CCNP Study Guide

Alexander

August 27, 2024

1.0 Architecture

1.1 Explain the different design principles used in an enterprise network

- 1.1.a High-level enterprise network design such as 2-tier, 3-tier, fabric, and cloud
- 1.1.b High availability techniques such as redundancy, FHRP, and SSO

In designing an enterprise network, it's essential to adopt a strategic approach that balances simplicity, scalability, and reliability. A 2-tier network design, typically suited for smaller networks, consists of an access layer that directly connects end-user devices and a core layer that handles high-speed, high-capacity routing between devices. While this design simplifies management and reduces costs, it may lack the scalability needed for larger environments. In contrast, a 3-tier network design is more robust and scalable, featuring an access layer for user connectivity, a distribution layer that manages routing and policy enforcement, and a core layer that serves as the high-speed backbone. This design supports extensive growth and complex routing needs, making it ideal for larger enterprises. For modern, high-performance environments, fabric network design, often implemented with a spine-leaf architecture, provides low-latency, high-bandwidth connectivity by interconnecting leaf switches to high-capacity spine switches. This design is particularly effective in data centers and large-scale networks due to its flexibility and ease of scalability. Additionally, as organizations increasingly migrate to cloud environments, cloud network design integrates network resources within public, private, or hybrid clouds, offering on-demand scalability and cost efficiency, which is crucial for dynamic and scalable applications.

To ensure continuous network operation and minimize disruptions, implementing high availability techniques is crucial. Redundancy is a fundamental approach, involving the duplication of critical components such as hardware devices and network links to prevent service interruptions in the event of failures. Complementing this are First Hop Redundancy Protocols (FHRPs) like Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP). These protocols enhance network reliability by providing failover mechanisms for default gateways, ensuring that network traffic can seamlessly reroute if a primary device fails. For example, HSRP and VRRP manage virtual IP addresses to present a unified gateway to the network, while GLBP not only provides redundancy but also distributes traffic among multiple routers to optimize load balancing. Additionally, Single Sign-On (SSO) simplifies user access by allowing authentication across multiple applications with a single set of credentials, enhancing user convenience and security. Integrating these design principles and high availability techniques ensures that enterprise networks remain robust, scalable, and resilient, adapting effectively to

organizational needs and technological advancements.

1.2 Describe wireless network design principles

- 1.2.a Wireless deployment models (centralized, distributed, controller-less, controller-based, cloud, remote branch)
- 1.2.b Location services in a WLAN design
- 1.2.c Client density

Wireless network design principles are critical for creating efficient and reliable wireless networks that meet the needs of users and applications. Key considerations include deployment models, location services, and client density.Wireless deployment models define how wireless access points (APs) and network controllers are organized and managed. In a centralized model, all wireless access points connect to a central controller. This controller manages the configuration, monitoring, and troubleshooting of all APs. This model simplifies management and provides consistent policy enforcement but may require high-capacity controllers and network infrastructure to handle the load. The distributed deployment model features access points that operate independently without a central controller. Each AP handles its own configuration and management, which can be beneficial in smaller or less complex environments. However, this approach can be more challenging to manage at scale and may lack unified policy enforcement. In the controller-less deployment model, APs are self-configuring and do not rely on a central controller. The configuration and management are done locally on each AP or through a minimal management interface. This model is often used in smaller networks or temporary setups where simplicity and cost are priorities. In the controller-based deployment model APs connect to a centralized controller for configuration and management, similar to the centralized deployment but with additional emphasis on the controller's role. This approach allows for centralized control over wireless policies, seamless roaming, and unified monitoring, making it suitable for larger and more complex environments. In cloud-based deployment, wireless APs are managed through a cloud service. This model offers scalability and flexibility, as the management and monitoring functions are offloaded to the cloud. It is ideal for organizations that need a global view of their wireless network or have multiple locations. A remote branch deployment model is designed for networks with multiple branch locations. It often combines elements of centralized and distributed models, using a central controller or cloud service for overall management while allowing branch APs to operate independently or in a localized manner. This approach balances centralized control with local autonomy.

Location services are integral to WLAN design, providing the ability to determine the physical location of devices within the wireless network. Basic location tracking uses signal strength and triangulation methods to approximate the location of a device. It provides general location information and is often used for asset tracking or to improve network performance. Advanced location services employtechnologies like real-time location systems (RTLS) and location-aware applications. These services can offer precise location tracking, which is valuable for applications such as indoor navigation, location-based services, and enhanced security. Heat maps and coverage analysis involves analyzing signal coverage and client density to ensure optimal placement of access points. Heat maps help visualize signal strength and coverage areas, allowing for adjustments to reduce dead zones and improve overall network performance. Location services can be integrated with business applications for functions like customer analytics, wayfinding, and operational efficiency. For instance, tracking customer movement patterns in retail environments can help optimize store layouts and enhance the shopping experience.

Client density refers to the number of wireless devices connected to an access point or within a given area. Properly addressing client density is crucial for network performance and user experience. Environments with high client density, such as auditoriums, conference halls, or large open-plan offices, require careful planning to ensure adequate coverage and performance. Strategies include deploying additional access points to distribute the load, optimizing channel usage to minimize interference, and implementing Quality of Service (QoS) to prioritize critical applications. In environments with lower client density, such as small offices or remote branches, fewer access points may be needed. However, considerations for future scalability and potential changes in client density should still be made to ensure the network can adapt as needed. Load balancing ensures that access points can handle the number of connected devices without degrading performance. This might involve configuring APs to manage load dynamically and deploying solutions like band steering to distribute clients across available frequency bands. Effective roaming and handoff mechanisms are crucial for maintaining a seamless user experience as clients move between access points.

Proper network design includes configuring APs to support fast and efficient handoff processes, reducing connection interruptions and maintaining network performance. By carefully considering these deployment models, location services, and client density factors, you can design a wireless network that is scalable, efficient, and capable of meeting the diverse needs of users and applications.

1.3 Explain the working principles of the Cisco SD-WAN solution

- 1.3.a SD-WAN control and data planes elements
- 1.3.b Benefits and limitations of SD-WAN solutions

Cisco SD-WAN is a software-defined approach to managing wide-area networks (WANs) that offers improved agility, security, and cost efficiency. It provides a centralized way to control network traffic and optimize connectivity across different sites, including branch offices, data centers, and cloud environments. The control plane of an SD-WAN solution is responsible for managing and directing traffic policies and network configurations. In Cisco SD-WAN, the control plane is handled by the Cisco vManage network management platform, which provides a centralized interface for network administrators to: define and apply policies related to application performance, security, and routing, configure and manage the network devices, such as vEdge routers and cloud gateways, and monitor network performance, collect and analyze metrics, and generate reports. The vManage platform interacts with the vSmart Controllers to distribute these policies and configurations to the various SD-WAN edge devices (vEdge routers) deployed across the network. The data plane in Cisco SD-WAN handles the actual transmission of data packets between endpoints. It operates independently of the control plane and is responsible for: directing data packets based on the policies set by the control plane, utilizing multiple WAN connections (MPLS, broadband, LTE) to ensure efficient and reliable delivery of data, securing data in transit using IPsec encryption, ensuring data confidentiality and integrity across the WAN. In Cisco SD-WAN, the data plane is managed by vEdge routers (or Cisco's Catalyst 8000 series) that sit at the network's edge and interface with various types of WAN links to provide connectivity and optimize traffic flow.

SD-WAN solutions can reduce costs by enabling the use of lower-cost broadband and LTE connections in addition to or instead of traditional MPLS connections. This flexibility helps optimize network expenses. Cisco SD-WAN allows for rapid deployment and configuration of WAN services. Network changes and policy updates can be implemented quickly and centrally managed via the vManage platform. By leveraging techniques like application-aware routing and dynamic path selection, SD-WAN optimizes application performance. It can steer traffic based on real-time network conditions and application requirements. Cisco SD-WAN provides a centralized management interface through vManage, which simplifies network configuration, monitoring, and troubleshooting. This reduces the complexity associated with managing multiple network devices and services. SD-WAN solutions include built-in security features, such as IPsec encryption for data in transit, integrated firewall capabilities, and secure direct cloud access. This helps protect data and applications from potential threats. By optimizing traffic routing and reducing latency, SD-WAN enhances the performance of cloud applications and services, leading to a better user experience. While SD-WAN offers numerous benefits, the initial deployment and integration with existing network infrastructure can be complex. Organizations may need to adapt their network architecture and processes. Although SD-WAN can reduce WAN costs, there can be additional expenses related to hardware, licensing, and cloud services that may offset some savings. For organizations relying on broadband and LTE connections, network performance and reliability are dependent on the quality of internet service providers (ISPs). This can be a limitation in regions with unreliable internet access. Depending on the SD-WAN solution provider, there may be concerns about vendor lock-in, where migrating to another SD-WAN solution could be challenging and costly. While SD-WAN can optimize network performance, the effectiveness can vary based on the quality and performance of the underlying WAN connections and the complexity of the network environment. By leveraging Cisco SD-WAN's control and data plane elements, organizations can benefit from enhanced network performance, cost savings, and improved agility. However, it is essential to consider potential limitations and ensure that the deployment aligns with the organization's specific needs and infrastructure.

1.4 Explain the working principles of the Cisco SD-Access solution

- 1.4.a SD-Access control and data planes elements
- 1.4.b Traditional campus interoperating with SD-Access

Cisco SD-Access (Software-Defined Access) is Cisco's solution for implementing a software-defined approach to campus networking. It simplifies network management, enhances security, and provides a more agile and scalable campus network infrastructure. SD-Access leverages Cisco's DNA (Digital Network Architecture) to deliver automated policy enforcement, segmentation, and network assurance. The Cisco DNA (Digital Network Architecture) Controller provides centralized management and automation of the network. It includes several elements: Cisco DNA Center, Cisco Identity Services Engine (ISE), Policy Management, and Automation and Orchestration. Cisco DNA Center acts as the central management platform for SD-Access, allowing network administrators to design, provision, and manage the network through a single interface. DNA Center facilitates policy creation, network segmentation, and monitoring. Cisco ISE works in conjunction with DNA Center to provide identity-based policy enforcement and network access control. ISE helps in user and device authentication, authorization, and accounting. DNA Center enables the creation and enforcement of policies across the network. It allows administrators to define policies based on user roles, devices, and applications, which are then applied consistently across the network. The control plane automates network provisioning, configuration, and updates. It simplifies tasks such as software updates, device configuration, and policy application. The data plane in SD-Access handles the actual transmission of data packets through the network, following the policies and configurations set by the control plane. Key components include: the network devices, overlay/underlay networks, and segmentation. In SD-Access, the data plane consists of network devices such as switches and access points that forward data based on the policies applied by the control plane. These devices are typically Cisco Catalyst 9000 series switches, which support SD-Access features like segmentation and automation. The overlay is created using technologies such as VXLAN (Virtual Extensible LAN) to segment network traffic. It allows for flexible and scalable network segmentation and isolation, enabling features like Virtual Networks (VN) for different applications or user groups. The underlay network is the physical network infrastructure that provides the connectivity between SD-Access devices. It supports the transport of overlay traffic and ensures connectivity between network nodes. SD-Access leverages network segmentation to isolate different types of traffic and enhance security. This is achieved through the use of VXLAN for overlay segmentation and VRF (Virtual Routing and Forwarding) for network isolation.

Integrating a traditional campus network with Cisco SD-Access involves several considerations and steps to ensure interoperability: network segmentation, device compatibility, policy enforcement, network management, migration strategy, integration points. Traditional networks often lack the granular segmentation capabilities provided by SD-Access. To integrate, organizations can create a hybrid environment where SD-Access segments interact with legacy VLANs and networks. This may require configuring VLAN-to-VXLAN mappings and ensuring compatibility between different segmentation schemes. Legacy network devices that do not support SD-Access features may need to be updated or replaced. Cisco SD-Access typically relies on Cisco Catalyst 9000 series switches, so integrating older devices may involve using network gateways or adaptors to bridge the gap between old and new technologies. Traditional networks may use different methods for policy enforcement compared to SD-Access's centralized approach. To ensure seamless operation, policies must be harmonized across the network. This can involve translating traditional access control lists (ACLs) and policies into the SD-Access framework. The transition to SD-Access introduces new management tools and processes. Traditional network management practices may need to be adapted to work with Cisco DNA Center and other SD-Access components. This can involve training staff and updating network management procedures. For a smooth transition, organizations often adopt a phased migration strategy. This involves gradually introducing SD-Access components and features while maintaining compatibility with existing infrastructure. The goal is to minimize disruption and ensure that both legacy and new systems operate effectively during the transition period. Key integration points include ensuring that SD-Access can communicate with existing network management systems and infrastructure components. This might involve setting up interfaces or APIs to allow data exchange between the SD-Access environment and traditional systems. By leveraging Cisco SD-Access, organizations can achieve greater network agility, enhanced security, and simplified management. However, successfully integrating SD-Access with traditional campus networks requires careful planning and consideration of how legacy systems will interact with the new SD-Access infrastructure.

1.5 Interpret wired and wireless QoS configurations

- 1.5.a QoS components
- 1.5.b QoS policy

Quality of Service (QoS) is a crucial aspect of networking, ensuring that various types of network traffic are handled appropriately to meet the performance requirements of different applications. QoS configurations are essential for both wired and wireless networks, although the specific implementations may differ. Classification is identifying and categorizing packets based on attributes such as source/destination IP address, MAC address, or type of service. This is often done using Access Control Lists (ACLs) or other matching criteria. Marking assigns a priority to packets. For example, marking packets with Differentiated Services Code Point (DSCP) or IP Precedence values to indicate their priority in the network. This marking is crucial for downstream QoS processing. Queuing mechanisms are used to manage how packets are handled when there's congestion. FIFO has packets processed in the order they arrive. Priority Queueing (PQ) will have packets placed into different priority queues and are processed according to their priority. Weighted Fair Queueing (WFQ) has packets divided amoung queues with weights, ensuring fair bandwidth distribution based on weights. Class-Based Weighted Fair Queuing (CBWFQ) is an extension of WFQ that allows for more granular control by assigning different weights to different classes of traffic. Policing enforces traffic limits by dropping or remarking packets that exceed specified rates. This helps in controlling the rate of traffic entering the network. Shaping temporarily buffers excess traffic to smooth out bursts and ensure that traffic conforms to a defined rate. It helps in managing traffic flow and preventing congestion. Techniques like Random Early Detection (RED) or Weighted Random Early Detection (WRED) are used to manage congestion by selectively dropping packets before the queue becomes full. Strategies to prevent congestion from occurring, such as Traffic Policing and Traffic Shaping. A link efficiency mechanisms example would be header compression to reduce the size of packet headers, which is particularly useful for wireless networks.

QoS policies are the configurations that define how QoS is implemented on a network device. They encompass various components and settings to ensure traffic is prioritized and managed according to the defined rules. A policy map defines the QoS policy and associates specific actions to different classes of traffic. Actions can include queuing, marking, or policing. A class map defines traffic classes based on certain criteria. For example, a class map might define a class for voice traffic, another for video, and another for data. Service policies are applied to interfaces to enforce the QoS policy. This is where the policy map is associated with a specific interface or direction (ingress or egress).

Class Maps:

```
class-map match-any VOICE
    match ip dscp ef
class-map match-any VIDEO
    match ip dscp af41
```

Policy Maps:

```
policy-map QoS-Policy
    class VOICE
        priority 1000
    class VIDEO
        bandwidth 500
    class class-default
        fair-queue
```

Applying Policy Maps:

```
interface GigabitEthernet0/1
    service-policy output QoS-Policy
```

For wired networks, QoS policies are typically implemented on switches and routers, where various queuing and marking mechanisms can be applied. Wired networks generally have more predictable performance and can support more sophisticated QoS configurations.

For wireless networks, QoS is crucial due to the shared medium and potential for interference. Configurations may include specific QoS settings for different wireless clients and access points. Techniques like Wi-Fi Multimedia (WMM) are used to prioritize different types of traffic, such as voice and video, on wireless networks.

1.6 Describe hardware and software switching mechanisms such as CEF, CAM, TCAM, FIB, RIB, and adjacency tables

In networking, particularly in Cisco environments, switching mechanisms and tables play crucial roles in how packets are processed and forwarded. Cisco Express Forwarding (CEF) is a high-performance, hardware-based switching method used by Cisco devices. It is designed to improve the efficiency and speed of packet forwarding by using two main tables: Forwarding Information Base (FIB) and adjacency tables. FIB contains the actual forwarding information used to make packet forwarding decisions. It maps IP prefixes to outgoing interfaces, enabling quick lookups and efficient packet forwarding. Adjacency tables maintain the MAC addresses of next-hop routers. It is used to map the next-hop IP address (as determined from the FIB) to the corresponding MAC address for the actual packet transmission. CEF operates by pre-computing the best path for each destination based on the routing table, and then using this information to forward packets efficiently without needing to perform a full route lookup for each packet. Content ADdressable Memory (CAM) is a specialized memory used in switches to perform rapid lookups of MAC addresses. CAM is used for MAC address tables (forwarding tables). These tables store MAC addresses associated with specific switch ports. When a frame arrives at the switch, CAM is used to quickly determine the port associated with the destination MAC address and forward the frame accordingly. CAM allows for very fast lookups because it can match an entire address in parallel rather than sequentially. Ternary Content Addressable Memory (TCAM) extends the capabilities of CAM by allowing for more complex lookups and multiple fields in a single operation. TCAM is used for: ACLs, and routing table lookups. TCAM helps in implementing ACLs by performing lookups based on multiple criteria (source IP, destination IP, etc.) and allowing for flexible matching (e.g., wildcard matches). TCAM is used in high-performance routers to quickly perform lookups in large routing tables, especially when dealing with large-scale networks. TCAM provides more flexibility than CAM because it can handle wildcard bits and multiple conditions, but it is generally more expensive and power-consuming. Forwarding Information Base (FIB) is a table used in conjunction with CEF to store the forwarding information. It contains IP prefixes (mapped to specific outgoing interfaces), and next-hop information (used to quickly forward packets based on their destination IP address). The FIB is built from the routing table and optimized for fast lookups, which helps in quick packet forwarding. Routing Information Base (RIB) is a table that stores all the routing information learned from various routing protocols. It includes: routing entries (metrics, next-hop addresses, associated interfaces), and routing protocol data (details from OSPF, EIGRP, or BGP). RIB is used to make routing decisions and build the FIB. The data in RIB is processed to create the optimized forwarding paths found in the FIB. Adjacency tables are used to map IP addresses to MAC addresses for the purpose of forwarding packets. For example, next-hop MAC addresses are stored in the adjacency table for quick retrieval during packet forwarding. Another example would be ARP tables. In routers, ARP tables map IP addresses to MAC addresses for devices on the same local network. This information is critical for correctly addressing packets when they are sent to the next-hop router or destination device.

2.0 Virtualization

2.1 Describe device virtualization technologies

- 2.1.a Hypervisor type 1 and 2
- 2.1.b Virtual machine
- 2.1.c Virtual switching

2.2 Configure and verify data path virtualization technologies

- 2.2.a VRF
- 2.2.b GRE and IPsec tunneling

2.3 Describe network virtualization concepts

- 2.3.a LISP
- 2.3.b VXLAN

3.0 Infrastructure

3.1 Layer 2

- 3.1.a Troubleshoot static and dynamic 802.1q trunking protocols
- 3.1.b Troubleshoot static and dynamic EtherChannels
- 3.1.c Configure and verify common Spanning Tree Protocols (RSTP, MST) and Spanning Tree enhancements such as root guard and BPDU guard

3.2 Layer 3

- 3.2.a Compare routing concepts of EIGRP and OSPF (advanced distance vector vs. link state, load balancing, path selection, path operations, metrics, and area types)
- 3.2.b Configure simple OSPFv2/v3 environments, including multiple normal areas, summarization, and filtering (neighbor adjacency, point-to-point, and broadcast network types, and passive-interface)
- 3.2.c Configure and verify eBGP between directly connected neighbors (best path selection algorithm and neighbor relationships)
- 3.2.d Describe policy-based routing

3.3 Wireless

- 3.3.a Describe Layer 1 concepts, such as RF power, RSSI, SNR, interference, noise, bands, channels, and wireless client devices capabilities
- 3.3.b Describe AP modes and antenna types
- 3.3.c Describe access point discovery and join process (discovery algorithms, WLC selection process)
- 3.3.d Describe the main principles and use cases for Layer 2 and Layer 3 roaming
- 3.3.e Troubleshoot WLAN configuration and wireless client connectivity issues using GUI only
- 3.3.f Describe wireless segmentation with groups, profiles, and tags

3.4 IP Services

- 3.4.a Interpret network time protocol configurations such as NTP and PTP
- 3.4.b Configure NAT/PAT
- 3.4.c Configure first hop redundancy protocols, such as HSRP, VRRP
- 3.4.d Describe multicast protocols, such as RPF check, PIM and IGMP v2/v3