# CMN_Summative_Assessment_2223_Updated21Feb

Words count 2,478.

## Task 1: Network Design and IP Addressing Scheme

Based on the requirements outlined in the scenario, a suitable network model and IP addressing scheme can be designed. The network design model chosen for this scenario is a hierarchical model consisting of three layers: the core, distribution, and access layers.

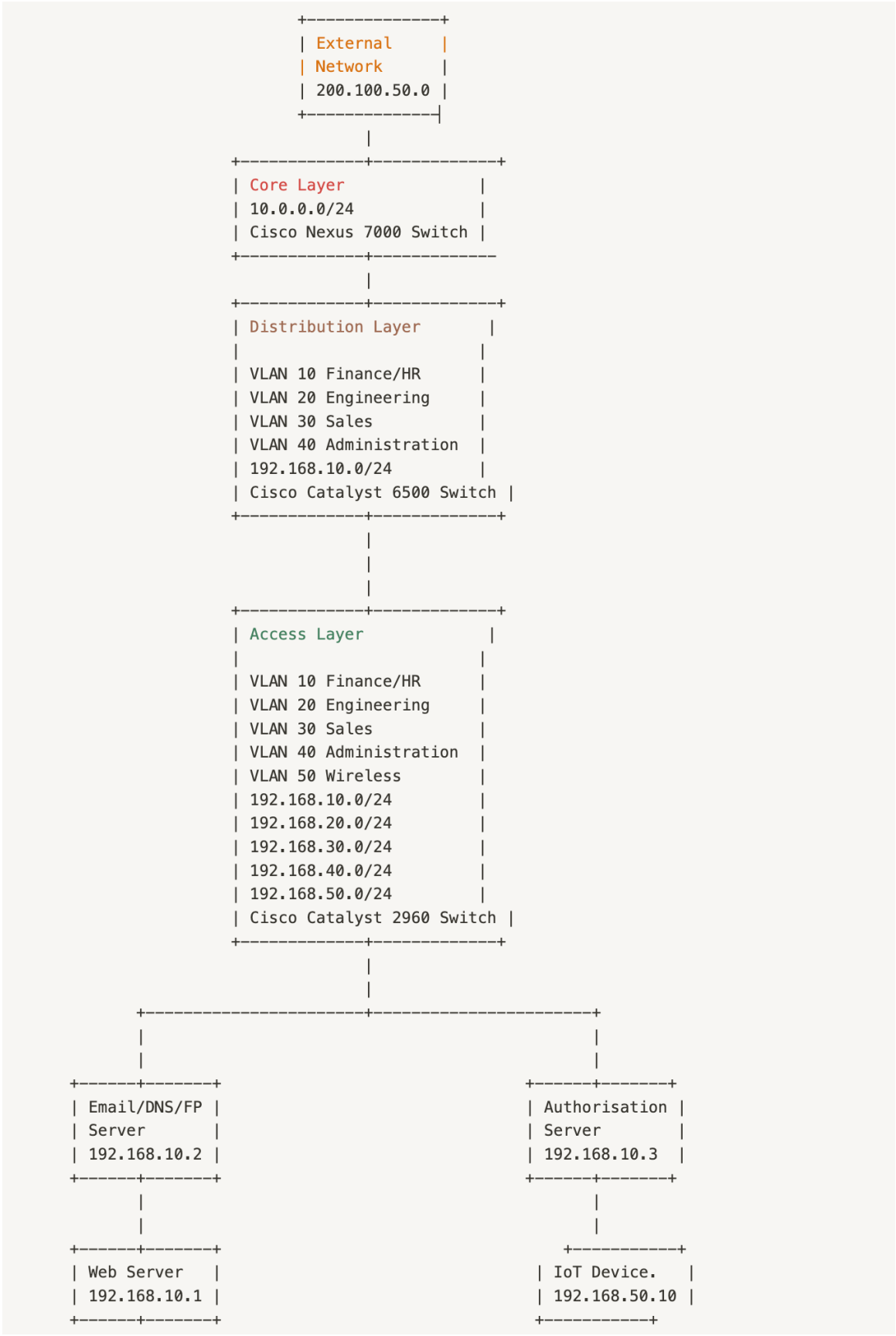
The core layer is responsible for high-speed data transfer between departments and external networks. The distribution layer connects the access layer to the core layer and provides routing, filtering, and policy enforcement services. The access layer provides end-user access to the network. It is responsible for connecting users to the distribution layer, allowing end users to access the web, connect user devices, and implement security policies.

To ensure each department's network is separated from other departments, a Virtual LAN (VLAN) should be configured for each department. Each VLAN should be assigned a unique subnet and IP address range. This will ensure that devices on one VLAN cannot communicate with devices on another VLAN. The IP addressing scheme for this scenario is Class C addressing, which provides 254 usable IP addresses per subnet.[1]

The network components used for this scenario are as follows:

1. Core Layer:
    - Cisco Nexus 7000 Switch
2. Distribution Layer:
    - Cisco Catalyst 6500 Switch
3. Access Layer:
    - Cisco Catalyst 2960 Switch

The network diagram for this scenario is shown below:


External
Network
200.100.50.0
Core Layer
10.0.0.0/24
Cisco Nexus 7000 Switch
Distribution Layer
VLAN 10 Finance/HR
VLAN 20 Engineering
VLAN 30 Sales
VLAN 40 Administration
192.168.10.0/24
Cisco Catalyst 6500 Switch
Access Layer
VLAN 10 Finance/HR
VLAN 20 Engineering
VLAN 30 Sales
VLAN 40 Administration
VLAN 50 Wireless
192.168.10.0/24
192.168.20.0/24
192.168.30.0/24
192.168.40.0/24
192.168.50.0/24
Cisco Catalyst 2960 Switch
Email/DNS/FP Server
192.168.10.2
Authorisation Server
192.168.10.3
Web Server
192.168.10.1
IoT Device.
192.168.50.10

Above is a network diagram that represents the proposed network design for YorkInc. The network consists of four departments - Finance/HR, Engineering, Sales, and Administration - with each department having its own dedicated wired LAN network that cannot access workstations in any other department.

In addition, a separate wireless network is provided for staff-owned devices to access the internet, with access to the company servers but not permitted to access the departmental networks. The network also includes five servers - Web, Email, DNS, Authorization, and a File/Print server - accessible by all company computers and authorized wireless devices.[2]

The diagram shows a hierarchical network model with a core, distribution, and access layer. At the core layer, a Cisco Nexus 7000 switch provides high-speed data transfer between different departments and external networks. The distribution layer is represented by a Cisco Catalyst 6500 switch, which connects the access layer to the core layer and provides services such as routing, filtering, and policy enforcement. The access layer is represented by a Cisco Catalyst 2960 switch, which provides end-user access to the network and is responsible for connecting users to the distribution layer.[3]

Using VLANs and Access Control Lists (ACLs) enhances network scalability and security, preventing unauthorized access and ensuring that each department's network remains separate from others. The different departments are segmented into separate VLANs to maintain network security, with each VLAN assigned a unique subnet and IP address range. VLAN 10 is set to Finance/HR, VLAN 20 to Engineering, VLAN 30 to Sales, VLAN 40 to Administration, and VLAN 50 to the wireless network.

The network design incorporates five servers: the Web server, Email server, DNS server, Authorization server, and File/Print server. These servers are accessible to all company computers and authorized wireless devices. The Web server has an IP address of 192.168.10.1 and is accessible by any user. The Email/DNS/FP server is assigned an IP address of 192.168.10.2, while the Authorization server is assigned an IP address of 192.168.10.3. In addition, an IoT device with an IP address of 192.168.10.4 is used to monitor the server room temperature and door.

Hierarchical network design is essential because it enhances performance, reliability, scalability, better security, easier management and design, and improved cost-efficiency. The proposed network design is highly versatile and can be used in various real-world scenarios. It is suitable for large corporations,

educational institutions, government agencies, and healthcare providers, providing a scalable and secure network infrastructure for different departments or faculties.

A hierarchical network routes data through high-performance switches, resulting in faster data transfer and better bandwidth management. The modularity of the design makes the grid more reliable, scalable, and cost-efficient. Additionally, hierarchical networks provide better security as access control can be more granular, and traffic can be shaped and blocked more effectively. Finally, the design consistency from one module to the next makes hierarchical networks easier to manage, deploy and troubleshoot.[4]

A hierarchical network model ensures high-speed interconnectivity and scalability, while VLANs and ACLs provide enhanced network security. The wireless network provides authorized access to company servers, ensuring that employees or students can use their devices to access the internet and organizational servers.

The considerations when designing a hierarchical network include the organization's business needs, budgetary constraints, network size, and using on-premises versus cloud services. Gathering information and developing a plan with clear targets that determine technical requirements, such as bandwidth and security, is essential. Budgetary constraints must be considered, meaning designing a network just enough for the organization's needs or expanding the network incrementally over time.

The network size affects technical requirements and can dictate the approach, such as a collapsed-core design for a smaller network. Adopting a hierarchical network design may also be driven by how users access network services, such as cloud services. Legal regulations can also affect the network's structure, so they should be considered for compliance purposes.[4]

The proposed network design and IP addressing scheme have been carefully selected to meet the different departments' needs and provide scalability and security. VLANs and ACLs ensure each department's network is separated and secure, while the hierarchical network model provides high-speed interconnectivity and scalability. With state-of-the-art network switches and servers, this proposed network design provides a reliable, safe, and efficient network infrastructure adaptable to the organization's changing needs.

## Task 2: Scalability and Availability

Numerous network components and supporting technologies can be incorporated into the chosen network architecture to meet the demanding scalability and availability requirements to elevate its capabilities.

1. Redundancy must be incorporated at different network architecture levels to ensure high availability. There are several factors to consider when designing network redundancy for switches and routers.

   First, network protocols should be chosen to provide rapid switchover to backup devices when a failure occurs. Second, subnets must be connected to multiple routers to provide redundancy, and protocols such as HSRP and VRRP can reduce the recovery time from a router failure. Third, backup options like RAID and continuous cloud backup should be considered to protect against data loss. Fourth, processors must be regularly updated, and redundancy should be built to ensure continuous network operation. Power failure can occur, so battery backup and generator options should be considered. Finally, WAN connections should be reliable, and enterprises can procure links from two different network service providers for added protection.[5]

   Multiple core switches can be added to provide redundancy at the core layer, while redundant distribution switches and access controls can be incorporated at the distribution and access layers. The redundant control can take over seamlessly and minimize network downtime. By utilizing redundant core switches, high availability can be guaranteed even during a core switch failure. This redundancy approach can benefit large corporations with critical data centers that cannot afford network disruptions.

2. Equal Cost Multipath (ECMP) or Link Aggregation Control Protocol (LACP) is a popular load-balancing protocol that can be employed. Load balancing can be implemented to distribute network traffic evenly across various network components, which helps prevent the overloading of any one component, reducing the risk of network downtime or degraded performance.

   For instance, an e-commerce website that receives high traffic volumes could use load balancing to distribute network traffic across multiple web servers. This ensures the website remains responsive during peak traffic,

enhancing the user experience.

3. Routing protocols like OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol) can route network traffic efficiently between various departments and external networks. Such protocols can ensure that network traffic is routed optimally and rerouted swiftly in case of network component failure.

   This means OSPF is a routing protocol that supports complex networks with multiple routers and backup routers to balance traffic load. It establishes neighbor relationships between routers by exchanging "hello" packets and link-state updates and forms adjacencies with neighboring routers to exchange routing information.

   OSPF adjacency is formed when two routers are designated as a router or a backup router or interconnected by a point-to-point or point-to-multipoint network type. The interfaces to create the relationship must be in the same OSPF area. An institution with multiple branch offices could use routing protocols such as OSPF to ensure that customer transactions are processed quickly and efficiently, thereby improving customer satisfaction.[6]

4. Addressing protocols like Dynamic Host Configuration Protocol (DHCP) can automate IP address assignment to network devices, ensuring efficient IP address management as the network grows. An educational institution with many students and staff could use DHCP to automate IP address assignment to network devices, streamlining IP address management.

5. A firewall can control network access and traffic flow between different segments, enhancing network security and preventing unauthorized access or data breaches. A Next-Generation Firewall (NGFW) can provide advanced security features like intrusion prevention and malware detection, improving network security.

   To ensure proper firewall security practices, you should constantly update your firewall as soon as possible, use antivirus protection, limit accessible ports, and hosts with an allowlist, segment your network and have active network redundancies to avoid downtime. [7] These practices can mitigate the cyber-attack risk and protect your network and devices. Kaspersky Total Security and Kaspersky Endpoint Security are security

solutions that protect personal and business appliances.

6. Network segmentation can divide the network into smaller segments to improve network performance, security, and manageability. Network segmentation divides a network into smaller segments called subnets, which can improve network performance and security by controlling access to applications and devices.

   Logical network segmentation uses concepts like virtual local area networks (VLANs) to segment the network. Network segmentation is necessary for PCI compliance to keep cardholder data separate from other network parts. It can also protect against ransomware attacks by limiting lateral movement.

   The main benefits of network segmentation are increased security, improved network performance, and easier compliance with regulations.[8] For example, a DMZ (Demilitarized Zone) can separate the company's public-facing servers from the internal network.

Incorporating these measures can make the network more scalable, secure, and resilient. These additions will allow the network to adapt to the changing needs of the business and provide a reliable and efficient network infrastructure. Adding these network components and supporting technologies can make the network more scalable and available. These additions will allow the network to grow in the future without compromising on performance or availability.

## Task 3: Wireless Security and Legal/Ethical Implications

First, wireless networks are vulnerable to various security threats, including rogue access point attacks. A rogue access point is an unauthorized access point installed on a network by an attacker. Once connected to the rogue access point, the attacker can intercept data, including personally identifiable information (PII), which can compromise user privacy and security.

To mitigate rogue access point attacks, organizations can implement Wireless Intrusion Detection Systems (WIDS) to scan the wireless environment for unauthorized access points and enforce the use of secure Wi-Fi protocols, such as Wi-Fi Protected Access II (WPA2). It's also essential to educate users about the risks of connecting to unauthorized access points and encourage using secure networks.
There are two types of rogue access point attacks: passive interception and an active interception. In passive interception, the attacker can read user data but

cannot modify it. For example, if a user enters their password on a website over an insecure connection, the attacker can read the password. In active interception, the attacker can read and modify user data, allowing them to redirect sensitive information, such as bank account details, to their account.[9]

This means rogue access point attacks are a severe threat to wireless network security, and organizations and users should take precautions to prevent them. By implementing WIDS, enforcing secure Wi-Fi protocols, and educating users about the risks, organizations can reduce the risk of rogue access point attacks and protect sensitive data from interception and manipulation.

Secondly, a man-in-the-middle (MitM) attack happens when a hacker intercepts and alters or eavesdrops on communication between two devices, often using rogue APs or exploiting wireless protocol vulnerabilities. MitM attackers can passively listen or actively block and terminate connections, setting up new connections to destinations.

MitM attacks date back to the 1980s and can be used to redirect efforts or steal resources. Mitigation techniques include enforcing secure Wi-Fi protocols, implementing VPNs, and using encryption protocols such as TLS. Quantum cryptography could also provide robust protection against MitM attacks. [10] To prevent MitM attacks, end-users should avoid public Wi-Fi and heed warnings from browsers. The best prevention methods are multi-factor authentication, network control and visibility maximization, and network segmentation.

Furthermore, denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks can be mitigated using traffic shaping mechanisms that classify traffic based on network statistics. However, these mechanisms do not consider the traffic priorities of the attacked target and operate according to a universal policy that may not be optimal for all targets.

DoS attacks overwhelm a network with traffic, rendering it unusable. To mitigate DoS attacks, organizations can prioritize critical traffic using Quality of Service (QoS) and intrusion prevention systems (IPS) to detect and block malicious traffic. Wireless access points should be centrally located and placed in secure areas to prevent unauthorized access and tampering.

When it comes to adopting a Bring Your Device (BYOD) policy, there are potential legal and ethical implications that must be evaluated. From a legal perspective, the organization must ensure that the BYOD policy complies with data privacy laws, such as the General Data Protection Regulation (GDPR) and

the Health Insurance Portability and Accountability Act (HIPAA), which require the protection of sensitive data.

From an ethical perspective, the BYOD policy must consider the privacy rights of employees who use their devices for work. The organization must provide clear guidelines on what data can be accessed and collected from employee-owned devices and ensure that the policy is transparent and does not infringe on employee privacy.

In conclusion, assessing potential wireless network attacks and implementing mitigation strategies to secure the network is essential. The location of the wireless access points should also be considered to provide maximum coverage and signal strength while preventing unauthorized access. Regarding BYOD policies, evaluating the legal and ethical implications of protecting sensitive data and employee privacy is essential.

[1 ] computernetworkingnotes[Online]. Available: https://www.computernetworkingnotes.com/ccna-study-guide/access-distribution-and-core-layers-explained.html[Accessed: 25 February 2023].
[2 ]en.wikipedia.org[Online]. Available: https://en.wikipedia.org/wiki/Computer_network[Accessed: 26 February 2023].
[3 ] www.cisco.com[Online]. Available: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-data-sheet-cte-en.html[Accessed: 27 February 2023].
[4 ]www.auvik.com[Online]. Available: https://www.auvik.com/franklyit/blog/hierarchical-network-design/[Accessed: 28 February 2023].
[5 ]techtarget[Online]. Available: https://www.techtarget.com/searchnetworking/tip/7-factors-to-consider-in-network-redundancy-design[Accessed: 28 February 2023].
[6 ] en.wikipedia.org[Online]. Available:https://en.wikipedia.org/wiki/Open_Shortest_Path_First [Accessed: 29 February 2023].
[7] The USA. Kaspersky [Online]. Available: https://usa.kaspersky.com/resource-center/definitions/firewall[Accessed: 29 February 2023].
[8 ]https://www.spamtitan.com/ [Online]. Available: https://www.spamtitan.com/web-filtering/network-segmentation-best-practices/[Accessed: 29 February 2023].
[9 ]khanacademy.org [Online]. Available:https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:cyber-attacks/a/rogue-access-points-mitm-attacks [Accessed: 29 February 2023].
[10]csoonline [Online]. Available:https://www.csoonline.com/article/3340117/man-in-the-middle-attack-definition-and-examples.html [Accessed: 27 February 2023].
[11 ] ResearchGate[Online]. Available:https://www.researchgate.net/publication/3950533_Mitigation_of_DoS_attacks_through_QoS_regulation [Accessed: 27 February 2023].