environments

- **Introduction**
  - Automation
    - Reduces the risk of human error, speeds up repetitive tasks, and frees up network administrators
  - *Orchestration*
    - Coordinates automated tasks across various interconnected systems
- **Infrastructure as Code (IaC)**
  - *Infrastructure as Code (IAC)*
    - Manage and provision infrastructure through code instead of manual processes
    - Refers to virtual machines, servers, clients, switches, routers, firewalls, and security appliances
  - *Scripted Automation and Orchestration*
    - Used in cloud computing for rapid deployment
    - DevSecOps (development, security, and operations) teams can deploy routers, switches, networks, servers, and security devices
    - Benefits of Scripted Automation
      - Less error-prone and faster deployment

- Reusable scripts ensure consistency and reduce mistakes
    - Key Areas of IAC Implementation
        - *Scripting*
            - Perform actions in a sequence with basic logic
        - *Security Templates*
            - Configuration files for network settings, access control, etc.
        - *Policies*
            - Define rules and permissions for deployments
    - *Orchestration*
        - Process of arranging or coordinating the installation and configuration of multiple systems
            - Machine learning and logic
        - Runs tasks on multiple servers/devices simultaneously, increasing efficiency and security
    - Snowflakes and Standardization
        - *Snowflake System*
            - Systems different from the standard configuration template used within the organization's IaC architecture
        - Add risk to security and long-term supportability
        - Standardization and scripting aim to eliminate special snowflakes for consistency and efficiency

- ○ Importance of Standardization

  - ■ Ensures consistency in large environments with thousands of virtual machines

  - ■ Reduces support and security issues

- **When to Automate and Orchestrate**

  - ○ Automation and Orchestration

    - ■ Critical for secure operations in modern IT and cybersecurity environments

      - ● Streamlines complex processes

      - ● Enhances security

      - ● Improves operational efficiencies

  - ○ Factors to Consider Before Implementing Automation and Orchestration

    - ■ Complexity of the process

    - ■ Cost of development, implementation, and maintenance

      - ● Upfront investment for development and implementation

      - ● Long-term cost savings due to increased efficiency

      - ● Conduct a comprehensive cost-benefit analysis

    - ■ Single points of failure

      - ● Mitigating Single Points of Failure

        - ○ Implement backup systems or manual processes as redundancy measures

- - - Ensure continuity of essential business processes if automation or orchestration fails
  - ■ *Technical debt*
    - ● Cost and complexity of poorly implemented software needing future adjustments
    - ● Managing Technical Debt
      - ○ Regular reviews and updates of automation and orchestration systems
      - ○ Refactoring outdated systems to maintain efficiency and security
  - ■ Ongoing supportability
    - ● Ensuring Ongoing Supportability
      - ○ Develop necessary skills within your team
      - ○ Update systems to adapt to changing technology landscapes
      - ○ Consider both technical and manual redundancy measures
- ○ Determining Whether to Automate or Orchestrate
  - ■ Automate
    - ● For simple, routine tasks like server backups
  - ■ Orchestrate
    - ● For complex tasks with multiple steps, like incident response

- ○ Choosing What to Automate or Orchestrate

  - ■ Focus on tasks and workflows that are repeatable and stable

  - ■ Identify consistent processes that can yield significant time and resource savings

- ○ Final Considerations

  - ■ <u>Decision to automate or orchestrate should be informed by specific needs, resources, and circumstances in an organization</u>

- ○ Continuous Monitoring and Adaptation

  - ■ Conduct continuous monitoring and adaptation of orchestration systems to remain effective

  - ■ Align systems with organizational goals over time

- ● **Benefits of Automation and Orchestration**

  - ○ <u>Increased Efficiency and Time Savings</u>

    - ■ Reduces manual tasks such as system patching, software deployments, and data backups

    - ■ Frees up human resources and reduces the risk of human errors

    - ■ Ensures reliable and consistent outcomes

  - ○ <u>Enforcement of Baselines</u>

    - ■ Enables consistent enforcement of security and compliance baselines across the enterprise network

- Defines standardized configurations and policies aligned with industry best practices and regulatory requirements
- Minimizes vulnerabilities and reduces the likelihood of security breaches

○ Implementation of Standard Infrastructure Configurations

- Increases security and operational stability by maintaining standardized configurations
- Facilitates the creation and enforcement of standard configurations for consistent system setups
- Triggers automated corrective actions for deviations from established standards

○ Scaling in a More Secure Manner

- Enables dynamic scaling of resources while adhering to security protocols
- Provides secure provisioning of new virtual machines, network resources, and access controls
- Ensures scalability without compromising security, especially in cloud environments

○ Increased Employee Retention

- Empowers employees to focus on strategic and creative aspects of their roles
- Leads to higher job fulfillment, engagement, and reduced burnout
- Improves overall satisfaction and retention levels

- ○ Faster Reaction Times

    - ■ Enables rapid response to security incidents and anomalies

    - ■ Automates intrusion detection, threat analysis, and incident response

    - ■ Provides real-time alerts and executes predefined response actions

- ○ Workforce Multiplier

    - ■ Augments the capabilities of existing staff, allowing a smaller team to manage a larger infrastructure

    - ■ Reduces the need for extensive staffing and optimizes resource allocation

    - ■ Saves costs over time compared to manual processes

- ○ Embracing automation and orchestration can bring transformative advantages beyond just efficiency

- **Playbooks**

    - ○ *Incident Response Playbook*

        - ■ Used to describe the specific actions taken in response to emergency scenarios of different types

    - ○ *Playbook*

        - ■ Serves as a checklist of actions to detect and respond to specific types of incidents, ensuring that teams are ready to respond when an incident occurs

- Most organizations have incident response plans documented for each major type of incident
  - Playbook serves as standard operating procedures to guide junior analysts and incident handlers in response to different situations
- Triage and Handling
  - When a triage analyst identifies a suspicious or malicious activity, they categorize it and assign it to an incident handler for remediation based on the organization's procedures
- Creation of Playbooks
  - Each type of incident (e.g., DDoS attack, virus, worm, phishing attack, data exfiltration) should have a playbook with specific responses and procedures
- Resources for Playbooks
  - If an organization doesn't have incident response playbooks, they can find examples online and tailor them to their organization's needs (e.g., incidentresponse.com/playbooks)
  - Example playbooks provide detailed steps for incident response phases (preparation, detection, analysis, containment, eradication, recovery, post-incident activity)

- ○ Automation with SOAR

    - ■ *Security Orchestration, Automation, and Response (SOAR)*

        - ● A class of security tools that facilitates incident response, threat hunting, and security configurations without any human assistance

    - ■ *Runbook*

        - ● An automated version of playbook that can partially or fully automate the incident response process

    - ■ By using runbooks and SOAR, organizations can gain efficiencies and allow analysts to focus on higher-level work

- ○ Common Threats

    - ■ Organizations should have playbooks and runbooks for common threats

        - ● Ransomware

            - ○ *Ransomware Playbook*

                - ■ Stress the need to isolate and disconnect networks and systems quickly to prevent the ransomware from spreading, without powering off systems to preserve evidence

- Data exfiltration
    - *Data Exfiltration Playbook*
        - Describe tasks needed to stop or mitigate an ongoing data exfiltration attack, including forensic analysis to determine data access and transmission
- Social engineering attacks
    - *Phishing Playbook*
        - Include responses to identifying phishing emails, determining user actions, and conducting dynamic analysis to identify indicators of compromise

- **Upgrades and Compliance**
    - Automation and Orchestration in Networking
        - Crucial tool to facilitate efficiency and accuracy in upgrades across large scale networks
        - Need to consider in high-velocity and high-availability environments
    - Role in Upgrades
        - *Streamlining Processes*
            - Helps in upgrading network components efficiently
        - *Reducing Human Error*
            - Minimizes the chances of errors during upgrades

- ■ *Ensuring Consistency*

    - ● Maintains uniformity across the network

- ■ *Version Control and Consistency*

    - ● Conducts regular scans to verify software versions against standards

    - ● Automatically updates devices not meeting baseline requirements

- ■ *Automated Testing and Validation*

    - ● Performs systematic testing of network functionalities post-upgrade

    - ● Checks routing tables, ARP caches, DNS caches, etc., for issues

- ○ Role in Compliance

    - ■ *Continuous Monitoring*

        - ● Compares network configurations against compliance standards

        - ● Identifies and rectifies any deviations promptly

    - ■ *Policy Enforcement*

        - ● Implements security policies uniformly across all systems

        - ● Automatically quarantines non-compliant devices

    - ■ *Log and Evidence Management*

        - ● Generates and preserves logs of network activities and compliance measures

        - ● Presents logs during compliance audits to ensure compliance

- Real-World Use Cases

    - Automated Patch Management

        - Ensures all systems are patched and maintained at the appropriate level

        - Saves time and effort, especially in large networks

    - Compliance Monitoring

        - Provides continuous monitoring and management of network configurations

            - Chef

            - Puppet

            - DNA Center

        - Enforces standard configurations and corrects deviations automatically

- **Automating Network Inventories**

    - Importance of Automated Network Inventories

        - Crucial for modern networks due to virtualization

        - Essential for tracking devices, users, and software

        - Helps manage scalability

            - Vertical scaling

- ● Horizontal scaling
  - ○ *Dynamic Inventory Approach*
    - ■ Transforms static, manually managed lists into real-time, automatically updating repositories
    - ■ Provides a comprehensive view of network assets
  - ○ Benefits of Automated Inventories
    - ■ Real-time updates on device connections and network risks
    - ■ Integration with management tools for automated configuration
      - ● Ansible
      - ● Chef
      - ● Puppet
    - ■ Reduces human error and improves efficiency
  - ○ Using Nmap for Network Scans
    - ■ Conducts IP and port scans to identify devices and services
    - ■ Helps visualize network topology and identify vulnerabilities
    - ■ Enables impact analysis to protect against single points of failure
  - ○ Security and Compliance
    - ■ Supports security and compliance programs (e.g., PCI DSS)
    - ■ Can be configured to block unauthorized access and quarantine devices
  - ○ <u>Automated inventories provide real-time insights into network hardware, software, versioning, and security</u>
    - ■ <u>Crucial for network defense and security</u>

- **Integrations and APIs**
  - *Integration*
    - Combining different subsystems or components into one comprehensive system to ensure they function properly together
  - *Application Programming Interface (API)*
    - A set of rules and protocols used for building and integrating application software
    - Allows products or services to communicate in a controlled environment using a specific data exchange format
  - API Usage
    - Enables software developers to access functions or features of another application programmatically
    - Facilitates automation of administration, management, and monitoring of services and infrastructures
  - API Types
    - *Representational State Transfer (REST)*
      - Uses standard HTTP methods, status codes, URIs, and MIME types for interaction
      - Relies on JSON for data transfer, making it lightweight and easily integrable with existing websites
      - Generally more straightforward and adaptable

- - *Simple Object Access Protocol (SOAP)*
    - Defines a strict standard for message structure, usually in XML format
    - Known for robustness, security features, and transaction compliance
    - Provides higher levels of security and transactional integrity
  - ○ Benefits
    - Drive efficiency, innovation, and scalability in modern systems
    - Allow direct integration of third-party applications into web-based applications
      - APIs enable integration between various services, especially cloud-based services like SaaS or PaaS
    - Allow for seamless experiences and interconnections between different services to enhance their capabilities

- **Source Control**
  - ○ *Git*
    - A distributed version control system for managing different versions of code
    - Developed in 2005 by the creator of Linux
    - Used by a vast number of software projects for version control

- ○ Core Concepts

  - ■ *Git Repository*

    - ● Storage area for code and related files

  - ■ Package Installation

    - ● Use package manager to install Git

- ○ Major Subcommands

  - ■ config

    - ● Set up repository or user options

  - ■ init

    - ● Create or reinitialize a Git repository

  - ■ clone

    - ● Create a working copy of an existing repository

  - ■ add

    - ● Add files to be tracked by the Git repository

  - ■ commit

    - ● Update the Git repository with changes, creating a snapshot

  - ■ status

    - ● Display the status of the repository

  - ■ branch

    - ● Manage branches or pointers to specific repository snapshots

- merge
  - Integrate changes from one branch into a master branch
- pull
  - acquire and merge changes that were made to other repositories and branches into the local working copy
- push
  - Upload a local working copy of a repository to a remote repository
- log
  - Display the changes made to a local repository
- checkout
  - Switch to a specific branch
- ○ Process Flow
  - 1 – Configure global settings including user name
  - 2 – Create a directory where the project will reside
  - 3 – Change into the created directory and then initialize it with Git to designate it as a Git repository
  - 4 – Add project files to the repository
  - 5 – Commit the changes and take a snapshot of the project
- ○ *Branching*
  - Creating a new branch for feature development or bug fixes
- ○ *Merging*
  - Merge changes from a branch back into the master branch

- Collaboration Workflow
    - Pull changes from remote repository, make local changes, and push changes back to remote repository
- Additional Concepts
    - *.gitignore*
        - File to identify files to be ignored during commit
    - **.git/*
        - Directory containing Git's version control files
- <u>Usage Notes</u>
    - Git is heavily used by software developers
    - <u>Understanding Git is important but not necessary to expert level for exams</u>

- **Using Source Control: Demonstration**

Documentation and Processes

Objective 3.1: Explain the purpose of organizational processes and procedures

- **Introduction**
    - IT Governance
        - Used to provide a comprehensive security management framework for the organization
        - Done using policies, standards, baselines, guidelines, and procedures
    - *Policy*
        - Defines the role of security inside of an organization and establishes the desired state for that security program
    - Levels of Security Policies
        - *Organizational*
            - Provide framework to meet the business goals and define the roles, responsibilities, and terms associated with it
        - *System-specific*
            - Address the security of a specific technology, application, network, or computer system
        - *Issue-specific*
            - Address a specific security issue such as email privacy, employee termination procedures, or other specific issues

- ■ *Standard*

  - ● Implements a policy in an organization

- ■ *Guideline*

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

- ● **Common Documentation**

  - ○ *Physical Network Diagrams*

    - ■ Used to show the physical arrangement of network components

    - ■ Includes cabling and hardware layout, similar to a floor plan

    - ■ Can also show rack layouts in data centers

  - ○ *Logical Network Diagrams*

    - ■ Illustrates data flow and device communication

    - ■ Includes subnets, network objects, routing protocols, and domains, etc.

    - ■ Traditionally drawn by hand with symbols for devices

  - ○ *Wiring Diagrams*

    - ■ Shows how cables are connected to devices

    - ■ Can be part of physical or logical network diagrams

    - ■ Includes floor plans or rack diagrams for cable routing

- *Site Survey Reports*

  - Often conducted for wireless network assessments

    - *Radio Frequency (RF) Site Survey/Wireless Survey*
      - Process of planning and designing a wireless network to provide a wireless solution
      - Show access point locations and signal strength

  - *Wired Site Survey*
    - Usually done as part of a preparation for a major upgrade or installation
    - Checks power, space, and cooling for new equipment

- *Audit and Assessment Reports*

  - Delivered after formal assessments
    - Executive summary
    - Scope and objectives
    - Assumptions and limitations
    - Methods and tools
    - Environment and system diagram
    - Security requirements
    - Findings and recommendations
    - Audit results

- ○ *Baseline Configurations*
    - ■ Most stable versions of device configurations
    - ■ Documented set of specifications agreed upon and changeable only through change control procedures
    - ■ Changes require proper testing, approval, and documentation
- ○ These types of documentation are essential for understanding, planning, and maintaining enterprise networks

- ● **Asset Management**
    - ○ *Asset Management*
        - ■ A systematic approach to the governance and realization of value of things over their entire life cycle
        - ■ Types of Assets
            - ● Tangible Assets
                - ○ Buildings, equipment, computers, servers
            - ● Intangible Assets
                - ○ Human capital, intellectual property, goodwill, reputation
        - ■ Key Processes
            - ● Developing, operating, maintaining, upgrading, and disposing of assets in a cost-effective manner
            - ● Includes costs, risks, and performance attributes associated with the asset

- ○ Asset Inventory

    - ■ Maintain a complete list of all assets in the organization

    - ■ Use a database system for efficient management and configuration of asset details

- ○ Asset Identification

    - ■ Each asset should have a unique asset tag and ID for tracking purposes

        - ● *Asset tags*

            - ○ Can be barcodes or RFID tags

            - ○ Critical to ensuring good governance of assets throughout the organization

- ○ *Procurement Lifecycle*

    - ■ Birth to death of an asset

    - ■ Use change management procedures for proper procurement and deployment

        - ● Change Request

            - ○ Verifies business impact

        - ● Procurement

            - ○ Determines the budget and identifies a supplier or vendor

        - ● Deployment

            - ○ Implements a procedure for installing the asset in a secure configuration with a secure baseline on the network

- Maintenance/Operations
    - Implements procedures for monitoring and support
- Disposal
    - Implements procedures for sanitizing any data remnants
- Warranty and Licensing
    - Keep track of asset warranties and support contracts
    - Ensure software licensing compliance for all devices
- User Assignment
    - Assign assets to users based on organizational policies
    - Use asset management database to track user assignments
- Key Points
    - Asset management is crucial for governance and value realization from assets
    - Tangible and intangible assets are managed over their life cycles
    - Use asset tags and IDs for unique asset identification
    - Maintain an inventory list of all assets in a database system
    - Follow the procurement life cycle for proper asset management
    - Keep track of warranties, support contracts, and software licenses
    - Assign assets to users based on organizational policies

- **IP Address Management (IPAM)**
  - *IP Address Management (IPAM)*
    - A methodology and suite of tools used to <u>plan, track, and manage the IP address space</u> inside a network infrastructure
  - Automation and Orchestration
    - Importance of automation and orchestration in managing IP addresses at scale
    - Automation in IP address assignment via DHCP servers is a part of IPAM, but not its entirety
  - Manual vs. Automated IPAM
    - In the past, IPAM was done manually, often with spreadsheets
    - Modern cloud-based networks require automation due to scale and complexity
  - Benefits of Automated IPAM
    - Detects and resolves IP conflicts to maintain network integrity
    - Integrates with DHCP and DNS servers for cohesive management
    - Supports horizontal cloud scaling by assigning IP addresses to new virtual machines automatically
  - Key Features of IPAM Solutions
    - Comprehensive reporting for network performance analysis and anomaly detection

■ Supports cybersecurity efforts by tracking devices connected to the network and identifying unauthorized devices or suspicious traffic patterns

○ Strategic Importance

■ IPAM is not just about adopting new tools, but also involves a strategic shift in managing network infrastructure to enhance efficiency, security, and resilience

- **Common Agreements**
  ○ Three Main Types of Agreements in Network Management
    ■ *Non-Disclosure Agreements (NDAs)*
      - Documented agreement between two parties defining confidential data
      - Used to protect intellectual property
      - Can be between organizations or between an organization and its employee
      - Includes non-competitive clauses
      - <u>An administrative control; not a technical control</u>
      - Legally binding
        ○ Can be enforced with penalties such as fines, forfeiture of intellectual property rights, or jail time

- ■ *Memorandum of Understanding (MOU)*

    - ● Non-binding agreement between two or more organizations

    - ● Details common actions and responsibilities

    - ● More formal than a gentleman's agreement

    - ● Often referred to as a letter of intent

    - ● Often used within organizations or between business units

    - ● Not legally enforceable

    - ● Can be modified or broken without serious consequences

- ■ *Service Level Agreement (SLA)*

    - ● Documented commitment between a service provider and a client

    - ● Defines quality, availability, and responsibilities

    - ● Primarily concerned with supporting and responding to problems within a given time frame

    - ● Outlines responsibilities, guarantees, and warranties for a service and its components

    - ● Can provide predictability in service delivery

    - ● Penalties for not meeting SLA terms depend on the agreement and contract

- **Product Lifecycle**
    - ○ Product Lifecycle
        - ■ Every product, including operating systems, follows a product life cycle

■ Manufacturers may dictate the life cycle, specifying support levels

○ Microsoft's Lifecycle Policy

■ Two types of support

● Mainstream Support

○ Lasts at least five years

● Extended Support

○ Can extend support for another three to five years or longer

○ *End of Life*

■ Once an OS reaches end of life, it is no longer supported by mainstream or extended support

■ *Legacy Operating Systems*

● Products that are no longer supported by the manufacturer

● Using a legacy OS can be dangerous due to lack of software patches and bug fixes

■ Windows XP Example

● Windows XP reached end of life in 2015

● Even though it's no longer supported, some systems still use it, especially in expensive-to-upgrade environments like ICS and SCADA systems

● While it can still be used, Windows XP is extremely vulnerable to attacks due to the lack of support and security patches

- Windows 10 and 11 Support

  - Windows 10 and 11 receive at least five years of mainstream support from Microsoft

  - Large corporations adopting an OS can lead to extended support

  - Feature updates occur every 6 to 12 months, adding new features to the OS without changing baseline requirements

  - Baseline requirements can change with feature updates, so it is important to ensure hardware compatibility

- General Recommendations

  - Upgrade legacy operating systems to modern, supported versions

  - Run the PC Health Check application to ensure hardware compatibility with the latest OS and feature updates

- **Change Management**

  - *Change Management*

    - Orchestrated strategy to transition from an existing state to a more desirable future state

    - Essential in modern business environments to handle inevitable changes like new software or organizational structure

    - Requires precision, planning, and a structured approach to avoid outages and other issue

- ■ Purpose
  - ● Ensure seamless integration of changes into existing architecture and processes
  - ● Ensure changes are properly controlled and implemented using a plan to avoid chaos and resistance from employees
- ■ Critical for guiding organizations safely through changes or transformations
- ○ Change Approval Process
  - ■ Changes must be approved and undergo an assessment process to determine their value and potential impacts
  - ■ *Change Advisory Board (CAB)*
    - ● A body of representatives from various parts of the organization that is responsible for evaluating any proposed changes
- ○ *Change Owner*
  - ■ Responsible for initiating the change request, advocating for the change, and detailing its reasons, benefits, and challenges
- ○ *Stakeholders*
  - ■ Any person with a vested interest in the proposed change, directly impacted or involved in its assessment or implementation
  - ■ Must be consulted, their feedback considered, and concerns addressed before implementing a change

- ○ *Impact Analysis*

    - ■ Conducted before implementing any proposed change to understand potential fallout and immediate effects on the organization, its processes, reputation, and users

    - ■ Helps prepare the organization for the change and maximize its benefits

- ○ By applying change management principles, organizations can adapt, thrive, turn challenges into opportunities, and uncertainties into a defined pathway forward

- ● **Configuration Management**

    - ○ *Configuration Management*

        - ■ Focuses on maintaining up-to-date documentation of network configuration

        - ■ Helps in incident response by ensuring that network diagrams reflect the actual network

    - ○ *Asset Management*

        - ■ Formalized system for tracking network components and managing their life cycle

            - ● Preparation and budget

            - ● Planning purchases

            - ● *Network Design*

                - ○ Determines the best configuration for network devices

            - ● Implementing the devices

- *Operations and Maintenance*
  - Includes operating, maintaining, and supporting the network on a daily basis
  - Accounts for 70% of time spent, emphasizing the need for optimization and improvement
- Optimizing operations
  - Baseline Creation
    - Install the entire network and collect data under normal conditions to create a baseline
    - Useful for troubleshooting by providing a reference for what is considered normal
  - *Cable Management*
    - Process of documenting the network's cable infrastructure
    - Involves labeling cables, documenting their locations, and using a standard naming convention for devices
  - Network Documentation
    - Keep documentation updated to reflect changes in the network
      - Diagrams
      - Wiring schematics
      - Contact information for administrators
      - Policies, procedures, and warranties

- Procedures and Documentation

    - Document procedures for network upgrades and maintenance

    - Store documentation in a centralized location accessible to all technicians

- Knowledge Base

    - Use a central repository (e.g., binder, share drive, SharePoint site) for storing network documentation

    - Ensure technicians know where to find documentation for quick access during incidents

- **Patch Management**

    - *Patch Management*

        - Planning, testing, implementing, and auditing of software patches

    - Purpose

        - Security Enhancement

            - Fixes vulnerabilities in servers, clients, routers, and switches

            - Installs software and OS patches to fix bugs

        - Uptime Improvement

            - Prevents resource exhaustion and crashes

            - Ensures devices and software are up to date

        - Compliance Support

            - A key aspect of compliance assessments

            - Ensures systems are patched against known vulnerabilities (CVEs)

- Feature Upgrades

    - Patches can add new features and functionality

    - Ensures systems are running the latest version for best security and features

- ○ Four Critical Steps

    - Planning

        - Create policies, procedures, and systems for tracking patches

    - Testing

        - Test patches in a small network or lab environment prior to deployment

    - Implementation

        - Deploy patches manually or automatically using tools like SCCM

    - Auditing

        - Scan and verify patch installation to ensure they are properly installed

- ○ Tools

    - Microsoft System Center Configuration Manager (SCCM) for patch management

    - Mobile Device Manager (MDM) for patch management of mobile devices

    - Device Expert by ManageEngine for firmware management of network devices

○ Testing Strategy

■ Use patch rings to deploy patches in stages

■ Start with a small group of machines and expand to larger groups if successful

■ Helps mitigate impact if patches cause issues

○ *Firmware Management*

■ Applies to routers, switches, firewalls, and other network devices

■ Update firmware to fix vulnerabilities and bugs

■ Use centralized tools like Cisco UCS Manager or third-party tools like Device Expert for firmware management

○ Considerations

■ Ensure patches are compatible with systems

■ Test patches before deployment to avoid new issues

■ Use automated tools for large networks for efficiency

■ Conduct auditing to verify patch installation and functionality

○ Patch management is essential for network security, uptime, compliance, and feature enhancement

○ Proper planning, testing, implementation, and auditing are key steps in effective patch management

Disaster Recovery

Objective 3.3: Explain disaster recovery (DR) concepts

- **Introduction**
    - *Disaster Recovery*
        - Enables software, data, or hardware recovery to resume performance of critical business functions after a disaster
- **High Availability Approaches**
    - High Availability Importance
        - High availability ensures continuous operations with minimal downtime for end users
    - *Network Redundancy*
        - Ensures networks remain up and running at all times, increasing availability
        - Servers have two or more network interface cards (NICs) for redundancy and load balancing
            - NICs can operate in pairs or groups for redundancy or increased throughput
        - Use switches and routers with redundant network cables for internal and external connections

- Should be planned in three parts
    - Devices
    - Network interface cards (NICs) and cables
    - Router and switch perspective
        - Ensure redundant paths inside the network and to the internet
- High Availability Approaches and Strategies
    - Active-Active Approach
        - Multiple systems run simultaneously and share the load
        - Maximize resource utilization and ensure service availability even if some systems fail
    - Active-Passive Approach
        - Standby systems remain idle until the primary system fails
        - Provides a reliable fallback mechanism
    - *Load Balancers*
        - Distribute network traffic across multiple servers
        - Ensure no single server bears too much load
        - Continuously monitor server health and reroute traffic away from failed nodes
    - *Content Delivery Networks (CDNs)*
        - Network of geographically distributed servers
        - Deliver content more efficiently and reliably

- Store cached content closer to end users to reduce latency
- Reroute requests to the next closest server in case of server failure or excessive traffic
  - ○ Implementing High Availability
    - ■ Design the network with redundancy at its core
    - ■ Deploy multiple NICs in servers, multiple pathways between switches and routers, and redundant internet connections
  - ○ Combining Strategies
    - ■ Combine active-active or active-passive approaches with load balancers and CDNs
    - ■ Achieve high availability, minimize downtime, and provide a seamless user experience

- **Designing Redundant Networks**
  - ○ Designing Redundant Networks
    - ■ Involves deciding where and how to use redundancy in the network
  - ○ Module/Parts Perspective or Chassis Redundancy
    - ■ e.g., power supplies, network interface devices, hard drives, routers, switches
  - ○ Cost Considerations
    - ■ Different redundancy options have varying costs
    - ■ Decisions impact the overall network cost

- ○ Software Redundancy

  - ■ Software solutions can often provide redundancy without the need for additional hardware

- ○ Protocol Characteristics

  - ■ Protocol choice (e.g., TCP vs. UDP) affects redundancy requirements

    - ● TCP provides additional redundancy by resending packets, while UDP does not

- ○ Redundancy Features in Design

  - ■ Consider redundancy features for powering infrastructure devices (e.g., internal power supplies, battery backups, generators)

- ○ Environmental Conditions

  - ■ Redundancy considerations for environmental conditions (e.g., air conditioning, generators) depend on the criticality of uptime

- ○ Technical and Operational Goals

  - ■ Identify technical goals (e.g., uptime percentage) and operational goals to determine network design and the budget

- ○ Business Application Profiles

  - ■ Categorize business applications into profiles to aid in redundancy design and quality of service considerations

- ○ Establishing Performance Standards

  - ■ Define performance standards to measure success in maintaining high availability networks

- ○ Managing and Measuring High Availability

  - ■ Use metrics and key performance indicators to manage and measure high availability solutions

  - ■ Metrics should align with performance standards and goals

- ○ Design Early for Cost Savings

  - ■ It is cheaper to integrate high-availability practices and design redundancy into a network from the beginning than to retrofit it into an existing network

- ○ Trade-offs in Network Design

  - ■ Key factors in network design

    - ● Time

    - ● Cost

    - ● Quality

  - ■ Trade-offs are necessary, and decisions should align with project goals and constraints

- **Disaster Recovery Metrics**

  - ○ *Disaster Recovery Metrics*

    - ■ Quantifiable standards for planning and evaluating recovery operations

    - ■ Focus on measuring and managing risks to critical operations

    - ■ Used to assess availability and service restoration speed

- ○ Availability and Uptime

  - ■ *Availability*

    - ● Being up and operational

    - ● Measured as uptime percentage (e.g., 5 9's = 99.999% uptime)

    - ● *5 9's of Availability*

      - ○ Maximum of 5 minutes of downtime per year

    - ● *6 9's of Availability*

      - ○ 31 seconds of downtime per year

    - ● Balancing high availability with maintenance needs (e.g., patching, upgrades)

- ○ *Reliability*

  - ■ Concerned with maintaining network operations and data transfer efficiency by not dropping packets

  - ■ Reliable network must be both highly available and pass data effectively

- ○ Measuring Metrics

  - ■ *Mean Time To Repair (MTTR)*

    - ● Average time to repair a network device after failure

  - ■ *Mean Time Between Failures (MTBF)*

    - ● Average time between failures on a device

  - ■ *Maximum Tolerable Downtime (MTD)*

    - ● Longest period a business can be down without causing failure

- The upper limit on the recovery time that the system and the asset owners must resume normal operations within
- Example of MTD Calculation
  - Dion Training's MTD for student support is 12 hours, balancing response speed and cost
  - Geographic team split (Philippines, USA, Egypt) ensures 24/7 coverage and disaster resilience
- *Recovery Time Objective (RTO)*
  - Time taken to resume normal business operations
  - Goal is to resume operations within a defined time frame (e.g., 60 seconds)
- Recovery Point Objective (RPO)
  - Longest tolerable period of data loss
  - Example
    - RPO of 6 hours means data backups should occur at least every 6 hours

- **Redundant Site Considerations**
  - *Redundant Site*
    - A backup location that can take over essential functions in case of primary site failure
    - Important for business continuity and disaster recovery planning

- Four categories based on continuity locations

  - *Hot Sites*

    - Up and running continuously

    - Ready for immediate switch over

    - Requires duplicate equipment and constant data mirroring

    - Expensive

      - Cloud computing has made hot sites more accessible and cost-effective

  - *Warm Sites*

    - Not fully equipped like hot sites

    - Can be up and running in a few days

    - Have basic facilities in place but may need to purchase additional equipment

    - Cheaper than hot sites but with longer response times

  - *Cold Sites*

    - Cheaper than hot and warm sites but adds more time to recovery

    - Contains fewer facilities than warm sites

      - May be just an empty building

    - Can be turned into a new headquarters in one to two months

  - *Mobile Sites*

    - Can be hot, warm, or cold sites, depending on configuration

    - Use portable units like trailers or tents for recovery

- Provide rapid deployment and full functionality for users
  - ○ Fifth category
    - ■ *Virtual Sites*
      - Represent a modern approach to redundant site strategies using cloud-based environments
      - Offer various alternatives for hot, warm, and cold sites.
      - Provide rapid scalability, cost-effectiveness, and easy maintenance
  - ○ Platform Diversity
    - ■ Diversifying operating systems, networking equipment, and cloud platform providers reduces the risk of a single point of failure
    - ■ Enhances resilience and adaptability in the face of unexpected disruptions
    - ■ Allows organizations to leverage unique features and pricing structures of different providers
  - ○ *Continuity of Operations*
    - ■ Refers to an organization's ability to maintain essential functions and services during a disruption
    - ■ Consider both tech stack and people's locations when choosing a redundant site
    - ■ Use geographic dispersion to spread resources across different locations for higher redundancy

- **Training and Exercises**
  - *Tabletop Exercises (TTX)*
    - Use an incident scenario against a framework of controls (red team)
    - Discuss simulated emergency situations and security events
    - Simple to set up but more theoretical, lacking practical evidence
  - *Penetration Testing*
    - Test using active tools and security utilities to simulate an attack
    - Verify threats and vulnerabilities, bypass security controls, and exploit vulnerabilities
    - Scope and resource properly before beginning
    - Can use internal or external teams, preferably third parties or separate internal red teams
      - CompTIA Pen Test+ curriculum is a good resource for learning penetration testing
  - Red, Blue, and White Teams
    - *Red Teams*
      - Hostile or attacking teams in penetration tests or incident response exercises
    - *Blue Teams*
      - Defensive teams in penetration tests or incident response exercises

- Includes system administrators, network defenders, and cybersecurity analysts
    - *White Teams*
    - Administer, evaluate, and supervise penetration tests or incident response exercises
    - Build and support simulated environments for testing
    - Act as referees and report on the exercise outcomes

Troubleshooting Methodology

Objective 5.1: Explain the troubleshooting methodology

- **Step One**
  - *Step 1: Identify the Problem*
    - First step in troubleshooting methodology
    - Gather information from the user
    - Identify user changes and perform backups if applicable
    - Inquire about environmental or infrastructure changes
  - Techniques
    - Ask user to describe the issue, symptoms, and changes
    - Ask about error messages, noises, or other symptoms
    - Inquire if others are experiencing the same problem
    - Determine how long the issue has been happening
    - Ask about recent changes to the system
    - Check if the user has tried any troubleshooting steps
  - Importance of Backups
    - Perform backups before proceeding with troubleshooting steps 2 through 6
    - Backup ensures data safety, especially when replacing hardware or making configuration changes

- ■ Helps restore data in case of unintended consequences during troubleshooting

- **Step Two**
  - ○ *Step 2: Establish a Theory of Probable Cause*
    - ■ Requires questioning the obvious and conducting internal or external research based on observed symptoms
    - ■ Goal
      - Guess the problem based on symptoms, severity, and initial questioning of end users
    - ■ Consider if the issue is hardware, software, operating system, application, or driver-related
    - ■ *Probable Cause*
      - Most likely reason for an issue among all the different possible causes
      - Select the most likely cause first
        - ○ If it does not solve the problem, try other possibilities systematically
  - ○ Research and Inspection
    - ■ External research
      - Utilize online resources like Google and DownDetector

- Internal research
  - Use system documentation, logs, and diagnostic tools for research
- Physically inspect the machine for clues like fan noise, hard drive sounds, or burning smells
- Reproduce the problem if necessary, especially in large organizations where there may be a delay in technician response
- Troubleshooting Approaches
  - *Top-to-bottom Approach*
    - Start from layer seven (application layer) of the OSI model and work down to layer one, checking each layer for issues
  - *Bottom-up Approach*
    - Start from layer one (physical layer) and work up to layer seven, checking each layer for issues
  - *Divide and Conquer Approach*
    - Start from a midpoint in the OSI model and test for issues, then determine if the problem lies above or below that point
- Collaboration and Knowledge Sharing
  - Communicate with other technicians or colleagues who may have worked on the same issue to avoid duplication of efforts
  - Learn from others' experiences and document what has already been tried to avoid repeating unsuccessful steps

- **Step Three**
    - *Step 3: Test the Theory*
        - Purpose
            - Determine the cause of the problem
        - CompTIA's Definition
            - Test the theory to determine the cause
                - Once confirmed, determine the next steps to resolve the problem
                - If not confirmed, establish a new theory or escalate
    - Step 3 Focus
        - Testing the theory without making any configuration changes to the system
            - Example
                - Testing a theory that a computer won't turn on because it's unplugged from the wall outlet
                - Solution
                    - Confirm the theory by plugging in the computer and turning it on
        - If Theory Is Not Confirmed
            - Establish a new theory based on observed symptoms

- Example
  - If the computer still doesn't turn on after being plugged in, consider that the wall outlet may not provide enough power
  - Testing the New Theory
    - Use tools like a volt meter to test the theory (e.g., measuring voltage in the wall outlet)
- If the theory is confirmed
  - Determine the next steps to resolve the problem (e.g., fixing or replacing the power supply)
- Possible Outcomes
  - Theory Confirmed
    - Proceed to fix the issue
  - Theory Not Confirmed
    - Come up with a new theory
    - Test the new theory
    - If confirmed, proceed to fix the problem
  - Lack of Skills and Authority
    - Escalate if the problem requires skills or authority
    - Example
      - If a fix requires a part replacement or policy change outside expertise, escalate to the relevant team

- Inability to Solve
    - Escalate to higher-tier support (e.g., Tier 2 or Tier 3 technicians) for additional assistance
    - Tiered Support Structure
        - Tier 1 – Basic problem-solving
        - Tier 2 – More advanced problem-solving
        - Tier 3 – Subject matter experts (SMEs) and system administrators

- **Step Four and Step Five**
    - *Step 4: Establish a Plan of Action*
        - Purpose
            - Solve the underlying probable cause identified in steps 2 and 3
        - Options
            - Repair
            - Replace
            - Create a workaround
        - Considerations
            - Repair costs versus replacement costs
            - Organizational guidelines on repair versus replacement
            - Temporary solutions for critical issues
            - Cost-effective solutions for temporary needs

- ○ *Step 5: Implement the Solution*
    - ■ Devise a plan detailing resources, time, and cost associated with the solution
    - ■ Identify impacts on other users or systems
    - ■ Seek permission according to corporate policies and procedures
    - ■ Examples
        - ● Rebooting servers
        - ● Updating systems
        - ● Replacing hardware
    - ■ Stick to the plan and seek reauthorization for any changes
    - ■ Impact of Solutions
        - ● Consider the scale of the system affected (e.g., end-user machine versus server)
        - ● Rebooting servers can impact authentication and access across the organization
        - ● Disconnecting users from a file server may not affect other services like printing
- ○ Final Notes
    - ■ Follow the established plan and seek reauthorization for any changes
    - ■ Ensure you are working as part of a larger team and consider the broader impact of your actions on the network

- **Step Six**

  - *Step 6: Verify System Functionality*

    - Purpose

      - Ensure the resolution implemented in previous steps effectively addresses the root cause and prevents future issues

  - Steps Recap

    - Step 1 – Identify Problem

    - Step 2 – Establish Theory of Probable Cause

    - Step 3 – Test Theory

    - Step 4 – Establish Plan of Action

    - Step 5 – Implement Solution

    - Step 6 – Verify Full System Functionality

  - Verification Process

    - Confirm resolution addresses original problem

    - Check replaced components for proper operation (e.g., power supply, RAM)

    - Ensure system functions normally post-resolution

    - Inspect for any additional damage or disconnected components

    - Verify disabled/uninstalled software remains inactive

    - Review logs and diagnostic tools for abnormalities

    - Update software and device drivers for security and functionality

- ○ Implementing Preventative Measures
    - ■ Educate users on secure practices (e.g., safe downloading habits)
    - ■ Enforce policies (e.g., restricting downloads, no food/drink near equipment)
    - ■ Address recurring issues by proposing policy changes to management
- ○ Role of Technician
    - ■ Ensure system functions as well as or better than before issue
    - ■ Prevent future issues through education and policy enforcement
    - ■ Collaborate with management to implement effective preventative measures

- **Step Seven**
    - ○ *Step 7: Troubleshooting Documentation*
        - ■ Documenting findings, actions, and outcomes
            - ● What was wrong
            - ● What was done about it
            - ● How to prevent it in the future
    - ○ Methods
        - ■ *Trouble Ticketing System*
            - ● Document problems, assignments, actions taken, and solutions
        - ■ *Internal Knowledge Base*
            - ● Store troubleshooting steps and lessons learned

- ■ *Frequently Asked Questions (FAQs)*

  - ● Contains support articles based on common user questions.

- ○ Benefits

  - ■ Helps new technicians learn from past experiences

  - ■ Facilitates trend analysis to identify common issues

  - ■ Justifies resource needs based on workload

- ○ Tools

  - ■ Any system can be used as long as it allows for documentation of findings, actions, and outcomes

  - ■ Examples

    - ● Freshdesk

    - ● Jira

    - ● HelpScout

    - ● Intercom

- ○ Usage

  - ■ Document findings as soon as problems are identified

  - ■ Update documentation as troubleshooting progresses

  - ■ For larger problems, update documentation regularly

- ○ Trend Analysis Example

  - ■ Password Reset Trend

    - ● Identified through ticket analysis

    - ● Led to implementing a self-service password reset option

- Resulted in a 90% reduction in password-related tickets
  - Resource Justification Example
    - Increased ticket volume due to new systems without user training
    - Used ticket data to justify need for more help desk staff
    - Highlights the importance of adequate resources for efficient support

- **Understanding the Troubleshooting Methodology: Demonstration**

Troubleshooting Tools

Objective 5.5: Given a scenario, use the appropriate tool or protocol to solve networking issues

- **Hardware Tools**
  - *Snips and Cutters*
    - Used to cut cables from a larger spool or bundle
  - *Cable Strippers*
    - Remove outer jacket and insulation from cables for connector attachment
  - *Cable Crimpers*
    - Attach connectors to cable ends
  - *Cable Testers*
    - Verify continuity and proper pinouts of cables, ensuring no breaks
    - *Multitester*
      - Supports various cables and connectors for testing
  - *Wire Maps*
    - Work like a cable tester
    - Diagnose issues in twisted pair Ethernet cables
      - *Open Pair*
        - Occurs when one or more conductors in the pair are not connected on one of the pins at either end of the cable

- *Shorted Pair*

    - Occurs when conductors of a wire pair are connected to each other at any location within the cable

- *Short Between the Pairs*

    - Conductors of two wires in different pairs are connected at any location within the cable

- *Reverse Pair*

    - Two wires in a single pair are connected to the opposite pins of that pair on the other end of the cable

- *Cross Pair*

    - Both wires of one color pair are connected to the pins of a different color pair on the opposite end

- *Split Pair*

    - A wire from one pair is split away from the other and crosses over the wire into an adjacent pair

- *Cable Certifiers*

    - Determine cable category, data throughput, length, and other characteristics

- *Multimeters*

    - Check voltage, amperage, and resistance of copper cables

- *Punchdown Tools*

    - Terminate wires on punchdown blocks and strip excess insulation

- *Tone Generators/Toner Probe*

    - Generate tones on one end of a connection for cable tracing

    - Used to understand where the cables are running inside the walls for unlabeled or undocumented network

- *Loopback Adapters*

    - Create a loopback for testing connectivity using transmit and receive pairs

    - Different for Ethernet and Fiber

- *Time Domain Reflectometers (TDR)*

    - Locate breaks in copper cables and estimate distance to the break

- *Optical Time Domain Reflectometers (OTDR)*

    - Locate breaks in fiber optic cables and measure loss

- *Fiber Light Meters*

    - Measure attenuation in fiber optic cables

        - Multimode fiber – use LED based

        - Single mode fiber – use laser-based

- *Fusion Splicers*

    - Permanently join two fiber optic cables together

- *TAPs*

    - Copy or split packets for analysis, security, or network management

- *Spectrum Analyzers*

    - Measure signal amplitude and frequency variation within a spectrum

        - x-axis – frequency

- y-axis – amplitude
  - ○ <u>Understand which tool to use to troubleshoot which type of cable and which type of issue</u>

- **Software Tools**
  - ○ *Wi-Fi Analyzers*
    - ■ Used for conducting wireless surveys to ensure proper coverage
    - ■ Helps prevent overlap between wireless access point coverage zones and channels
    - ■ Display information of detected networks
      - ● SSID
      - ● Signal strength
      - ● Channel information
    - ■ Useful for visualizing network coverage areas on floor plans
  - ○ Protocol Analyzers and Packet Capturing Tools
    - ■ *Protocol Analyzer*
      - ● Used to capture and analyze signals and data traffic over a communication channel
        - ○ <u>Wireshark</u>
        - ○ Ethereal
        - ○ Protocol expert
        - ○ Netasyst

- - - Network analyzer
    - Observer
    - LanHound
    - EtherPeek
  - *Packet Capturing Tool*
    - Captures packets running over a network connection in real time and save them for later analysis
      - <u>Wireshark</u>
      - tcpdump
      - WinDump
      - PRTCG network monitor
      - SolarWinds
      - NetworkMiner
  - Helps troubleshoot network performance issues by analyzing packet flow
  - Used by cybersecurity professionals to trace connections and identify malicious traffic
- *Bandwidth Speed Testing Tools*
  - Used to measure real-world throughput across a network
    - LAN Speed test
    - Helios LAN test software
  - Helps determine if internet or local area network performance is adequate

- ○ *Port Scanners*

  - ■ Used to determine which ports are open on a network

    - ● <u>Nmap</u>

    - ● SolarWinds Port Scanner

    - ● Lansweeper

  - ■ Reveals open, closed, or filtered ports and presence of security devices like firewalls

- ○ *NetFlow Analyzers*

  - ■ Used for monitoring, troubleshooting, and analyzing traffic flow data

  - ■ Helps conduct capacity planning and ensure appropriate resource usage

  - ■ Can identify types of traffic consuming network resources and optimize performance

- ○ *IP Scanners*

  - ■ Used to search for and detect IP addresses and devices on a network

    - ● <u>Nmap</u>

    - ● Free IP Scanner

    - ● IP Address Manager

    - ● PRTG Network Monitor

    - ● Angry IP Scanner

    - ● Network Scanner

    - ● IP Range Scanner by Lansweeper

■ Helps manage networks and identify rogue devices connected to the network

○ <u>Understand when and which of the software tools should be used for a particular thing in network management and troubleshooting</u>

- **ipconfig, ifconfig, and ip**
    - *IP Configuration (ipconfig)*
        - Used in Windows to display TCP/IP network configuration values and refresh DHCP and DNS settings for Windows client servers
        - Commands
            - ipconfig
                - Displays basic TCP/IP network configuration
            - ipconfig /release
                - Releases current IP address
            - ipconfig /renew
                - Attempts to get a new DHCP address
            - ipconfig /all
                - Detailed TCP/IP configuration including hostname
                - Network adapter model
                - Physical address (MAC)
                - DHCP and auto-configuration status
                - Lease times

- ○ Default gateway
- ○ DHCP server
- ○ DNS server IP addresses
- ○ *Interface Configuration (ifconfig)*
  - ■ Used in Unix, Linux, and OS X to display and configure IP address information
  - ■ Commands
    - ● ifconfig
      - ○ Displays status of currently active interfaces
    - ● ifconfig [interface]
      - ○ Displays information for a specific interface (e.g., ifconfig en0)
    - ● ifconfig -a
      - ○ Displays all interfaces, including inactive ones
      - ○ Provides detailed information similar to `ipconfig /all` in Windows
    - ● ifconfig -v
      - ○ Verbose – display additional information or details
    - ● ifconfig down
      - ○ Turns off a network interface
    - ● ifconfig up
      - ○ Activates a network interface

https://www.DionTraining.com

- ○ Deprecated in modern systems in favor of the `ip` command
- ○ *Internet Protocol (ip)*
  - ■ Modern replacement for `ifconfig` in Unix, Linux, and OS X
  - ■ Supports interface configuration, routing, and more
  - ■ Commands
    - ● ip a
      - ○ Displays interface configuration information
    - ● ip a add [ip_address] dev [device]
      - ○ Assigns a static IP address to an interface (e.g., ip a add 192.168.1.123 dev eth0)
    - ● ip a del [ip_address] dev [device]
      - ○ Removes a static IP address from an interface
    - ● ip link set dev [device] address [MAC_address]
      - ○ Changes the MAC address (Mac spoofing)
    - ● ip link set dev [device] promisc on
      - ○ Sets the interface to promiscuous mode
    - ● ip link set dev [device] down / ip link set dev [device] up
      - ○ Disables/enables a network interface

- **ping and traceroute**
    - ○ ping
        - ■ Checks connectivity between two devices, commonly used in network troubleshooting
        - ■ Commands
            - ● ping [domain name]
                - ○ Example – ping jasondion.com
            - ● ping -n [number] [domain name]
                - ○ Sends a specified number of pings (e.g., ping -n 10 jasondion.com to ping 10 times)
            - ● ping -t [domain name]
                - ○ Sends pings continuously
                - ○ For Windows
                - ○ Useful to see if WAN link is up all the time to see if the connection is working or not, or if it is having any issues
            - ● ping -c [count] [domain name]
                - ○ Sends a specified number of pings
                - ○ For Linux/Unix/OSX
        - ■ Usage in Windows
            - ● Sends four pings by default
            - ● Use `-t` for continuous pinging

- ■ Usage in Linux/Unix/OSX

  - ● Runs continuously by default

  - ● Use `-c [count]` to specify the number of pings

- ■ Stopping Continuous Pings

  - ● Ctrl + C

- ■ IPv6 Usage

  - ● ping -6 [domain name]

- ○ traceroute/tracert

  - ■ traceroute – Unix, Linux, and OS X

  - ■ tracert – Windows

  - ■ Displays the path between your device and its destination, showing source and destination IP addresses for each hop (router/firewall)

    - ● *Hop*

      - ○ Any router or firewall that is in the path of the transmission from the client to the destination

  - ■ Command

    - ● traceroute [domain name]

  - ■ IPv6 Usage

    - ● traceroute -6 [domain name]

  - ■ How it Works

    - ● Uses the Time to Live (TTL) field in the IP packet header to identify each hop

- Firewall/Device Responses
    - Some devices may not respond to ICMP or ping traffic, causing timeouts in the traceroute output
- Troubleshooting Steps
    - 1 – Ping a well-known website (e.g., `google.com`) to check network and internet connectivity
        - If successful, but domain name resolution fails, check DNS settings
    - 2 – If unable to ping a known IP address (e.g., `8.8.8.8`), check internet connection
    - 3 – If unable to ping the default gateway, check local network connections
    - 4 – If unable to ping the local IP address, check network card and drivers
- traceroute Usage in Troubleshooting
    - Helps identify issues between the router and the destination by showing all routers in between

- **nslookup, dig, and hostname**
    - *nslookup (Name Server Lookup)*
        - Used to query the Domain Name System (DNS) for mapping domain names to IP addresses or other DNS records
        - *Non-interactive Mode*
            - Displays just the name and requested information for a host or domain name

- - ■ *Interactive Mode*
      - Allows more in-depth queries and control over the environment
      - Can change the server for queries and the type of records to search for
  - ○ *dig*
    - ■ Used for queries against DNS name servers
    - ■ Available for Linux, Unix, and OS X systems
    - ■ Does not support an interactive mode like nslookup
      - Focuses on non-interactive queries
    - ■ Specify record types when entering the command
  - ○ *hostname*
    - ■ Displays the hostname portion of the full computer name for a system
    - ■ Works on Windows, Linux, Unix, and OS X

- **arp**
  - ○ *arp (Address Resolution Protocol) command*
    - ■ Displays and modifies entries in the arp cache
    - ■ *arp Cache*
      - Stores IP addresses and their associated MAC addresses
    - ■ Interacts with Layer 2 (MAC addresses) and Layer 3 (IP addresses) bindings

- ■ Compatibility
  - ● Windows
  - ● Linux
  - ● Unix
  - ● OS X
- ○ Commands
  - ■ arp -a
    - ● View ARP cache
  - ■ arp -d [IP]
    - ● Delete IP address mapping
  - ■ arp -d
    - ● Clears entire cache
  - ■ arp -s [IP] [MAC]
    - ● Static mapping
      - ○ Useful for pre-configuring devices or preventing timeouts
- ○ An arp entry will be deleted by default after 21,600 seconds (about 6 hours)

- ● **netstat**
  - ○ *netstat (Network Statistics)*
    - ■ Used to display information for IP based connections on a client
      - ● Current sessions
      - ● Source and destination IPs

- Port numbers
  - Usage
    - Windows
    - Linux
    - Unix
    - OS X
- Basic Command
  - netstat
    - Displays a simplified output with four columns
      - Protocol
      - Local address
      - Foreign address
      - State
- Advanced Options
  - netstat -a
    - Shows all sockets (listening and non-listening) and all protocols (TCP, UDP, ICMP)
  - netstat -n
    - Displays all IP address numbers instead of hostnames
  - netstat -an
    - Combines both options to show IP address numbers and listening status

- netstat -ano
  - Shows IP address numbers and listening status and includes a fifth column (PID) to identify which process owns each network connection
    - Use the PID column with `tasklist` command to identify which application or service is communicating over the network
  - Malware Detection
    - Use `netstat ano` to identify suspicious connections that may indicate malware or botnet activity
- netstat -s
  - Used to get statistics
    - IPv4 – use TCP and UDP connections
    - IPv6 – use TCP and UDP connections
    - ICMPv4
    - ICMPv6
  - Helps determine network health and baseline

- **tcpdump**
  - *tcpdump*
    - Command line tool for displaying TCP/IP and other packets on a network
    - Platform Compatibility

- ● Included by default in Linux, Unix, and OS X
- ● Needs to be downloaded and installed on Windows
  - ■ Captures network traffic for real-time display
  - ■ Can be stored in a Packet Capture (PCAP) file for later analysis
- ○ Packet Information
  - ■ Timestamp
  - ■ IP version
    - ● IPv4 – IP
    - ● IPv6 – IP6
  - ■ Source and destination IP addresses and ports
  - ■ Flags
  - ■ Sequence number
  - ■ Acknowledgment number
  - ■ Windowing number
  - ■ Length
  - ■ Options – (if available) can be found between windowing number and length
- ○ PCAP File can be loaded into Wireshark for graphical analysis or reloaded into tcpdump for text-based analysis
- ○ tcpdump and Wireshark are often used together to capture, and then analyze packets
- ○ tcpdump Demonstration

- **nmap**

  - *nmap (Network Mapper)*

    - Used to discover hosts and services on a computer network

    - Features

      - Host discovery

      - Service detection

      - Operating system detection

    - Usage

      - Port scanning

      - IP scanning

      - Software fingerprinting services

      - Creating network maps

      - Documenting networks

      - Identifying rogue devices

  - nmap Demonstration

- **Basic Network Device Commands**

  - *Network Platform*

    - Refers to routers, switches, and firewalls regardless of brand

    - Each manufacturer has its own command line interface but they are similar in function and commands, often based on Cisco

- Cisco
    - show interface
    - show config
    - show route
- Juniper
    - show interfaces
    - show configuration
    - show route
- Sidewinder
    - cf interface
    - cf config
    - cf route status
  - Focus Commands
    - *show interface*
      - Displays <u>interface statistics</u>
      - Use `show interface <interface>` for specific interfaces
      - Check for interface and line protocol status
        - IP address validity
        - Bandwidth
        - MTU size
        - Runs, giants, or errors
        - Collisions

- ■ *show config*
    - ● Displays <u>current system configuration</u>
    - ● No options or arguments, just `show config`
    - ● Key areas
        - ○ Shared secrets
        - ○ System settings
        - ○ SNMP settings
        - ○ IP settings
        - ○ VMPS (VLAN Management Policy Server)
        - ○ DNS settings
        - ○ TACACS + configuration
        - ○ Bridge
        - ○ VTP settings (VLAN Trunking Protocol)
        - ○ Spantree protocol settings
        - ○ CGMP (Cisco Group Management Protocol) – Cisco-specific
        - ○ Syslog
        - ○ NTP (Network Time Protocol) settings
        - ○ Permit list – ACL
        - ○ Device module
- ■ *show route*
    - ● Displays routing table information
    - ● Normally used as `show ip route` for IP-based networks

- Key areas:
  - Code legends
  - Gateway of last resort
    - Derived sources
    - Type of route
    - Remote network address
    - Administrative distance and metric
    - Next router IP
    - Time
    - Interface

- **More Network Device Commands**
  - *show mac address-table*
    - Displays the Mac address table on a Cisco switch
    - Maps Mac addresses to corresponding switch ports
    - Used for troubleshooting and identifying connected devices and ports
  - *show arp*
    - Displays the ARP table (Address Resolution Protocol) on a device
    - Maps IP addresses to Mac addresses
    - Used to verify correct mappings and detect ARP cache poisoning or spoofing

- ○ *show vlan*

    - Configures VLAN (Virtual Local Area Network) settings on a switch

    - Segments network traffic for improved performance and security

    - Displays VLAN mappings, including VLAN numbers, names, status, and associated ports

- ○ *show power*

    - Displays and configures power settings, especially for Power over Ethernet (PoE) devices

    - Manages power distribution and troubleshoots PoE issues

    - Shows power allocated, used, and available per port

- **Discovery Protocols**

    - ○ *Discovery Protocols*

        - Simplify the task of understanding and managing various connected devices on network

        - Crucial for managing complex network environments

    - ○ *Link Layer Discovery Protocol (LLDP)*

        - Open standard protocol defined in IEEE 802.1AB

        - Allows devices on a network to advertise themselves and discover information about other devices

        - Promotes interoperability across multiple vendors

        - Provides central details

- Device identification

- Capabilities

- Associated ports

■ Offers clear view of network topology for effective network management

○ *Cisco Discovery Protocol (CDP)*

■ Proprietary protocol developed by Cisco

■ Similar functionalities to LLDP but tailored for Cisco-based environments

■ Facilitates collection of detailed device information

- Model numbers

- IP addresses

- Connected interfaces

- Power consumption

■ Optimizes performance and troubleshooting in Cisco networks

■ Provides proprietary insights into device communication

○ Role in Network Management

■ Essential for maintaining an accurate and comprehensive inventory of network devices

■ Dynamic and updating environment providing rich dataset of device interconnections and data flow

■ Ensures network security, performance, and reliability

■ Helps identify unauthorized or rogue devices for immediate action

■ Performance Optimization

- Enables informed decisions for network segmentation, load balancing, and quality of service settings
  - ○ Security Considerations
    - ■ Requires careful configuration and management to avoid network issues and security vulnerabilities
    - ■ Misconfiguration can expose network topology to attackers
    - ■ Information accessibility must be restricted to authorized personnel and devices
  - ○ Conclusion
    - ■ LLDP and CDP are foundational tools for modern network management
    - ■ Detailed view of network infrastructure empowers network administrators
    - ■ Vital as networks grow in size and complexity
    - ■ LLDP suitable for multi-vendor environments
    - ■ CDP preferred for Cisco-only networks due to additional detailed information

Troubleshooting Physical Networks

Objective 5.2: Given a scenario, troubleshoot common cabling and physical interface issues

- **Network Cable Limitations**
    - Twisted Pair Copper Cables
        - Cat5
            - Also known as Fast Ethernet or 100BASE-TX
            - Operates at 100 Mbps up to 100 meters
        - Cat5e
            - Also known as Gigabit Ethernet or 1000BASE-T
            - Operates at 1000 Mbps/1 Gbps up to 100 meters
        - Cat6
            - Also known as 1000BASE-T/10GBASE-T
            - Operates at 1 Gbps up to 100 meters, or 10 Gbps up to 55 meters
        - Cat6a/Cat7
            - Also known as 10GBASE-T
            - Operates at 10 Gbps up to 100 meters
        - Cat8
            - Also known as 40GBASE-T
            - Operates at 40 Gbps up to 30 meters

- ○ Coaxial and Twin Axial Copper Cables

  - ■ Coaxial Cables

    - ● Supports speeds up to 100 Mbps up to 500 meters

  - ■ Twin Axial Cables

    - ● Supports speeds up to 10 Gbps, but limited to 5 meters

    - ● Newer versions can reach 100 Gbps up to 7 meters

- ○ Fiber Cables

  - ■ Multimode Fiber

    - ● 100BASE-FX – 100 Mbps up to 2 kilometers

    - ● 100BASE-SX – 100 Mbps up to 300 meters

    - ● 1000BASE-SX – 1 Gbps up to 220-500 meters

    - ● 1000BASE-LX – 1 Gbps up to 550 meters

    - ● 10GBASE-SR – 10 Gbps up to 400 meters

  - ■ Single Mode Fiber

    - ● 1000BASE-LX – 1 Gbps up to 5 kilometers

    - ● 10GBASE-LR – 10 Gbps up to 10 kilometers

- ○ Cable Considerations

  - ■ Shielded vs. Unshielded Twisted Pair

    - ● Shielded offers more protection from EMI but is more expensive

      - ○ Note: Fiber cables are truly immune to EMI

    - ● Unshielded

      - ○ Inexpensive

- ○ Easy to install
        - ○ lightweight
        - ○ Flexible
      - ● 100 meters – maximum recommended length for twisted pair cables
  - ■ Plenum vs. Riser Rated
    - ● Plenum cables
      - ○ Have higher fire ratings for spaces between ceilings and floors
      - ○ Used horizontally
    - ● Riser cables
      - ○ Used vertically between floors
      - ○ Used in non-plenum areas only
- ○ Cable Applications
  - ■ *Rollover/Console Cables*
    - ● A type of null-modem cable that connects a computer terminal to a router's console port for out-of-band communication
  - ■ *Crossover Cables*
    - ● Special type of network cable that connects two Ethernet devices directly without a switch or router in between

- *Power over Ethernet (PoE)*
    - Technology that passes electrical power over Ethernet cables to power devices like wireless access points or IP cameras
    - Requires at least Category 5e cables
    - Can provide 15.4 to 100 watts of power using twisted pair

- **Cable Signal Issues**
    - *Attenuation*
        - Loss of signal strength on a network cable or connection over the length of the cable
        - Common in both wired and wireless connections
        - Mainly affects copper cables like twisted pair or coaxial cables
        - Longer cables have higher resistance, causing the signal to weaken
            - Maximum distance for twisted pair cables is about 100 meters due to attenuation
            - Coaxial cables can reach distances of up to about 500 meters before attenuation becomes too much
        - Factors Affecting Attenuation
            - Distance is the main factor
            - Other factors
                - Frequencies used

- All networking and electrical cables operate at specific frequencies
- Higher frequencies allow for higher bandwidth but can lead to interference if neighboring cables use similar frequencies
  ○ *Noise in the environment*
    - Additional electrical or radio frequency noise in the area where the cables are operating
      - Noise from machinery or power generators can increase attenuation
  ○ *Physical surroundings*
    - Things like temperature, the construction of the walls or other barriers, and the type of wire insulation, etc.
- Mitigating Attenuation
  - Use proper cables for the environment
  - Shorten cable distances
  - Use amplifiers or repeaters to boost signals for longer distances
- Fiber Cables
  - Attenuation occurs at much longer distances compared to copper cables
  - Cheaply constructed or dirty connectors can cause attenuation

- Use higher quality cables or clean connectors to mitigate attenuation
  - *Interference*
    - Occurs when multiple cables operate in the same frequency band and are in close proximity
    - Mitigation
      - Use high-quality twisted pair cables or higher category rated cables
      - Plan cable runs to avoid running cables directly next to high-power cables
  - *Decibel (dB) Loss*
    - Measures the amount of signal deterioration on a connection
    - Higher dB loss indicates more signal deterioration
      - For copper cables
        - Decrease in voltage
      - For fiber cables
        - Amount of light lost
    - Use higher quality cables or clean connectors to mitigate dB loss
  - Testing Tools
    - *Cable Certifier*
      - Measures attenuation and dB loss on network cables

- ■ *Fiber Light Meter*
  - ● Tests for attenuation on and dB loss fiber connections
- ■ *Spectrum Analyzer*
  - ● Detects interference by analyzing frequencies and signals on a cable (copper and fiber)
- ■ *Cable Analyzer*
  - ● Measures dB loss in copper cables
- ○ Exam Tip
  - ■ Understand the tools used to troubleshoot cable signaling issues

- **Copper Cable Issues**
  - ○ *Incorrect Pinouts*
    - ■ Testing a twisted pair network connection that is not working may indicate an incorrect pinout
    - ■ Can occur at the patch panel, wall jack, or RJ45 connector
      - ● Patch Panels
        - ○ Typically use a TIA568B pinout
        - ○ Visually inspect the back of the patch panel and its punch down block to verify correct colors in proper pins
      - ● Wall Jacks
        - ○ Also know as keystone
        - ○ Have 4 pins on each end

- - - Labeled as pins 1 through 8 or using color-coded stickers/markers
    - RJ45 Connectors
        - Connect copper pins to inner twisted pair wires
        - Pins can be counted from left to right when the small plastic clip is facing downward (1 to 8 pins)
        - Ensure inner twisted pair wires are color coded correctly
    - Testing and Verification
        - Use a cable tester or wire mapping tool to test and verify pinouts
        - If incorrectly pinned out
            - Re-strip and re-punch wires
            - Replace the RJ45 connector
- Bad Ports
    - Network interface cards (NICs) and Ethernet ports on switches/routers can have issues
    - Use a loopback plug and specialized software to test Ethernet ports on NICs
        - For switches/routers
            - Connect a loopback plug to the port and run a test using specialized software
        - Replace the NIC or switch/router port if found to be faulty

- Opens and Shorts

    - *Open*

        - Occurs when there is a break in the wires between the source and destination

    - *Short*

        - Indicates two wires are connected together somewhere in the connection

        - To fix a short

            - Rewire the RJ45 connection

            - Examine the cable for damage

- Tools

    - For incorrect pinouts, opens, and shorts

        - Cable tester

        - Cable certifier

        - Wire mapping tool

    - For bad ports

        - Loopback adapter

        - Loopback plug

- Exam Tip

    - Understand the tools used to troubleshoot copper cable connectivity issues

- **Fiber Cable Issues**
  - ○ Incorrect Transceivers
    - ■ *Transceivers*
      - Both transmitters and receivers in one device
      - Convert network connections from one type to another
      - Work at Layer 1 in the OSI model
      - Commonly used in routers and switches for fiber connections
    - ■ If the wrong transceiver is used, the connection won't work
    - ■ Many transceivers are hot-pluggable, allowing easy replacement without shutting down devices
    - ■ Use the correct transceiver to avoid data loss and connectivity issues
  - ○ Reversed Transmit and Receive
    - ■ Most fiber connections consist of separate cables for transmission and reception
    - ■ Connecting the transmit cable to the receive port, and vice versa, will prevent a valid connection
    - ■ Easily identified and fixed by swapping the cables
  - ○ Dirty Optical Cables
    - ■ Dirt or dust on fiber optic cables and connectors can cause performance issues or connection problems
    - ■ Even small particles can severely block light transmission

■ Cleaning methods

  ● *Dry cleaning*

    ○ Involves simply using light pressure while rubbing the end face of a fiber cable or connector using a dry cleaning cloth in one direction

  ● *Wet cleaning*

    ○ Lightly moistening a piece of lint-free cloth with a fiber optic cleaning solution (91% or higher isopropanol alcohol), and then wiping the end face of the cable in one direction as well

    ○ More invasive but necessary for removing fingerprints

■ <u>Use a fiber light meter to quantify the need for cleaning based on decibel readings</u>

● **Ethernet Issues**

  ○ *LED Status Indicators*

    ■ Used to diagnose issues in fiber optic and copper connections

    ■ Network interface cards (NICs) typically have two lights

      ● Activity light

        ○ Off – no link or connection established

        ○ Solid orange – link or connection established

        ○ Blinking orange – data activity occurring

- Link speed light

  - Off – operating at 10 Mbps

  - Orange – operating at 100 Mbps

  - Green – operating at 1 Gbps

- Network switches also have LEDs for each Ethernet port to indicate status and activity

- Duplexing Issues

  - *Duplex Mismatch*

    - Occurs when one device thinks the connection is full duplex, while the other thinks it is half duplex

    - Most common issue

    - Symptoms

      - High rate of packet loss without hight rate of jitter

      - High receive error rate

      - Runt packets

    - Prevention

      - Configure both devices to use autonegotiate

      - Manually configure devices as full or half duplex if autonegotiate fails

      - <u>Use full duplex for switches, as each switch port is its own collision domain</u>

- **Interface Issues**
  - *Interface Issues*
    - Refer to any problems in the network's interface operation that can impact data transmissions and network performance
  - Types of Interface Issues
    - Increasing Interface Counters
      - *Cyclical Redundancy Check (CRC) Errors*
        - Occur when the data block's integrity check upon reception does not match the value attached during transmission, indicating data corruption or alteration
        - Causes
          - Noise interference
          - Physical issues affecting network conductivity
      - *Runts*
        - Frames smaller than the minimum frame size
        - Created by collisions or disruptions during packet transmissions
        - Causes
          - Network card malfunction
          - Using a large collision domain
          - Cabling issues

- *Giants*
  - Frames that exceed the maximum frame size of the network
  - Often created due to misconfiguration or malfunctioning of a network device
  - Effects
    - Network congestion
    - Poor performance
- *Drops*
  - Occur when a device's buffer is full and can't accommodate incoming frames or packets anymore
  - Causes
    - High network traffic
    - Device operating beyond its capacity limits
- Issues with Various Port Statuses
  - *Error Disabled Port Status*
    - Indicates that a port on a switch has been automatically shut down due to a network error or policy violation
  - *Administratively Down Port Status*
    - Signifies that a network port has been intentionally disabled by network administrators, not due to an error

- *Suspended Port Status*
  - Indicates a violation of an established protocol or policy within the network
  - Remediation
    - Monitor network traffic to identify and address the root cause of interface issues
    - Address physical issues such as electrical interference, cable damage, or hardware faults
    - Resolve configuration issues, network card malfunctions, or collision domain size problems
  - Understanding and addressing these interface issues can significantly improve network performance and reliability

- **Power over Ethernet (PoE) Issues**
  - *Power over Ethernet (PoE)*
    - A technology that allows network cables to carry both electrical power and data over a single line
    - Useful for devices like IP cameras, VoIP phones, and WiFi access points, enabling them to receive power and data through the same cable
    - Types
      - Power over Ethernet (PoE)
        - Defined by IEEE 802.3af standard

- ○ Provides up to 15.4 Watts of DC power per device
- Power over Ethernet Plus (PoE+)
  - ○ Defined by IEEE 802.3at standard
  - ○ Provides up to 30 Watts of DC power per device
- ■ *Power Loss*
  - Occurs as power moves from the switch to the end device, resulting in a lower actual power available at the device
- ○ Issues
  - ■ *Power Budget Exceeded Error*
    - Occurs when the power demand from devices exceeds the switch's power supply capacity
    - *Power Budget*
      - ○ Sum of all of the DC power available to the endpoint devices, not just the amount of power available on a single switchport
    - Resolution
      - ○ Check and compare power requirements of devices with the total power budget available
      - ○ Consider removing non-essential devices or upgrading the PoE source

- ■ Incorrect Standard
    - ● Occurs when there is a mismatch between the PoE standard supported by the end device and the switch
    - ● Resolution
        - ○ Check and ensure compatibility between the end device and the switch
    - ● Resolution for Mismatch
        - ○ Replace the switch with one that supports the required standard
        - ○ Use PoE injectors that match the required standard to provide more power
            - ■ *PoE Injector*
                - ● Device that adds electrical power to a standard Ethernet data cable so that both power and data can be provided to PoE-capable endpoint device
- ■ Symptoms of Issues
    - ● Devices may randomly restart, behave erratically, or refuse to power on
- ○ Understand issues to identify and resolve PoE issues within the network effectively

Troubleshooting Wireless Issues

Objective 5.4: Given a scenario, troubleshoot common performance issues

- **Introduction**

  -
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 1900 Mbps	100-500 Mbps
802.11ax	10 Gbps	600-900 Mbps

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

- ○ *RSSI (Received Signal Strength Indicator)*
    - ■ Estimated measure of the power level that a radio frequency client device is receiving from a wireless access point or wireless router
        - ● Over -90 dB - Extremely weak
        - ● Around -65 dB - Fairly strong
        - ● -55 dB - Strong
        - ● -30 dB - Extremely strong
- ○ EIRP (Effective Isotropic Radiated Power)
    - ■ The maximum amount of power that could be radiated from an ideal isotropic antenna, given its antenna gain, and the transmitted power of the radio frequency system

- **Wireless Coverage Issues**
    - ○ *Coverage* (Wireless Networks)
        - ■ Measure of the area around a wireless transmitter with sufficient signal strength for device use
        - ■ Conducted via wireless site surveys to create a heat map showing signal strength levels (green to red)
    - ○ Signal Measurement
        - ■ Client Side
            - ● Received Signal Strength Indicator (RSSI) – decibels
        - ■ Access Point Side
            - ● Effective Isotropic Radiated Power (EIRP) – dBi

- ○ Common Coverage Issues

    - ■ Insufficient coverage in multi-story buildings

        - ● Signal degradation with distance and obstacles like ceilings

        - ● RSSI decreases when the signal has to penetrate through the floor

- ○ Improving Coverage

    - ■ Use signal boosters

    - ■ Antennas with higher dBi ratings

        - ● Two factors affecting single wireless access point

            - ○ Amount of power the transmitter is sending out

            - ○ Size of antenna

            - ○ Example

                - ■ Replacing a 5 dBi antenna with a 9 dBi antenna can double range under ideal conditions

    - ■ *Wireless Repeaters*

        - ● Layer one devices with two radios that receive and retransmit signals at full strength, extending coverage area

        - ● Useful in multi-story buildings, with repeaters placed strategically to boost signals from lower floors to upper floors

    - ■ Additional access points in Extended Service Set (ESS) configuration

        - ● *Extended Service Set (ESS)*

            - ○ Combining multiple access points into a single network with seamless roaming for devices

- ○ Example
    - ■ Using two access points on different floors of a house connected by Ethernet cables for complete coverage
- ■ *Wireless Mesh Systems*
    - ● Combination of repeaters and access points into a single device to create a mesh network
    - ● Ideal for larger homes and offices, eliminating the need for Ethernet cables to each device

- **Interference Issues**
    - ○ Interference in Wireless Networks
        - ■ *Interference*
            - ● Occurs when multiple wireless networks communicate on the same channel at the same frequency
        - ■ Overlapping channels (e.g., channel 4 and channel 6) can lead to interference and network slowdowns
        - ■ Conduct a site survey to identify channels and frequencies in use and plan access point locations accordingly
    - ○ Channel Planning in 2.4 GHz Networks
        - ■ <u>Use channels 1, 6, and 11 to avoid overlap</u>
        - ■ For extended service set networks

- Plan access point locations and channel assignments carefully to minimize interference
  - Maintain a 10-15% overlap between access points for sufficient coverage and seamless device handoff
  - Channel Planning in 5 GHz Networks
    - Utilize a honeycomb pattern for access point installation
    - Ensure no channel repetition until at least two zones away to minimize interference and ensure coverage
  - Attenuation in Wireless Networks
    - *Attenuation*
      - Reduction of signal strength between transmission and reception
      - Can occur within antenna cables or in the radio frequency wave as it travels
    - Causes of Attenuation
      - Distance
      - Physical obstacles (e.g., walls)
      - Signal interference
    - Reducing Attenuation
      - Use higher quality, lower resistant components for antennas and cables to reduce attenuation

- ■ Radio Frequency Wave Signal Attenuation

  - ● Multipath Reception

    - ○ Occurs when signals bounce off objects

    - ○ Can cause attenuation and weaker signals

    - ○ Signals may reach the receiver but with lower signal strength, leading to lower throughput

- ● **Client Disassociation Issues**

  - ○ Disassociation Issues in Wireless Networks

    - ■ Reasons for client disassociation

      - ● *Idle Timeout*

        - ○ Occurs after 300 seconds (5 minutes) of inactivity

          - ■ Default setting on most access points

        - ○ Some clients send keep-alive packets

      - ● *Session Timeout*

        - ○ Occurs after 1800 seconds (30 minutes)

        - ○ Client should re-authenticate and re-establish connection automatically

      - ● *Wireless Network Change*

        - ○ Disables and re-enables the network

        - ○ Requires devices to reconnect and re-authenticate

- *Manual Deletion*

    - Occurs when an administrator removes a client

- *Authentication Timeout*

    - Occur when authentication/key exchange process fails to finish in time

    - Client needs to restart authentication process

- *Access Point Radio Reset*

    - Occurs when a change is made to the wireless network

○ Deauthentication Attack

- Used by hackers to disassociate clients

- Attacker captures packets used in association/authentication processes to crack shared passphrase

- Continual deauthentication should be investigated for possible attacks.

○ Understanding these disassociation issues is crucial for network administrators to differentiate between normal disassociations and potential attacks, allowing for appropriate responses and network security

- **Incorrect Wireless Configurations**
    - ○ Incorrect Configurations in Wireless Networks
        - ■ Wrong SSID
            - ● *Service Set Identifiers (SSIDs)*
                - ○ Natural language names used to identify wireless networks in 802.11 protocol
                - ○ Examples
                    - ■ "Starbucks Wi-Fi"
            - ● Incorrect SSID not usually an issue due to dropdown menu selection
            - ● Manually entering SSID may lead to mistyping errors
            - ● *Evil Twin SSID*
                - ○ Similar SSID in the same area may indicate an evil twin
                - ○ Connecting to wrong SSID can lead to malware infection or on-path attack
        - ■ Incorrect Passphrase
            - ● *Passphrase/Pre-shared Key*
                - ○ Required for authentication to wireless networks
                - ○ Used to encrypt and decrypt data
            - ● Entering wrong passphrase leads to disassociation from access point

- Troubleshooting Incorrect Passphrase
    - Reinstall wireless network adapter drivers if passphrase is correct but access point reports it as incorrect
- Corruption in drivers may cause passphrase encryption issues
    - Encryption Protocol Mismatch
        - Encryption Protocols
            - WEP uses RC4
            - WPA uses TKIP
            - WPA2 uses AES
- Network Security Key Mismatch
    - May indicate wrong password or using wrong encryption protocol
    - Solutions
        - Manually change protocol
        - Disable antivirus tools
        - Reinstall wireless drivers
- Ensure correct SSID, passphrase, and encryption protocol
- If issues persist, investigate deeper OS or driver issues

- **Captive Portal Issues**
    - *Captive Portal*
        - Webpage displayed to newly connected users of a wireless network before they're granted broader access to network resources

- ■ Purpose
    - ● Authentication
    - ● Payment
    - ● Acceptance of agreements
    - ● Survey completion
    - ● Other information collection
- ○ Implementation
    - ■ *HTTP Redirect*
        - ● Redirects all traffic to a web server controlled by the network
        - ● Uses 302 HTTP status code
    - ■ *ICMP Redirect*
        - ● Sends error messages and operational information indicating the success or failure of communicating with another IP address
        - ● Uses ICMP packets to redirect
        - ● Less common
    - ■ *DNS Redirect*
        - ● Redirects to a captive portal page via DNS server
        - ● Most common type
- ○ Common Issues
    - ■ Smartphones and laptops may not automatically load the captive portal
        - ● Troubleshooting steps for smartphones and laptops
            - ○ Try opening a web browser

- If that fails, enter the default gateway IP address in the browser
- Verify DNS server settings and enable DHCP if necessary
- Captive portals are essential for controlling network access but can lead to issues if not properly configured

- **Wireless Considerations in Troubleshooting**
  - Antennas
    - Types
      - Omnidirectional
        - Radiates RF waves in all directions
        - Common in wireless APs
        - Located in vertical form factor
          - *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
        - Radiates RF waves in two directions
        - Less commonly used

https://www.DionTraining.com

- Yagi
    - Unidirectional
    - Used for longer-distance wireless links
- Parabolic Grid/Disk
    - Unidirectional
    - Used for site-to-site connections over longer distances

■ Placement

- Site-to-site
    - Unidirectional antennas mounted outside with clear line of sight
        - Parabolic
        - Yagi
- Indoor
    - Omnidirectional – placed on the ceiling
    - Unidirectional patch antennas – placed on an outer wall of the building, facing inward

■ *Polarization*

- The orientation of of the electric field, or transmissions that are occurring from the antenna
- Vertical polarization
    - Most Wi-Fi networks

- Horizontal polarization

- Wireless access point could use vertical or horizontal polarization

- Poor RSSI near the access points could indicate polarization issues

○ *Channel Utilization*

■ A statistic or measure of airtime utilization for a frequency or channel

■ Higher utilization indicates more traffic

- Aim for under 30% to have faster wireless network

■ Overlapping channels can lead to congestion and slower speeds

■ Devices use CSMA/CA to avoid collisions and Clear Channel Assessment (CCA) to assess channel availability

■ *Site Survey*

- Process of planning and designing wireless network to provide the required wireless solution

- Helps determine optimal channel selection and coverage areas to overcome the negative effect of having high channel utilization

○ Wireless Access Point Association Times

■ Seven-step process for client connection

- Wireless client sends a probe request

- Receiving access point checks to see if it can support the data rate requested

- Wireless client sends a low-level authentication frame

- Access point receives the authentication frame and responds with an acknowledgement
- Wireless client chooses the access point it wants to associate with and sends association request
- Access point processes the association request
- Client is fully connected and associated
- Association times can vary based on network load and signal strength
- Faster association in high signal strength areas
- Delay can be up to 30-60 seconds in busier networks

Troubleshooting Network Services

Objective 5.3: Given a scenario, troubleshoot common issues with network services

- **Duplicate Addresses**
    - Duplicate MAC Addresses at Layer 2
        - *MAC Address*
            - A 12-digit hexadecimal number used to uniquely identify a network interface card (NIC) on a network
            - 48 bits in total length
                - First 24 bits – assigned by the hardware manufacturer
                - Next 24 bits – used to uniquely identify the NIC
        - Duplicate MAC Addresses
            - Can cause network issues
                - Confusion in switch forwarding tables (CAM tables)
                - Connectivity problems
            - MAC Spoofing
                - Using a self-assigned address (locally administered address), can lead to duplicate MAC addresses
            - Virtual machines (VMs)
                - Can also create duplicate MAC addresses

- - ○ *Logical Domain Manager*
      - Used as preventive solution by monitoring and reassigning MAC addresses
  - Identifying Duplicate MAC Addresses
    - Network connectivity issues or intermittent connectivity for affected devices
    - Use of a protocol analyzer like Wireshark to analyze ARP traffic for duplicate MAC address mappings
  - Preventing and Resolving Duplicate MAC Addresses
    - Enable port security on devices to allow only one MAC address per switch port
    - Use the `show arp` command on switches to identify switch ports with duplicate MAC addresses
    - Check and correct hardware manufacturing issues or MAC spoofing
    - Replace the NIC if it is a hardware issue
  - ○ Duplicate IP Addresses at Layer 3
    - Duplicate IP Addresses
      - Also known as IP address conflict
      - Occur when two devices on the same network have the same IP
      - Causes
        - ○ Static IP assignments

- - - ○ DHCP server issues

  - ○ Rogue DHCP servers

  - Causes intermittent connectivity as routers may not know which device to send traffic to

  - ■ Identifying Duplicate IP Addresses

    - Check network adapter properties to see if the IP address is statically assigned or obtained dynamically

    - Use the `show arp` command on routers to identify duplicate IP addresses

  - ■ Preventing and Resolving Duplicate IP Addresses

    - Correct static IP address assignments or switch to dynamic IP assignment if necessary

    - Use DHCP server properly and check for rogue DHCP servers

    - Verify configurations on individual clients to ensure proper IP assignment

- **DHCP Issues**

  - ○ *Dynamic Host Configuration Protocol (DHCP)*

    - ■ A network management protocol used on IP networks to automatically assign IP addresses and other communication parameters to devices using a client-server architecture

- ○ *Rogue DHCP Server*

    - ■ A DHCP server on the network that is not under administrative control

    - ■ Risks

        - ● Can be installed maliciously to redirect traffic or accidentally by employees

            - ○ Causes IP conflicts and network connectivity issues

    - ■ Prevention

        - ● Configure DHCP snooping to exclude rogue DHCP server traffic

        - ● Use port security on switch ports

        - ● Configure an intrusion detection system

- ○ *DHCP Scope Exhaustion*

    - ■ Occurs when the DHCP server runs out of valid IPs to assign

    - ■ Causes

        - ● Too many devices requesting IPs simultaneously

        - ● Long lease times

    - ■ Solutions

        - ● Increase the DHCP scope size

        - ● Decrease lease times for transient users

        - ● Enable port security or Network Access Control (NAC) to limit the number of devices using DHCP

- **Routing Issues**
  - *Multicast Flooding*
    - *Multicast Networks*
      - Send group communications to multiple destination computers simultaneously
    - Occurs when no specific host is associated with the multicast MAC address in the switch's CAM table
    - Results in multicast traffic being flooded throughout the LAN or VLAN, wasting resources
    - Prevention
      - <u>Configure switches to block unknown multicast packets</u>
  - *Asymmetrical Routing*
    - Occurs when packets leave via one path and return via a different path
    - Can happen across different layer two bridge pair interfaces, routers, or firewalls in a high availability cluster
    - Problematic for security devices and network appliances performing deep packet inspection or using stateful firewalls
      - Does not cause any routing issues necessarily, but do cause issues with dropped packet flows
    - Solution
      - Adjust firewall placement and internal routing to ensure traffic flows through the same firewall in both directions

- ○ Put firewalls closer to the systems, instead of at the edge of the network
- ○ *Missing Routes*
  - ■ Occur when a router cannot reach a destination due to a missing route in the routing table
  - ■ Common with static routes if mistyped or not properly added
  - ■ Troubleshoot by checking the routing tables
    - ● show ip route – Cisco
    - ● route print – Windows
    - ● For dynamic routing protocols like OSPF or BGP
      - ○ Verify that the dynamic routing protocol is enabled
      - ○ Ensure routers can communicate

- ● **Switching and Routing Loops**
  - ○ *Switching Loops*
    - ■ Occur when there is more than one path between a source and destination device
    - ■ Can lead to broadcast storms due to repeated broadcast messages in a looped architecture
    - ■ Prevention
      - ● Enable Spanning Tree Protocol (STP) on switches
        - ○ show spanning tree – check STP configuration

- ○ *Routing Loops*
    - ■ Formed when there is an error in the routing algorithm, creating a circular route
    - ■ Caused by incorrect configurations of routing protocols
    - ■ Prevention
        - ● Routing Protocols
            - ○ Have methods in place to prevent physical loops that cause issues
        - ● *Split Horizon*
            - ○ Prevents a route from being advertised back in the direction it came from
            - ○ ip split-horizon – set up split horizon on Cisco router
        - ● *Route Poisoning*
            - ○ Increases the metric of a failed route to an infinitely high number
        - ● *Hold-down timers*
            - ○ Prevent bad routes from being restored and passed to other routers
            - ○ Hold-down period default – 180 seconds (3 minutes)
- ○ General Tips
    - ■ Use the right routing protocols and ensure proper configuration to avoid routing loops

- Be cautious when adding static routes, as they can lead to routing loops if not configured properly

- Static routes are highly trusted by routers

  - Default metric – 1

- **Firewall Issues**

  - *Firewalls*

    - Network security devices that monitor and filter incoming and outgoing network traffic based on established rule sets

    - Act as an inspection point and barrier between a private internal network and the public internet or other private internal networks

  - Types of Firewalls

    - *Host-based Firewall*

      - Software that runs on an individual computer or device, protecting that single device (e.g., Windows Defender firewall)

    - *Network-based Firewall*

      - A network security device deployed in line with network traffic flow, monitoring and filtering traffic (e.g., Cisco firewall)

  - Common Firewall Issues

    - 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

- ○ Troubleshooting Steps

    - ■ 7-step Troubleshooting Method

    - ■ Understand the OSI model to troubleshoot each layer from Layer 1 physical to identifying the issue

        - ● Verify physical connectivity (Layer 1) by checking cables and link lights

        - ● Check Layer 2 by ensuring communication using ARP and MAC addresses

        - ● Check Layer 3 for valid IP address, subnet mask, and default gateway

    - ■ Inspect firewall for misconfigured rule sets, such as ACLs

- ○ *Access Control Lists (ACLs)*

    - ■ Collection of permit and deny conditions providing security by blocking unauthorized users and allowing authorized users

        - ● show access-lists – command for Cisco devices

    - ■ Verify ACL rules for typos, correct protocol and port numbers, source and destination addresses, and rule order

        - ● Example ACL Troubleshooting

            - ○ Identify ACL rules causing connectivity issues (e.g., denying TCP traffic from any IP to any IP)

            - ○ Adjust ACL rule order to prioritize more specific rules (e.g., moving specific allow rules to the top of the list)

○ Software Firewall Considerations

■ Verify IP addresses, ports, applications, and services are correctly allowed or blocked

■ Double-check ACLs to ensure they're blocking, and allowing exactly what is intended and in the right order

● **IP Configuration Issues**

○ IP Settings

■ Incorrect IP settings can cause issues

■ Every network client needs four key pieces of information

● IP address

● Subnet mask

● Default gateway IP

● DNS server IP

○ Troubleshooting Steps

■ 1 – Identify the Issue

● Use ping to test connectivity (e.g., ping 8.8.8.8)

■ 2 – Analyze IP Settings

● Check IP address, subnet mask, and default gateway

○ Ensure they are correct and in the same subnet

- 3 – Resolve Issues
  - Wrong default gateway
    - Change it to the correct IP address in the same subnet
  - IP address in the wrong subnet
    - Change it to an IP address in the correct subnet
- DNS Configuration
  - Ensure DNS server IP addresses are correct
  - If no DNS servers are available
    - Use public DNS servers (e.g., google DNS of 8.8.8.8 and 8.8.4.4)

- **VLAN Issues**
  - VLAN Communication
    - Devices in different VLANs cannot communicate directly
    - Routing between VLANs is necessary for communication to occur
    - Devices within the same VLAN must belong to the same logical subnet
  - Improper VLAN Configuration
    - Can cause devices to be unable to communicate
    - Verify VLAN configuration and routing setup to resolve issues
  - Avoiding Default VLAN
    - Not using VLANs places all traffic in the default VLAN (VLAN 1)
      - Leads to a large broadcast domain

■ Segregate servers into their own VLAN to improve performance and reduce broadcast traffic

- **DNS and NTP Issues**
  - ○ DNS
    - ■ Matches domain names with corresponding IP addresses
    - ■ Symptom
      - ● Network clients unable to resolve domain names to IP addresses
    - ■ Determine if the issue is on a single client or network-wide
      - ● Single Client Issue
        - ○ Possible Cause
          - ■ TCP/IP settings on the client
        - ○ Resolution Steps
          - ■ Check assigned DNS server IP
          - ■ Verify connectivity to DNS server
      - ● Network-wide DNS Issue
        - ○ Possible Cause
          - ■ DNS server not responding
        - ○ Resolution Steps
          - ■ Flush DNS cache
          - ■ change to a different DNS server (e.g., Google's DNS servers at 8.8.8.8 and 8.8.4.4)

- DNS Server Troubleshooting

    - Issue

        - DNS server not properly responding

    - Resolution Steps

        - Verify A records and CNAME records

        - Ensure TTL is set correctly

- DNS Records Verification

    - A Records

        - Verify domain name and IP address are correct

    - CNAME Records

        - Verify source and destination domain names are spelled correctly

    - nslookup – command to use for verification

- DNS Time to Live (TTL)

    - Issue

        - TTL set too high causes old DNS records to remain cached

    - Recommended TTL

        - Keep TTL short (e.g., 300 seconds) for frequent network or website changes

- Reducing DNS Latency

    - Issue

        - High latency due to distant DNS servers

- ■ Resolution
  - ● Use DNS servers closer to users, such as those hosted within your network or by your ISP
- ○ Troubleshooting NTP Issues
  - ■ NTP Purpose
    - ● Synchronize system clocks for distributed applications
  - ■ Issue
    - ● NTP packets not received, processed, or contain errors
  - ■ Troubleshooting Network Communication Issues
    - ● Verify physical and network layer connections
      - ○ NTP on LAN
        - ■ Verify communication between the client and the server using their MAC addresses properly
      - ○ NTP outside LAN
        - ■ Verify communication between clients and servers using Layer 3 IP addresses
    - ● NTP packets not being received
      - ○ Indicates general communication issue at Layer 1, 2, and 3, or a DNS server issue (using domain name)
    - ● NTP received but not being processed
      - ○ Look at the network client or the NTP server to ensure they are operating the NTP service

- NTP process or service not acting on the NTP packets being received
  - Indicates network communication issues with other services, like HTTPS and network authentication processes
- Errors or packet loss in processed NTP packets
  - Can lead to time synchronization loss
    - High dispersion or delayed values
      - Indicate packets take too long to reach the client from the server, affecting time accuracy
  - Saturated links or buffering can delay NTP packets
  - Varying timestamps in NTP packets can disrupt synchronization
  - Resolution
    - Ensure network connections are not saturated and have adequate connectivity for timely NTP packet delivery

Troubleshooting Performance Issues

Objective 5.4: Given a scenario, troubleshoot common performance issues

- **Collisions and Broadcast Storms**
  - *Collisions*
    - Occur when two hosts on the network transmit at the same time, causing their signals to combine and become unreadable
    - Can occur in both wired and wireless networks
    - Prevention
      - Architecting networks with smaller collision domains
    - *Collision Domain*
      - A network segment where simultaneous data transmissions can collide
      - Use Layer 2 devices like switches to break collision domains into smaller ones
    - Detect collisions by monitoring network performance and using the "show interface" command on network device
      - *Deferred Counters*
        - Count the number of times the interface has tried to send a frame
        - Indicate carrier sensing

- - - ○ <u>Normal in hub-based networks but should not occur in switch-based networks</u>
  - ■ Types of Collisions
    - ● *Late Collisions*
      - ○ Detected after 5.12 microseconds
      - ○ Usual causes
        - ■ Incorrect cables
        - ■ Bad network interface cards
        - ■ Too many hubs
    - ● *Excess Collisions*
      - ○ Occur when a device exceeds the limit for retransmitting after a collision
      - ○ *show controller ethernet*
        - ■ Command that displays the exact number of excessive collisions
      - ○ Usual causes
        - ■ Devices using full duplex communication over a shared Ethernet segment
        - ■ Broken network interface card
        - ■ Too many clients connected to the same collision domain

- Solutions
  - Turn off autonegotiation for the speed and duplex of an interface
  - Hard code the speed to a lower setting
  - Change duplex to half duplex
- *Broadcast Storms*
  - Occur when a network is overwhelmed by continuous multicast or broadcast traffic
  - Can quickly overwhelm switches and devices, leading to decreased network performance or denial of service
  - <u>Addressed at both Layer 2 and Layer 3</u>
    - Layer 2 – FF:FF:FF:FF:FF:FF
    - Layer 3 – 255.255.255.255
  - *Broadcast Domain*
    - A logical division of a computer network where all nodes can reach each other by broadcast at the data link layer
    - Can be within the same LAN segment, or can be bridged to other LAN segments
  - Main Causes
    - Too large singular broadcast domain
    - Large volume of DHCP requests
    - Loops are created in the switching environment

- <u>Prevention</u>
  - <u>Break up large broadcast domains</u>
    - <u>Use Layer 3 devices</u>
  - <u>Limit MAC addresses per port</u>
  - <u>Set up loop prevention mechanisms like Bridge Protocol Data Units (BPDUs)</u>
- Identifying Broadcast Storms
  - Look for rapid increases in packet counters beyond normal baselines
- Monitor network monitoring tools for increased packet loss
  - Use packet analyzers like Wireshark or TCPdump to identify rapid broadcast packets
- Monitor network performance and use preventive measures to avoid excessive collisions and broadcast storms

- **VoIP Issues**
  - *Voice Over Internet Protocol (VoIP)*
    - Set of protocols for sending streaming voice and video in real-time over the internet
    - <u>Importance of low latency and high quality of service (QoS)</u> for good voice and video connections
    - Used for making phone calls over the internet

- *Latency*
    - Time it takes for a signal to reach the intended client
    - Measured in milliseconds (ms)
        - For VoIP connections – under 50 to 100ms
    - Impact on VoIP
        - Latency over 100-200ms can cause noticeable audio issues, such as echoes
    - Example
        - Satellite internet connections typically add 150-250ms due to the distance the signal travels
- *Jitter*
    - Variation in delay over time
    - Measured by sampling the elapsed time between packet arrivals
    - Impact on VoIP
        - Can cause robotic or static-like sound in conversations
    - Causes
        - High latency environments or packets taking different routes and being reassembled in the incorrect order
            - Jitter starts when latency increases by up to 30-50ms
- *Quality of Service (QoS)*
    - Mechanism to prioritize certain traffic over others

- ■ Implementation
    - ● Configure network devices to prioritize VoIP traffic
        - ○ Reduces latency and jitter
- ■ Limitation
    - ● Only affects traffic inside your network
    - ● Internet service providers (ISPs) may not prioritize VoIP traffic over the internet
- ○ Conclusion
    - ■ The two main issues with VoIP are high latency and jitter
    - ■ Solutions
        - ● Increase network performance
        - ● Implement QoS to prioritize VoIP traffic within your network, ensuring a higher quality of service for end users

- ● **Packet Loss**
    - ○ *Packet Loss*
        - ■ Occurs when data packets fail to reach their intended destination
        - ■ Leads to issues like slow internet speeds, lags in video or audio streaming, and disruptions to communication
    - ○ Symptoms of Packet Loss
        - ■ Unexplained network slowdowns
        - ■ Jitter during voice calls

- Abrupt disconnections in streaming media playback
  - Causes of Packet Loss
    - *Network Congestion*
      - Too much data exceeding the network's handling capacity, causing slowdowns or complete stops in traffic flow
    - *Faulty Router Configurations*
      - Routers set up incorrectly, leading to misdirected or improperly prioritized data
    - *Bad Cables*
      - Physically damaged or deteriorating wires disrupting network data transmissions
    - *Hardware Failures*
      - Malfunctioning network devices like switches, routers, or modems
  - Troubleshooting Packet Loss
    - Use command line tools like ping and traceroute to identify the source of packet loss
      - *Ping*
        - Helps determine the reachability of a specific device on the network
      - *Traceroute*
        - Used to map the path that data will take to reach its intended destination

- Utilize network monitoring tools for more comprehensive insights into traffic patterns
  - Strategies to Mitigate Packet Loss
    - Network congestion issues
      - Increase bandwidth
      - Optimize network layout
      - Employ Quality of Service (QoS)
    - Hardware issues
      - Routine inspection
      - Replace faulty cables
      - Firmware updates
    - Configuration errors
      - Verify configuration settings across all network devices
    - Proactive Measures
      - Implement regular network performance monitoring
      - Maintain a well-documented network configuration policy to prevent misconfigurations

- **Network Performance Issues**
  - Most Common Causes Of Network Performance Issues
    - High CPU Usage
      - Network devices are essentially computers with CPUs

- Increases latency, jitter, and packet loss

- Can slow down devices and the network

- Solutions

    ○ Upgrade to more powerful devices

    ○ Simplify processing load

■ High Bandwidth Usage

- Causes delays and packet drops

- Solutions

    ○ Increase bandwidth

    ○ Analyze traffic to optimize usage (netflow analysis)

■ Poor Physical Connectivity

- Solutions

    ○ Check and test cables for damage

    ○ Test connections from demarcation point to isolate issues

        ■ Cable tester for twisted pair connections

        ■ Fiber light meter for fiber optic connections

■ Malfunctioning Network

- Misconfigurations or hardware failures can affect performance

- Solution

    ○ Use troubleshooting methods to identify and resolve

    issues

- ■ DNS Problems
  - ● High DNS latency can slow down user experience
  - ● Solution
    - ○ Ensure DNS servers are functioning properly

- ● **Other Performance Issues**
  - ○ Low Optical Link Budget
    - ■ *Optical Link Budget*
      - ● A calculation of anticipated losses along the length fiber optic connection
    - ■ Factors
      - ● Distance
      - ● Multiplexing
      - ● Bends
      - ● Imperfect connections
      - ● Patches
      - ● Splices
    - ■ Effects
      - ● Reduced transmission efficiency
      - ● Slower speeds
      - ● Downtime

- ■ Measurement
    - ● Use an Optical Time Domain Reflectometer (OTDR) to measure losses in decibels (dB) per kilometer
    - ● Normal – 0.25 dB per kilometer
    - ● Higher rates – indicate low optical link budget
- ■ Calculation
    - ● Total optical link budget = Power budget minus Losses
- ○ Certificate Issues
    - ■ *Digital Certificates*
        - ● Used as a credential for verifying identities in transactions
    - ■ Common Issues
        - ● Not signed by a trusted authority, expired, or missing
    - ■ Resolution
        - ● Purchase from a trusted authority, renew, or install properly
- ○ License Feature Issues
    - ■ *License Feature Errors*
        - ● May occur due to wrong license for needed features
    - ■ Resolutions
        - ● Determine the license
        - ● Compare loaded license with required features
        - ● Contact manufacturer if necessary

- ○ BYOD Challenges

  - ■ *Bring Your Own Device (BYOD)*

    - ● Policy allowing employees to use personal devices

  - ■ Support Challenges

    - ● Need to support various device types and software configurations

  - ■ Security Concerns

    - ● Ensuring secure access and network segregation for BYOD devices

- ○ Hardware Failures

  - ■ *Identifying Failures*

    - ● Pinpointing failed device and component

  - ■ Resolution

    - ● Replace failed components or devices

    - ● Ensure backups and spare parts availability

Conclusion

- **Conclusion**
    - Review of Five CompTIA Network+ Domains
        - Networking Concepts (23% of exam questions)
            - Network topologies
            - Protocols
            - Networking components
        - Network Implementation (20% of exam questions)
            - Routing technologies (static and dynamic routing)
            - Switching technologies (VLANs and STP)
            - Wireless technologies (channel selection, encryption, and authentication methods)
            - Physical aspects of network installations (equipment placement and environmental considerations)
        - Network Operations (19% of exam questions)
            - Organizational documentation
            - Lifecycle management
            - Network monitoring methods (SNMP and SEEMS)
            - Disaster recovery concepts and metrics
            - Implementation of network services across IPv4 and IPv6

- Management and comparison of network access and performance
    - Network Security (14% of exam questions)
        - Encryption
        - IAM (Identity and Access Management)
        - Common security terminologies
        - Physical and logical security measures
        - Network segmentation
        - Enforcement of security policies
    - Network Troubleshooting (24% of exam questions)
        - Troubleshooting methodology
        - Common cabling and interface issues
        - Addressing service-related problems
        - Performance issues (bandwidth, latency, packet loss)
        - Tools and protocols for diagnosing and resolving network issues
  - Scheduling the Exam
    - Exam can be taken at any Pearson VUE testing center worldwide or online using the Pearson VUE OnVUE testing system
    - Purchase an exam voucher from Pearson VUE or the CompTIA web store
        - Save 10% by purchasing the voucher from diontraining.com/vouchers
    - Schedule the exam day, time, and location on Pearson VUE's website
    - Arrive early at the testing center to relax before the exam starts

- ○ <u>Exam Tips</u>
    - Use a cheat sheet (whiteboard or digital whiteboard) to brain dump important information at the beginning of the exam
    - Skip the simulations at the beginning of the exam and do them after completing the multiple-choice questions
    - Take a guess if you're unsure of the answer, as there is no penalty for guessing
    - Pick the best time of day to take your exam based on your performance peak
    - Be confident in your preparation and take practice exams to build confidence and understanding
- ○ Post-Exam
    - Share your success story on social media and in online communities
    - Continue climbing the CompTIA certification ladder into Security+, CySA+, and PenTest+