

Design and Implementation of Hierarchical Network

Hein Arkar Zaw 001354122

Supervisor: Dr. Aung Htein Maw

COMP1682 Final Year Project

Computing (Network Systems), BSc Hons

Due Date: 29th April 2024

Word Count: 9190

Abstract

This project uses a simulation tool to design and implement a hierarchical network. Today, organizations are facing challenges such as congested networks, complexity in management, cyber security threats, speed limitations, and high expenses. Thus, hierarchical network design is considered to solve these issues. It comprises three layers. They are access, distribution, and core layers. Each layer comprises the networking devices. This design aims to build a scalable, manageable, efficient, secure, and reliable network to reflect the real-world enterprise network. The entire network is implemented through researched networking theories. This report includes theory explanations, design, configurations, testing results, project conclusion, and references.

Table of Contents

1. Introduction	8
2. Aims and Objectives	9
2.1. Aims	9
2.2. Objectives	9
3. Research Approach	10
3.1. Literature Review on Current Network Technologies	10
3.1.1. Exploring the Open Systems Interconnection (OSI) Model.....	10
3.1.2. Exploring the TCP/IP Model	13
3.1.3. Overview of Network Protocols	14
3.1.4. Exploring Wireless Technologies.....	16
3.1.5. Exploring Wired Technologies	16
3.1.6. Understanding Routing Concepts	16
3.1.7. Understanding Switching Concepts	17
3.1.8. Enhancement of Network Security	17
3.1.9. Understanding IP Addressing.....	17
3.2. Literature Review on Existing Network Designs	18
3.2.1. Network Topologies.....	18
3.2.2. Hierarchical Network Design	21
3.3. Hierarchical Network Design Approach	23
4. Design and Implementation	26
4.1. Review on Simulation Tools	26
4.2. Design and Configuration.....	26
4.2.1. Hierarchical Network Design Demonstration	26
4.2.2. Initial Configuration on Network Devices.....	30
4.2.3. Initial Security Configuration	30
4.2.4. SSH Configuration on Multilayer Switches and Routers.....	31
4.2.5. Standard ACL Configuration for SSH	31
4.2.6. Creating VLAN on Layer 2 Switches	32
4.2.7. IP Addressing on Multilayer Switches.....	33
4.2.8. Inter-VLAN Routing Configuration on Multilayer Switch	33
4.2.9. Creating EtherChannel Between Multilayer Switches.....	33
4.2.10. OSPF Configuration on L3 Switches, Core and ISP Routers	34
4.2.11. DHCP Server Configuration	35

4.2.12.	Port Security Configuration on Server Switch	36
4.2.13.	HSRP Configuration on Multilayer Switches	36
4.2.14.	Enabling STP PortFast and BPDU Guard on All Access Ports.....	38
4.2.15.	Configuring NAT ACL	39
4.2.16.	Wireless LAN Controller Configuration	40
4.2.17.	Setting Up DNS Server	44
4.2.18.	Setting Up WEB Server	45
4.2.19.	Setting Up EMAIL Server	45
4.3.	Testing and Evaluation	47
4.3.1.	Password Testing.....	47
4.3.2.	Testing Secure Remote Access for Only PCs from D4	47
4.3.3.	Testing DHCP Requests Provided by the DHCP Server.....	48
4.3.4.	Testing Wi-Fi Functionality	49
4.3.5.	Testing the DNS and WEB Servers Via Wi-Fi.....	50
4.3.6.	Testing EMAIL Server by Sending Mails.....	51
4.3.7.	Testing HSRP	52
4.3.8.	Verifying EtherChannel Status	53
4.3.9.	Testing Conclusion.....	54
5.	Project Conclusion	55
6.	References	56
7.	Appendix.....	58
7.1.	Proposal Overview.....	58
7.2.	Aims and Objectives	59
7.3.	Legal, Ethical, Social, and Professional Issues	60
7.4.	Research Approach Overview.....	61
7.5.	Project Planning.....	61

Figure List

Figure (3.1): The Layers of OSI (Bouchard, 2020)	10
Figure (3.2): TCP/IP Model (the-internet-protocols, n.d.)	13
Figure (3.3): Bus Topology (advantages-and-disadvantages-of-bus-topology, n.d.)	18
Figure (3.4): Ring Topology (what-is-a-ring-topology, n.d.)	19
Figure (3.5): Star Topology (what-is-star-topology, n.d.)	19
Figure (3.6): Mesh Topology (what-is-mesh-topology, n.d.)	20
Figure (3.7): Hierarchical Network Design (three-layer-hierarchical-model-in-cisco, n.d.)	21
Figure (5.1): Complete Hierarchical Network Design	26
Figure (5.2): Initial Configuration in Cisco Router	30
Figure (5.3): Configuration for Authenticity in Cisco Router	30
Figure (5.4): SSH Configuration on Router	31
Figure (5.5): Standard ACL Configuration for SSH	31
Figure (5.6): Creating VLAN on D1-SW	32
Figure (5.7): Configuring Trunk Ports and Access Ports	32
Figure (5.8): Created VLAN 10	32
Figure (5.9): IP Assigning on Routed Interface G1/0/1 of HQ-MLS1	33
Figure (5.10): Configuring Inter-VLAN Routing on HQ-MLS1	33
Figure (5.11): LACP EtherChannel	33
Figure (5.12): Creating LACP EtherChannel by Aggregating G1/0/8 and G1/0/9	34
Figure (5.13): OSPF configuration on HQ-MLS1	34
Figure (5.14): Creating Pools on the DHCP Server	35
Figure (5.15): Port Security Configuration on SEV-SW	36
Figure (5.16): Shutting Down Unused Ports on SEV-SW	36
Figure (5.17): HSRP Configuration on HQ-MLS1	36
Figure (5.18): HSRP Active State on HQ-MLS1	37
Figure (5.19): HSRP Configuration on HQ-MLS2	37
Figure (5.20): HSRP Standby State on HQ-MLS2	37
Figure (5.21): Enabling STP PortFast on All Access Ports	38
Figure (5.22): Enabling STP BPDU Guard on All Access Ports	38
Figure (5.23): Configuring NAT Inside and Outside	39
Figure (5.24): Configuring ACL for NAT and PAT	39
Figure (5.25): IP Configuration on WLC Management	40

Figure (5.26): IP Configuration on WLC-PC	40
Figure (5.27): Creating Admin Account and Setting Up Controller	41
Figure (5.28): Creating the First Wireless Network and Completing the Setup	42
Figure (5.29): Accessing WLC.....	42
Figure (5.30): Configuring VLANs for Interfaces of APs from D1, D2, D3, and D4	43
Figure (5.31): Creating WLANs	43
Figure (5.32): Adding AP Groups.....	44
Figure (5.33): Setting Up DNS Server	44
Figure (5.34): Setting Up WEB Server	45
Figure (5.35): Setting Up EMAIL Server	45
Figure (5.36): Configuring Mail on D1-Laptop	46
Figure (5.37): Result of Initial Security Configuration.....	47
Figure (5.38): Secure Remote Access to the Multilayer Switch from D4-PC1	47
Figure (5.39): Rejection of Remote Access from D1-PC1 to the Multilayer Switch	48
Figure (5.40): Successful DHCP Request from D1-PC1.....	48
Figure (5.41): Adding WPC300N Module to all Laptops	49
Figure (5.42): Successful DHCP Request of D1-Laptop.....	49
Figure (5.43): No Wireless Connection of D1-Laptop	50
Figure (5.44): After D1-Laptop Connects to the D1-AP.....	50
Figure (5.45): Composing Mail from D1-Laptop.....	51
Figure (5.46): D2-Laptop's Received Mail	51
Figure (5.47): Remove AC Power Supply from HQ-MLS1	52
Figure (5.48): Checking Active State in HQ-MLS2.....	52
Figure (5.49): Successful DHCP Request from D1-PC1 When HQ-MLS1 Fails	53
Figure (5.50): EtherChannel Summary.....	53
Figure (5.51): Providing Redundancy.....	54

Table List

Table (5.1): VLAN Segmentation and Assigned Networks for Departments.....	27
Table (5.2): Static IP Addresses for Servers in Server Room.....	28
Table (5.3): Static IP Addresses for WLC Management.....	28
Table (5.4): IP Addresses Between the Core Routers and Multilayer Switches.....	28
Table (5.5): IP Addresses Between the Core Routers and ISPs	29
Table (5.6): Network Cable Types Installation.....	29

1. Introduction

Today, many enterprises must have a robust network design to make daily conversations, access servers, and share data. When the network is not well-designed, there will be complexities while managing networks. Network administrators may face challenges in managing and troubleshooting networks. It may impact not only the enterprise's performance but also its reputation. The hierarchical network design can solve these issues. Since it works with layers (access, distribution, and core), network administrators can partly manage the network. Network devices in each layer can process their functions efficiently. It enhances the overall network performance, security, and reliability. The network can be expanded by adding new network devices in the future. Therefore, the hierarchical network design is a preferred choice for many enterprises as it is scalable, manageable, efficient, secure, and reliable.

2. Aims and Objectives

2.1. Aims

This project aims to design and implement the 3-layer hierarchical network using the simulation tool.

2.2. Objectives

The following objectives are considered for researching, designing, implementing, and testing the hierarchical network to complete the project. The objectives are:

1. Research [3. 2]

- 1.1. Research on current network technologies [1. 0]
- 1.2. Research on network designs [1. 0]
- 1.3. Discussion with supervisor [1. 0]
- 1.4. Title approval by the supervisor [0. 2]

2. Research approach [5. 0]

- 2.1. Literature review on current network technologies [3. 5]
- 2.2. Literature review on existing network designs [3. 2]
- 2.3. Hierarchical network design approach [1. 2]

3. Design and implementation [12. 3]

- 3.1. Review of simulation tools [2. 0]
- 3.2. Design and configuration [9. 2]
- 3.3. Testing and evaluation [1. 3]

4. Documentation and project conclusion [2. 4]

- 4.1. Review of the whole project [0. 6]
- 4.2. Validation and verification [0. 6]
- 4.3. Finalize the documentation [0. 6]

3. Research Approach

3.1. Literature Review on Current Network Technologies

Current network technologies are researched to evaluate their roles in network infrastructures. This session includes research on the OSI reference model, TCP/IP model, network protocols, wireless and wired technologies, routing and switching concepts, security features, and IP addressing.

3.1.1.Exploring the Open Systems Interconnection (OSI) Model

The OSI model is a reference model. It is a theoretical concept to understand networking concepts. It has 7 layers. Each layer has a specific function and purpose. **Figure (3.1)** represents these 7 layers of the OSI model.

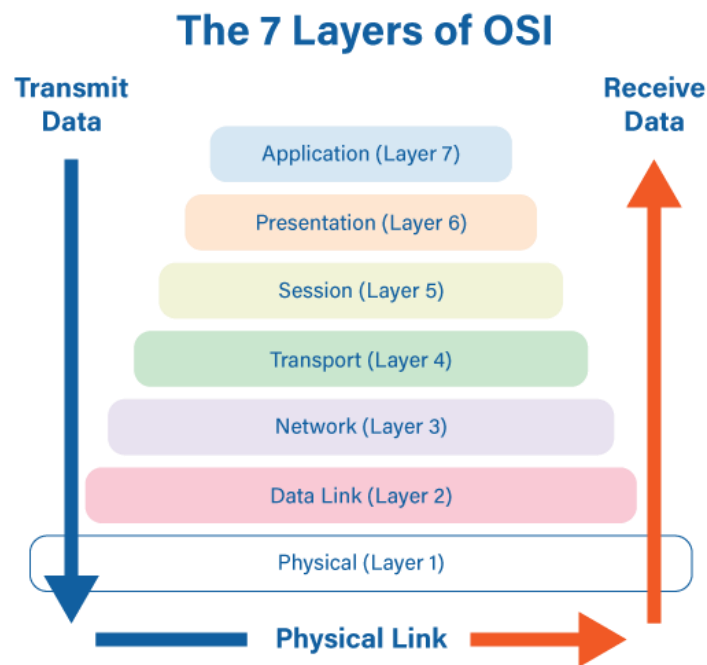


Figure (3.1): The Layers of OSI (Bouchard, 2020)

In **Figure (3.1)**, the sender's data transmission begins at the application layer. It descends through the layers to the physical layer with encapsulation processes. Subsequently, the data ascends from the physical layer to the application layer with decapsulation processes. Finally, the recipient receives the data. Each layer is discussed below.

1. Layer 1 or Physical Layer

The physical layer is responsible for transferring data bits between physical devices. These data bits are converted into electrical signals for wired connections and radio signals for wireless connections. Cable and pin layouts are determined in this layer. The bits transmitted from the sender are equally received by the receiver. It has an error detection function such as Cyclic Redundancy Check (CRC) while transmitting data.

2. Layer 2 or Data Link Layer

The data link Layer breaks incoming data into frames. It is responsible for connectivity of end host to switch, switch to router, etc. It enables error detection function by Frame Check Sequence (FCS). It controls data flow including multiplexing. It ensures that the transmission is error-free and reliable. It has two main tasks, Logical Link Control (LLC) and Media Access Control (MAC). LLC controls the virtual connections and MAC controls the physical connections between devices. Switches work at this layer.

3. Layer 3 or Network Layer

The network layer is responsible for the connection between end hosts on different networks. It has functions of IP addressing and path selection between source and destination. There are two main key protocols, Internet Protocol (IP) and Internet Control Message Protocol (ICMP). Routers work at this layer. It includes routing protocols such as Open Shortest Path First (OSPF) and Routing Information Protocol (RIP). In this layer, the protocol data unit (PDU) is called a packet.

4. Layer 4 or Transport Layer

The transport layer is responsible for accepting the incoming data. Its PDU is called a segment. Small segments can be sent over the network with fewer errors. Transmission Control Protocol (TCP), and User Datagram Protocol (UDP) are the two main protocols in this layer.

TCP is connection-oriented which means there is a creation of a connection between two endpoints before data transmission. UDP is connectionless, meaning there is no connection creation before data transmission. TCP is more reliable than UDP because TCP has an acknowledgment process. Therefore, messaging applications prefer TCP for data integrity while real-time applications prefer UDP to reduce latency.

5. Layer 5 or Session Layer

The session layer controls sessions between communicating hosts. It can establish, manage, and terminate the connection. In addition, it has a recovery session by making checkpoints when failure occurs.

6. Layer 6 or Presentation Layer

The presentation layer's main task is to translate data formats during transmission. It has encryption, and decryption functions for data integrity. Plus, it has a compression function to reduce data load during transmission.

7. Layer 7 or Application Layer

The application layer is the closest layer to the end users. Users must use an interface such as a web browser to communicate with each other. It allows network services such as HTTP, files, and email to the end users.

(Tanenbaum & Wetherall, The OSI Reference Model, 2010) (Secgin, 2023)

3.1.2.Exploring the TCP/IP Model

The TCP/IP model is a universal standard for networking protocols. It is used in practice today. It serves as the backbone of the internet for communication across the networks. It has 4 layers. They are the application, transport, internet, and link layers. **Figure (3.2)** represents the TCP/IP model.

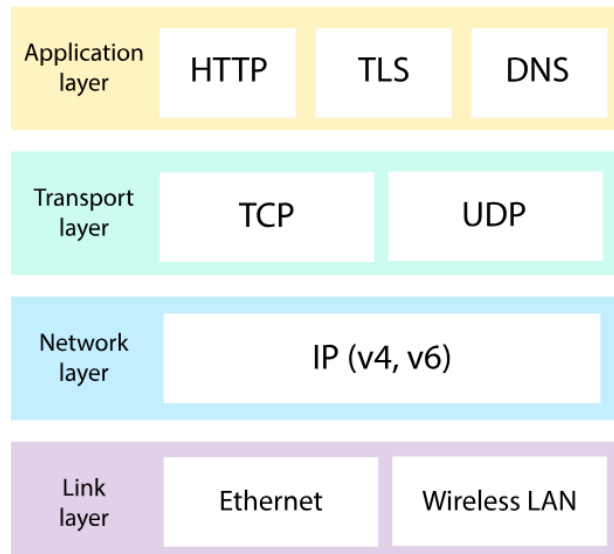


Figure (3.2): TCP/IP Model (the-internet-protocols, n.d.)

In **Figure (3.2)**, the TCP/IP model comprises 4 layers. They are the link layer, the network layer, the transport layer, and the application layer. They operate with respective protocols. Ethernet and wireless LAN protocols work in the link layer by transmitting data over network cables or wireless connections. Then, IPv4 and IPv6 protocols in the network layer make routing, determining the path for data packets to travel across the interconnections. After that, TCP and UDP protocols in the transport layer handle data delivery between applications. Moreover, HTTP, TLS, and DNS protocols in the application layer work with web browsers, email clients, and file transfers.

(Tanenbaum & Wetherall, The TCP/IP Reference Model, 2010)

3.1.3. Overview of Network Protocols

Protocols are rules to give instructions on how the devices in a network would communicate. They include network layer protocols, transport layer protocols, and application layer protocols.

Network Layer Protocols

Some protocols are working in the network layer. They are Internet Protocol (IP), Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP), and Address Resolution Protocol (ARP).

1. Internet Protocol (IP) – It provides logical addressing and routing.
2. Internet Control Message Protocol (ICMP) – It provides diagnostics and error-reporting functionality between network devices.
3. Internet Group Management Protocol (IGMP) – It manages how devices join and leave multicast groups which means one sender sends data to multiple receivers.
4. Address Resolution Protocol (ARP) – It maps the IP address to its MAC address.

(GeeksforGeeks, network-layer-protocols, 2024)

Transport Layer Protocols

Some protocols are working in the transport layer. They are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

1. Transmission Control Protocol (TCP) – It provides a reliable connection.
2. User Datagram Protocol (UDP) – It provides faster connection.

Application Layer Protocols

Some protocols are working in the application layer. They are Hypertext Transfer Protocol (HTTP and HTTPS), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), Internet Message Access Protocol (IMAP), Domain Name System (DNS), and Simple Network Management Protocol (SNMP).

1. Hypertext Transfer Protocol (HTTP) – It provides web communication.
2. Hypertext Transfer Protocol Secure (HTTPS) – It provides encryption to web communication.

3. File Transfer Protocol (FTP) – It provides efficient file transferring between client and server.
4. Simple Mail Transfer Protocol (SMTP) – It works for sending electronic mail.
5. Post Office Protocol (POP) - Downloads messages to your device and then deletes them from the server.
6. Internet Message Access Protocol (IMAP) – It allows accessing and managing messages on the server without downloading them.
7. Domain Name System (DNS) – It translates domain names into IP addresses that computers understand.
8. Simple Network Management Protocol (SNMP) - It allows monitoring and management of network devices like routers, switches, and servers.

(GeeksforGeeks, protocols-application-layer, 2024)

These protocols work together to make different devices and applications communicate effectively on a worldwide network.

3.1.4.Exploring Wireless Technologies

Wireless technologies perform data transmission without physical connections. Wi-Fi is one of the great wireless technologies. It allows devices to access the internet and share data. Besides Wi-Fi, there are cellular networks such as 4G, and 5G which provide mobile broadband internet. Another technology is Bluetooth technology which provides short-range wireless connections for daily devices such as keyboards, mice, controllers, etc. The next technology is Radio Frequency Identification (RFID) which provides connectivity between IoT applications and devices by radio waves. Moreover, there is also Near Field Communication (NFC) technology which offers contactless data exchange between mobile devices.

(HO, 2018)

3.1.5.Exploring Wired Technologies

Wired technologies possess various physical connectivity for data transmission. Ethernet is a popular wired technology that uses twisted-pair cables to perform high-speed, and reliable connections within Local Area Networks (LANs). Fiber optics can be used for long-distance transmission. It transmits light signals through glass or plastic fibers with high bandwidth. Another cable is a coaxial cable in which a central conductor. It is commonly used in television. Wired technologies are more stable than wireless technologies. They provide more consistent performance than wireless.

(BrainKart, n.d.)

3.1.6.Understanding Routing Concepts

Routing packets from source to destination is the main function in the network layer. There are static and dynamic routing algorithms. Static routings are used when the routes are determined while dynamic routings are used when the routes may vary. Packets must be timely and securely delivered to the destination. In dynamic routing, protocols such as OSPF, and RIP perform the path selection process. OSPF algorithm chooses the path that contains less costs while RIP selects the path that contains fewer hop counts. OSPF is the link state routing protocol that uses Dijkstra's Algorithm and RIP is the distance-vector routing protocol that uses the Bellman-Ford Algorithm. While routing, traffic can be managed, and prioritized with Quality of Service (QoS) by limiting network capacity. These routing concepts are essential for efficient communication between different networks.

(GeeksforGeeks, what-is-routing, 2023) (Misra & Goswami, 2014)

3.1.7. Understanding Switching Concepts

Switching operates at the data link layer based on MAC addresses. There are layer 3 switches. Virtual Local Area Networks (VLANs) can be created in switches. Layer 3 switches have both routing and switching capabilities. They are used to handle high traffic of Inter-VLAN routing. There are other switching concepts called cut-through switching and store-and-forward switching. Store-and-forward switching is more reliable than cut-through switching but it has higher latency. Switching learns the MAC address of frames automatically to update its table.

(GeeksforGeeks, what-is-switching, 2023)

3.1.8. Enhancement of Network Security

Security measures are important to protect the network. Every network has potential threats such as unauthorized access, data theft, cyberattacks, etc. Encryption methods can be used to keep data safe. Firewalls can be used to filter unwanted traffic coming from outside the network. Therefore, network traffic should be monitored continuously. In addition, there is an Intrusion Detection System (IDS) to monitor the network. For authentication, passwords and biometrics are popular methods to verify user identities. Moreover, software and firmware must be up to date for patching vulnerabilities. Virtual Private Network (VPN) technology can make communication secure by virtual tunnels across the networks. These above measures can work together to protect the network against potential threats.

(Insider, n.d.)

3.1.9. Understanding IP Addressing

IP addresses are unique for every device in the network. There are two versions, IPv4 and IPv6. IPv4 is 32-bit addresses and IPv6 is 128-bit addresses. IP addresses can be divided into network and host portions. When assigning IP addresses, it takes much time as the network grows. Dynamic Host Configuration Protocol (DHCP) is a useful protocol that assigns IP addresses to devices automatically. Subnetting is an essential method to divide networks into smaller ones to reduce unnecessary traffic. IP addressing provides the right place for the right traffic. Therefore, it is an essential task for devices to communicate with each other.

(Jim Kurose, 2020)

3.2. Literature Review on Existing Network Designs

3.2.1. Network Topologies

Network topologies describe how devices are interconnected within a network. They define the layout and structure of communication paths. Common topologies include bus, ring, star, and mesh. Understanding these topologies helps in designing and managing efficient networks for various sizes of organizations.

Bus Topology

Bus topology is formed when all devices share a single communication channel. It is simple but data collision may occur during transmission. However, the entire network will fail if there is a failure at one point.

Bus topology

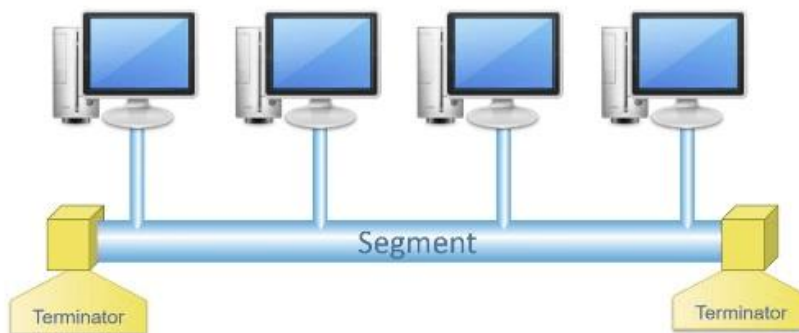


Figure (3.3): Bus Topology (advantages-and-disadvantages-of-bus-topology, n.d.)

Ring Topology

Ring topology is formed when devices are connected circularly. There is only one direction for data transmission. Therefore, a failure at one point may disrupt the entire network.

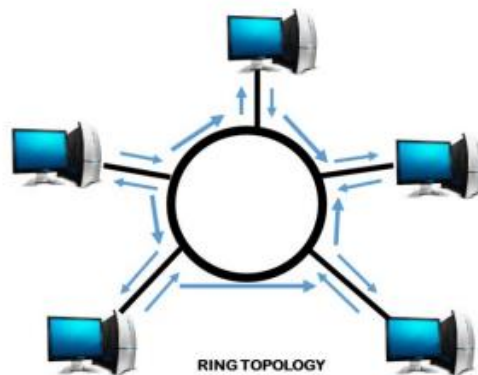


Figure (3.4): Ring Topology (what-is-a-ring-topology, n.d.)

Star Topology

Star topology is formed when all devices connect to a central hub. It is easy to manage the network. However, the entire network will fail if the central hub fails.

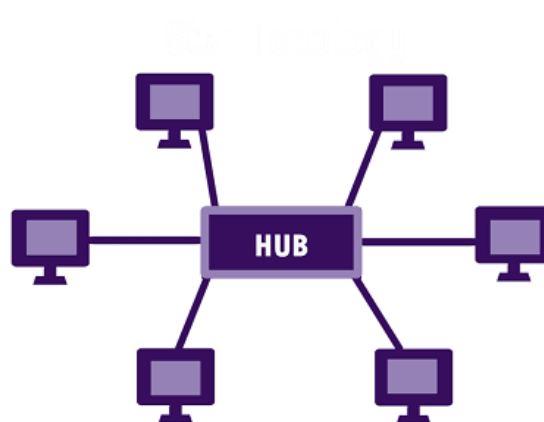


Figure (3.5): Star Topology (what-is-star-topology, n.d.)

Mesh Topology

Mesh topology is formed when one device is connected to every device in the network. Therefore, there are multiple links for data transmission. If one link fails the other link will perform as a backup link. It improves the reliability of the network. On the other hand, there may be high cost and complexity. However, it forms a robust network.

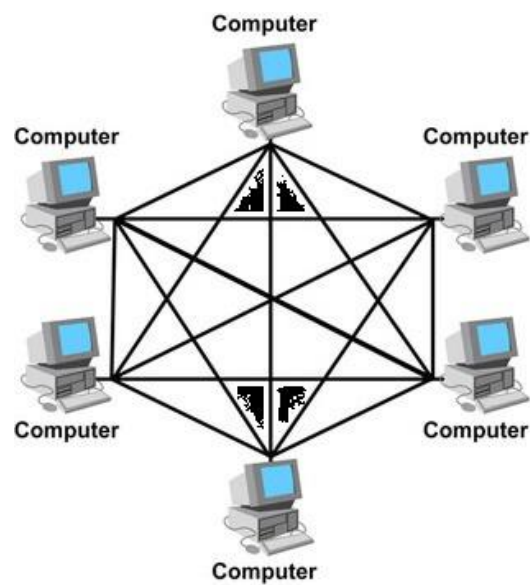


Figure (3.6): Mesh Topology (what-is-mesh-topology, n.d.)

3.2.2. Hierarchical Network Design

Hierarchical network design is modularly formed by 3 layers. They are access, distribution, and core layers. The access layer is responsible for end-user device connectivity. The distribution layer is responsible for managing traffic and policy configuration. The core layer is responsible for high-speed switching.

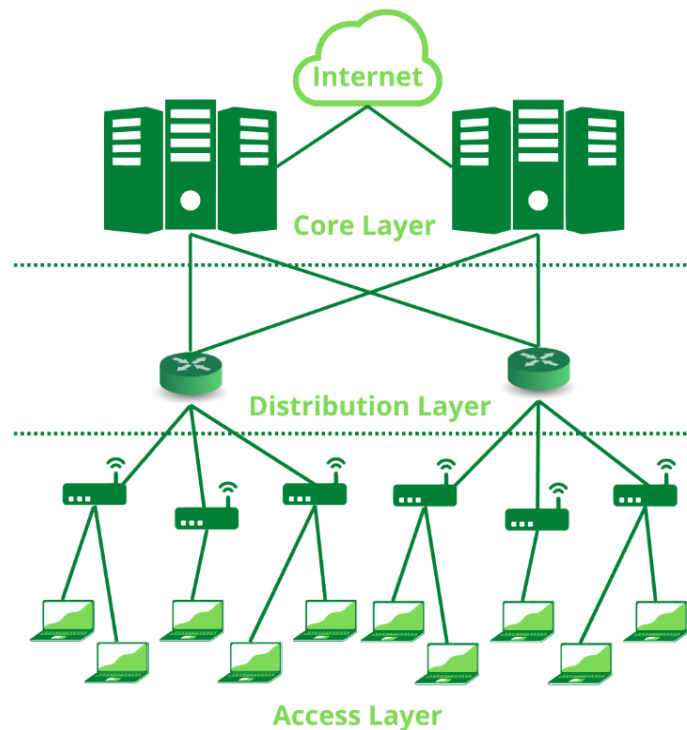


Figure (3.7): Hierarchical Network Design (three-layer-hierarchical-model-in-cisco, n.d.)

Hierarchical network design is a popular approach for building robust and scalable network architectures, comprising distinct layers, each serving specific purposes for efficient communication and controlling the network. This review discusses the key concepts underlying hierarchical network design.

1. Hierarchical Design Principles

The principles of hierarchical network design consist of modularity, scalability, and flexibility. In a modular design, each layer independently performs specific functions. This modularity enhances scalability by allowing new components to be added or existing ones to be modified without impacting the entire network.

2. Access, Distribution, and Core Layers of Hierarchical Network Design

The hierarchical design consists of access, distribution, and core layers. The access layer connects end devices and provides local network access. The distribution layer aggregates traffic from access switches and provides policy-based routing and access control. The core layer handles high-speed backbone connectivity and efficiently routes and forwards packets.

3. Benefits of Hierarchical Network Design

Hierarchical network design offers several advantages. They are ease of management, improved performance, and enhanced security. The whole network enables better traffic management and reduces network congestion by providing multiple redundant paths for data transmission.

4. Scalability and Redundancy of Hierarchical Network Design

Scalability is critical in hierarchical network design. Seamless network growth is enabled by expanding existing infrastructure. Redundancy mechanisms provide reliability and high availability to the network by minimizing downtime.

5. Convergence and Traffic Optimization of Hierarchical Network Design

The hierarchical design operates traffic flow efficiently by deploying dynamic routing protocols such as OSPF and EIGRP in the distribution layer to adapt to network changes in infrastructure. It has the advantages of optimal path selection with redundancies and load balancing.

(Academy, 2014)

6. Security Considerations of Hierarchical Network Design

Security is carefully considered by integrating Access Control Lists (ACLs), firewalls, VPNs, and Intrusion Detection Systems (IDS) to protect sensitive data and prevent unauthorized access. Therefore, Network Access Control (NAC) should be considered who can access and who will be denied. These measures help the network protect against potential threats and ensure the confidentiality, integrity, and availability of data.

(Stallings, 2018) (Perez, 2014)

3.3. Hierarchical Network Design Approach

Before initiating the project configuration, the hierarchical network design approach is discussed. Considerations for hierarchical network design are outlined below.

1. Access Layer

In the access layer, there are PCs, Laptops, Access Points, printers, servers, and layer 2 switches. It lets them access the network through wired and wireless access points. This layer also implements VLANs for logical segmentation. It can separate network domains for each department.

2. Distribution Layer

In the distribution layer, there are multilayer switches and they gather traffic from multiple layer 2 switches and provide routing with dynamic routing protocols. It enables efficient inter-VLAN communication. Security measures such as Access Control Lists (ACLs) are implemented for network protection.

3. Core Layer

In the core layer, there are core routers to transfer data with high-speed packet switching. It focuses on high availability through redundant links and dynamic routing protocols.

4. Spanning Tree Protocol

Spanning Tree Protocol (STP) can make the network loop-free by blocking backup links. As soon as the active link fails, it enables the backup link active.

5. Virtual LANs (VLANs)

VLANs are used to segment the network logically. It enhances security and manageability within the hierarchical structure.

6. Dynamic Host Configuration Protocol (DHCP)

DHCP server is used for automatic IP addressing. It saves time and effort for network administrators as the network grows in the future.

7. Access Control Lists (ACLs)

ACLs can be implemented in the distribution layer. Rules must be configured carefully for the right purpose. They can secure the network by restricting specific traffic depending on the organization's policies.

8. Open Shortest Path First (OSPF)

In hierarchical network design, OSPF (Open Shortest Path First) provides dynamic routing, ensuring optimal path selection and load balancing across different network layers for efficient traffic management.

(Borthakur, 2022)

9. Load Balancing

Load balancing is an important mechanism not to cause bottlenecks and network failure. It takes place at the distribution layer. The load balancer equally distributes traffic to the servers. It improves the performance of the servers.

10. Dynamic Host Configuration Protocol (DHCP)

DHCP provides automatic assignment of IP address. When the device connects to the network, DHCP automatically assigns the available IP address from the created pool. It is very suitable in hierarchical network design since it expects the growth of devices by avoiding manual assignment of IP addresses reducing the complexity.

(Rajput, Tewani, & Dubey, 2016)

11. EtherChannel

EtherChannel aggregates multiple links into a virtual single link. It can not only increase bandwidth but also provide fault tolerance in hierarchical network design. There are two types of dynamic EtherChannel. Link Aggregation Control Protocol (LACP) enables the automatic creation of the channel while the Port Aggregation Protocol (PAgP) is Cisco-specific.

12. Wireless LAN Controller

To provide a wireless network within the design, a wireless LAN controller is a preferred device to control many access points via a single controller. It reduces complexity providing better manageability and ease of troubleshooting Wi-Fi issues. It is a good choice for such a hierarchical network design.

13. Hot Standby Router Protocol (HSRP)

The main point of using HSRP in hierarchical network design is for high availability at the gateway. If one router fails, the standby router will become an active state to fail over the failure router. Downtime can be minimized in this way.

14. Domain Name System (DNS)

Every resource on the internet has a unique name called the domain name. Users can access the websites which are provided by the web servers. Also, Users can send electronic mail which is sent by the mail servers. The domain names can be memorized by users easily while the IP addresses are not. Therefore, the domain name system performs the translation of domain names into IP addresses so that users can access their desired programs or websites.

(Chandramouli & Rose, 2013)

15. Network Address Translation (NAT)

NAT is important for communication between different networks. It translates multiple private IP addresses into a single public IP address for inside and public IP addresses into multiple private IP addresses for outside. It covers the internal network and the internet will see only the public IP of NAT.

16. Secure Shell (SSH)

SSH provides secure remote login into the network by the network administrators. It protects sensitive information by encryption. Only authorized persons can access the network resources.

(Forouzan B. , 2012) (Kurose & Ross, 2018) (Tanenbaum & Wetherall, Computer Networks, 2011)
(Forouzan B. A., 2009)

4. Design and Implementation

4.1. Review on Simulation Tools

There are many networking simulation tools today. Among them, the Cisco Packet Tracer is chosen to build the hierarchical network design. It provides a real-time simulation process and a wide range of networking features.

(packet-tracer, n.d.)

4.2. Design and Configuration

4.2.1. Hierarchical Network Design Demonstration

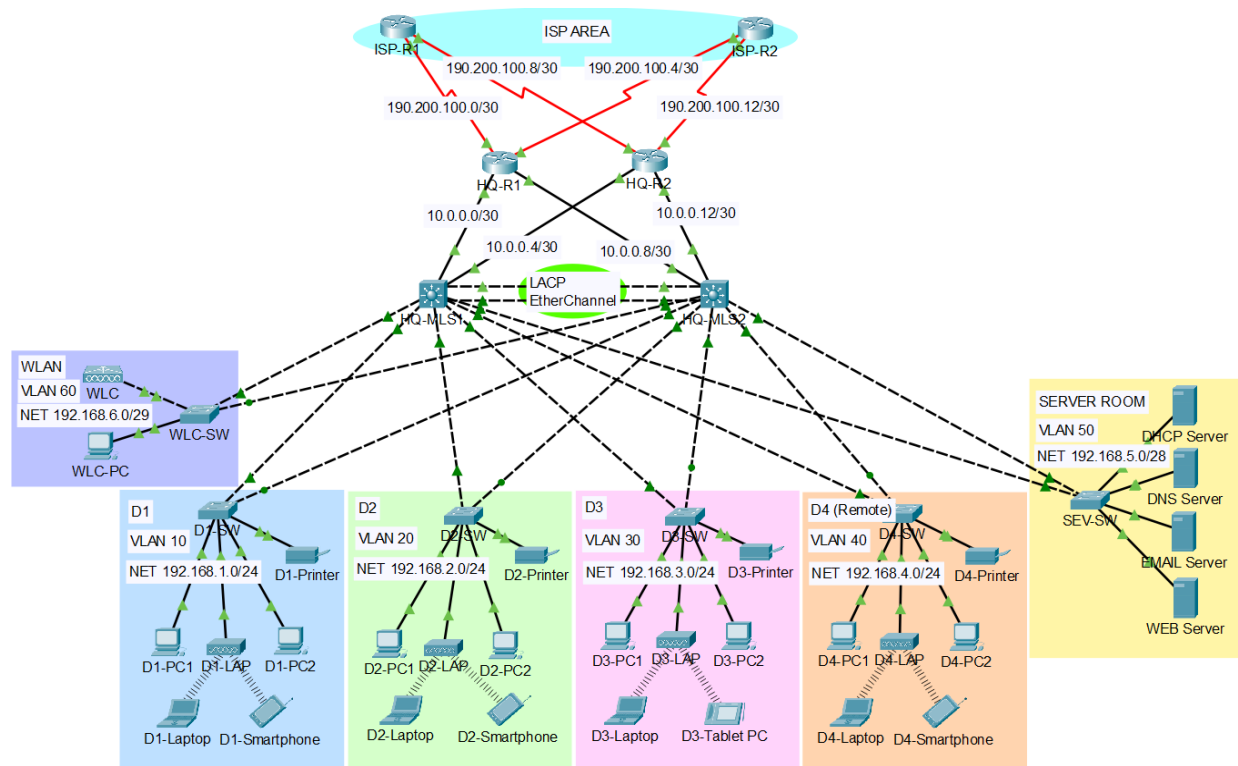


Figure (5.1): Complete Hierarchical Network Design

In **Figure (5.1)**, the complete hierarchical network design is demonstrated. This design provides modularity, scalability, and flexibility. There are two multilayer switches interconnected via LACP EtherChannel, ensuring high-bandwidth links between network segments. HSRP is configured on those switches, providing redundancy for seamless failover in case of a switch or link failure. Each multilayer switch connects to both core routers, establishing redundant

connections to the network backbone. The core routers further connect to redundant ISP routers via serial DCE links.

There are four departments which are called D1, D2, D3 and D4. There is a server room that includes DHCP, DNS, EMAIL, and WEB servers. VLANs are assigned to each department, server room, and wireless LAN controller management. Inter-VLAN routing is configured on the multilayer switches, enabling communication between different VLANs.

DHCP service is provided to all departments. All the access ports are configured with Spanning Tree PortFast and BPDU Guard to enhance the loop-free network. As the dynamic routing protocol, OSPF is used for scalable and efficient routing.

The Wireless LAN Controller (WLC) manages access points in all departments. SSH and its standard ACLs safeguard network devices from unauthorized access. Access Control Lists (ACLs) for Network Address Translation (NAT) enable secure communication with external networks. These various technologies are implemented in this hierarchical network design. VLAN segmentation and assigned networks for departments are described in **Table (5.1)**.

Department Name	VLAN ID	Network and Subnet Mask	Valid Host Addresses	Default Gateway	Broadcast
D1	10	192.168.1.0/24	192.168.1.1 to 192.168.1.254	192.168.1.1	192.168.1.255
D2	20	192.168.2.0/24	192.168.2.1 to 192.168.2.254	192.168.2.1	192.168.2.255
D3	30	192.168.3.0/24	192.168.3.1 to 192.168.3.254	192.168.3.1	192.168.3.255
D4	40	192.168.4.0/24	192.168.4.1 to 192.168.4.254	192.168.4.1	192.168.4.255
Server Room	50	192.168.5.0/28	192.168.5.1 to 192.168.5.14	192.168.5.1	192.168.5.15
WLAN Management	60	192.168.6.0/29	192.168.6.1 to 192.168.6.6	192.168.6.1	192.168.6.7

Table (5.1): VLAN Segmentation and Assigned Networks for Departments

Static IP Addresses are assigned to servers from the server room. See **Table (5.2)**.

Name	IP Address	Subnet Mask
DHCP Server	192.168.5.2	255.255.255.240
DNS Server	192.168.5.3	255.255.255.240
EMAIL Server	192.168.5.4	255.255.255.240
WEB Server	192.168.5.5	255.255.255.240

Table (5.2): Static IP Addresses for Servers in Server Room

Static IP Addresses are assigned for WLC management. See **Table (5.3)**.

Name	IP Address	Subnet Mask
WLC	192.168.6.2	255.255.255.248
WLC-PC	192.168.6.3	255.255.255.248

Table (5.3): Static IP Addresses for WLC Management

IP addresses are assigned between the core routers and multilayer switches. See **Table (5.4)**.

Name	Interface	IP Address	Subnet Mask
HQ-MLS1	GigabitEthernet1/0/1	10.0.0.1	255.255.255.252
HQ-MLS1	GigabitEthernet1/0/2	10.0.0.5	255.255.255.252
HQ-MLS2	GigabitEthernet1/0/1	10.0.0.9	255.255.255.252
HQ-MLS2	GigabitEthernet1/0/2	10.0.0.13	255.255.255.252
HQ-R1	GigabitEthernet0/0	10.0.0.2	255.255.255.252
HQ-R1	GigabitEthernet0/1	10.0.0.10	255.255.255.252
HQ-R2	GigabitEthernet0/0	10.0.0.6	255.255.255.252
HQ-R2	GigabitEthernet0/1	10.0.0.14	255.255.255.252

Table (5.4): IP Addresses Between the Core Routers and Multilayer Switches

IP addresses are assigned between the core routers and the ISP routers. See **Table (5.5)**.

Name	Interface	Network Address	Subnet Mask
HQ-R1	Se0/2/0	190.200.100.1	255.255.255.252
HQ-R1	Se0/2/1	190.200.100.5	255.255.255.252
HQ-R2	Se0/2/0	190.200.100.13	255.255.255.252
HQ-R2	Se0/2/1	190.200.100.9	255.255.255.252
ISP-R1	Se0/2/0	190.200.100.2	255.255.255.252
ISP-R1	Se0/2/1	190.200.100.10	255.255.255.252
ISP-R2	Se0/2/0	190.200.100.14	255.255.255.252
ISP-R2	Se0/2/1	190.200.100.6	255.255.255.252

Table (5.5): IP Addresses Between the Core Routers and ISPs

The types of network cables installed are shown in **Table (5.6)**.

Area	Cable Type
Between ISPs and Core Routers	Serial DCE
Between Core Routers and Multilayer Switches	Copper Straight-Through
Between Multilayer Switches and Access Layer Switches	Copper Cross-Over
Between Access Layer Switches and End Devices (Servers, PCs, Printers)	Copper Straight-Through
Between Access Layer Switch and Wireless LAN Controller	Copper Cross-Over

Table (5.6): Network Cable Types Installation

4.2.2. Initial Configuration on Network Devices

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname HQ-R1
```

Figure (5.2): Initial Configuration in Cisco Router

In **Figure (5.2)**, the initial configuration is made in the Cisco network devices. First, enable privileged mode, then enter global configuration mode. After that, assign hostnames to the network devices. Every network device has to be assigned host names.

4.2.3. Initial Security Configuration

```
HQ-R1(config)#enable password cisco
HQ-R1(config)#line console 0
HQ-R1(config-line)#password cisco
HQ-R1(config-line)#login
HQ-R1(config-line)#exit
HQ-R1(config)#banner motd #NO UNAUTHORISED ACCESS!!!#
HQ-R1(config)#no ip domain-lookup
HQ-R1(config)#service password-encryption
```

Figure (5.3): Configuration for Authenticity in Cisco Router

In **Figure (5.3)**, configure the enable password for both privileged access and the console port on Cisco network devices. Next, provide a login banner message warning against unauthorized access. Then, block unnecessary DNS lookups and encrypt the stored passwords. This security configuration needs to be configured on L2, and L3 switches and routers.

4.2.4. SSH Configuration on Multilayer Switches and Routers

```
HQ-R1(config)#username cisco password cisco
HQ-R1(config)#ip domain-name cisco.com
HQ-R1(config)#crypto key generate rsa
The name for the keys will be: HQ-R1.cisco.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

HQ-R1(config)#ip ssh version 2
*Mar 1 0:4:48.207: %SSH-5-ENABLED: SSH 1.99 has been enabled
HQ-R1(config)#line vty 0 15
HQ-R1(config-line)#login local
HQ-R1(config-line)#transport input ssh
HQ-R1(config-line)#exit
```

Figure (5.4): SSH Configuration on Router

In **Figure (5.4)**, first, a local user account and password are set, and then the domain name for the device is set to 'cisco.com'. Next, 1024-bit RSA keys are created for secure encryption. Then, SSH version 2, which is more secure than version 1, is enabled. After that, local logins on VTY lines 0-15 are allowed. Finally, SSH connections are established for logins. SSH is configured in all L3 switches and routers.

4.2.5. Standard ACL Configuration for SSH

```
HQ-MLS1(config)#access-list 10 permit 192.168.4.0 0.0.0.255
HQ-MLS1(config)#access-list 10 deny any
HQ-MLS1(config)#line vty 0 15
HQ-MLS1(config-line)#access-class 10 in
HQ-MLS1(config-line)#exit
```

Figure (5.5): Standard ACL Configuration for SSH

In **Figure (5.5)**, an ACL is created to permit access from the 192.168.4.0/24 network, which corresponds to Department 4, D4. Except for IPs from D4, access to SSH from any other IP address is denied. Incoming connections on Virtual Terminal Lines (VTY) 0 to 15 are commonly used for SSH access.

4.2.6. Creating VLAN on Layer 2 Switches

```
D1-SW(config)#vlan 10
D1-SW(config-vlan)#name D1
D1-SW(config-vlan)#exit
```

Figure (5.6): Creating VLAN on D1-SW

In **Figure (5.6)**, VLAN 10 is created and named D1 in the L2 switch from department 1, D1-SW after that trunk ports and access ports will be configured as in **Figure (5.7)**.

```
D1-SW(config)#int range fa0/1-2
D1-SW(config-if-range)#switchport mode trunk
D1-SW(config-if-range)#exit
D1-SW(config)#int range fa0/3-24
D1-SW(config-if-range)#switchport mode access
D1-SW(config-if-range)#switchport access vlan 10
D1-SW(config-if-range)#exit
```

Figure (5.7): Configuring Trunk Ports and Access Ports

In **Figure (5.7)**, interfaces fa0/1 and fa0/2, which are connected to the multilayer switch, will be configured as trunk ports to carry VLAN information. After that, the remaining ports to LAN will be configured as access ports and added to VLAN 10.

```
D1-SW(config)#do sh vlan
```

VLAN	Name	Status	Ports
1	default	active	Gig0/1, Gig0/2
10	D1	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Figure (5.8): Created VLAN 10

In **Figure (5.8)**, interfaces from Fa0/3 to Fa0/24 are configured as VLAN 10 access ports and are active. VLAN 20, 30, 40, 50, and 60 are configured the same on D2-SW, D3-SW, D4-SW, SEV-SW, and WLC-SW.

4.2.7. IP Addressing on Multilayer Switches

```
HQ-MLS1(config)#interface GigabitEthernet1/0/1
HQ-MLS1(config-if)#no switchport
HQ-MLS1(config-if)#ip address 10.0.0.1 255.255.255.252
```

Figure (5.9): IP Assigning on Routed Interface G1/0/1 of HQ-MLS1

In **Figure (5.9)**, a multilayer switch can perform both switching and routing functions. To operate as a routed interface, interface g1/0/1 must have the 'no switchport' command applied so that an IP address can be assigned to that interface. All the routed interfaces on both L3 switches, HQ-MLS1 and HQ-MLS2, are assigned IP addresses as in the previous **Table (5.4)**.

4.2.8. Inter-VLAN Routing Configuration on Multilayer Switch

```
HQ-MLS1(config)#ip routing
HQ-MLS1(config)#interface vlan 10
HQ-MLS1(config-if)#ip add 192.168.1.1 255.255.255.0
HQ-MLS1(config-if)#exit
```

Figure (5.10): Configuring Inter-VLAN Routing on HQ-MLS1

In **Figure (5.10)**, to perform Inter-VLAN routing, a multilayer switch uses a Switch Virtual Interface (SVI). First, routing functionality must be enabled using the command "ip routing". After that, an IP address, 192.168.1.1, and a subnet mask, 255.255.255.0 are assigned to the VLAN 10 SVI. Respective IP addresses are assigned in other VLAN 20, 30, 40, 50, and 60 SVIs on both L3 switches, HQ-MLS1 and HQ-MLS2.

4.2.9. Creating EtherChannel Between Multilayer Switches

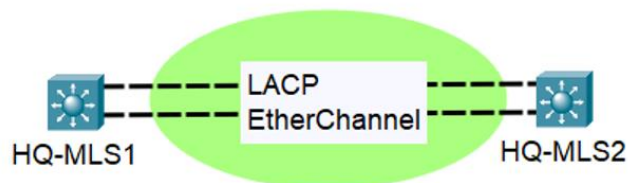


Figure (5.11): LACP EtherChannel

In **Figure (5.11)**, LACP EtherChannel is configured between two multilayer switches, HQ-MLS1 and HQ-MLS2, to aggregate multiple physical links. This enhances bandwidth and provides redundancy for high availability in the network.

```
HQ-MLS1(config-if)#interface range g1/0/8-9
HQ-MLS1(config-if-range)#channel-group 1 mode active
HQ-MLS1(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/8,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/8,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/9,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/9,
changed state to up

HQ-MLS1(config-if-range)#interface port-channel 1
HQ-MLS1(config-if)#switchport mode trunk
HQ-MLS1(config-if)#exit
```

Figure (5.12): Creating LACP EtherChannel by Aggregating G1/0/8 and G1/0/9

In **Figure (5.12)**, EtherChannel is created by aggregating the two Interfaces g1/0/9 and g1/0/9. First, set the channel-group number to 1 and mode to active to allow both interfaces to transmit and receive traffic. Then, configure that port-channel 1 interface as a trunk link to carry multiple VLANs.

4.2.10. OSPF Configuration on L3 Switches, Core and ISP Routers

```
HQ-MLS1(config)#router ospf 10
HQ-MLS1(config-router)#router-id 1.1.1.1
HQ-MLS1(config-router)#network 10.0.0.0 0.0.0.3 area 0
HQ-MLS1(config-router)#network 10.0.0.4 0.0.0.3 area 0
HQ-MLS1(config-router)#network 10.0.0.8 0.0.0.3 area 0
HQ-MLS1(config-router)#network 10.0.0.12 0.0.0.3 area 0
HQ-MLS1(config-router)#network 192.168.1.0 0.0.0.255 area 0
HQ-MLS1(config-router)#network 192.168.2.0 0.0.0.255 area 0
HQ-MLS1(config-router)#network 192.168.3.0 0.0.0.255 area 0
HQ-MLS1(config-router)#network 192.168.4.0 0.0.0.255 area 0
HQ-MLS1(config-router)#network 192.168.5.0 0.0.0.15 area 0
HQ-MLS1(config-router)#network 192.168.6.0 0.0.0.7 area 0
HQ-MLS1(config-router)#exit
```

Figure (5.13): OSPF configuration on HQ-MLS1

In **Figure (5.13)**, first, process ID 10 is created, followed by assigning a router ID of 1.1.1.1 to HQ-MLS1. Then, networks connected to routers and LANs are advertised, enabling participation in routing within area 0. The same configuration is made on HQ-MLS2 with router-id 2.2.2.2. HQ-R1 and R2, ISP-R1 and R2 will configure respective router-id and OSPF network.

4.2.11. DHCP Server Configuration

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: D1Pool

Default Gateway: 192.168.1.1

DNS Server: 192.168.5.3

Start IP Address : 192 168 1 2

Subnet Mask: 255 255 255 0

Maximum Number of Users : 254

TFTP Server: 0.0.0.0

WLC Address: 192.168.6.2

Buttons: Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
D3Pool	192.168.3.1	192.168.5.3	192.168.3.2	255.255.255.0	254	0.0.0.0	192.168.6.2
D1Pool	192.168.1.1	192.168.5.3	192.168.1.2	255.255.255.0	254	0.0.0.0	192.168.6.2
D2Pool	192.168.2.1	192.168.5.3	192.168.2.2	255.255.255.0	254	0.0.0.0	192.168.6.2
D4Pool	192.168.4.1	192.168.5.3	192.168.4.2	255.255.255.0	254	0.0.0.0	192.168.6.2
serverPool	0.0.0.0	0.0.0.0	0.0.0.0	255.255.255.0	0	0.0.0.0	0.0.0.0

Figure (5.14): Creating Pools on the DHCP Server

In **Figure (5.14)**, the created DHCP pools are displayed. Initially, the DHCP service is enabled. Then, pools are created by assigning a pool name. After that, the default gateway and DNS server IP addresses are configured. Subsequently, the usable IP address range and maximum number of users are defined. Finally, the WLC address is added for wireless connections.

4.2.12. Port Security Configuration on Server Switch

```
SEV-SW(config)#int range fa0/3-6
SEV-SW(config-if-range)#switchport port-security maximum 1
SEV-SW(config-if-range)#switchport port-security mac-address sticky
SEV-SW(config-if-range)#switchport port-security violation shutdown
SEV-SW(config-if-range)#exit
```

Figure (5.15): Port Security Configuration on SEV-SW

In **Figure (5.15)**, the ports connected to all servers are configured as follows settings. Only one MAC address is allowed to be learned and communicated through each interface. Any additional attempts to connect to the interface will be blocked until the existing MAC address is removed. Additionally, the switch will dynamically learn the MAC address, and that address will become the secure sticky address. Only authorized devices with the specific MAC address will be allowed access to the port. Furthermore, the switch is configured to shut down the port when a violation occurs automatically. All unused ports on the switch are configured to be shut down. See **Figure (5.16)**.

```
SEV-SW(config)#int range fa0/7-24, g0/1-2
SEV-SW(config-if-range)#shutdown
```

Figure (5.16): Shutting Down Unused Ports on SEV-SW

4.2.13. HSRP Configuration on Multilayer Switches

```
HQ-MLS1(config)#int vlan 10
HQ-MLS1(config-if)#standby 10 ip 192.168.1.1
HQ-MLS1(config-if)#standby 10 priority 110
HQ-MLS1(config-if)#standby 10 preempt
HQ-MLS1(config-if)#exit
```

Figure (5.17): HSRP Configuration on HQ-MLS1

In **Figure (5.17)**, HSRP will be configured on both HQ-MLS1 and HQ-MLS2. HQ-MLS1 will be in the active state, while HQ-MLS2 will be in the standby state. First, on VLAN 10, a standby group with group number 10 and a virtual IP address within VLAN 10 is created to configure this.

Next, the priority is set to 110. Finally, preemptive mode is enabled to allow HQ-MLS1 to perform as the active switch.

```
HQ-MLS1(config)#do sh standby br
P indicates configured to preempt.
|
Interface    Grp  Pri P State    Active        Standby        Virtual IP
Vl10         10   110 P Active    local         192.168.1.1   192.168.1.1
Vl20         20   110 P Active    local         192.168.2.1   192.168.2.1
Vl30         30   110 P Active    local         192.168.3.1   192.168.3.1
Vl40         40   110 P Active    local         192.168.4.1   192.168.4.1
Vl50         50   110 P Active    local         192.168.5.1   192.168.5.1
Vl60         60   110 P Active    local         192.168.6.1   192.168.6.1
```

Figure (5.18): HSRP Active State on HQ-MLS1

In **Figure (5.18)**, after HSRP configuration on HQ-MLS1, it will be in the active state, while HQ-MLS2 will be on standby. This is because of the priority setting of 110 on HQ-MLS1, which is higher than that of HQ-MLS2.

```
HQ-MLS2(config)#int vlan 10
HQ-MLS2(config-if)#standby 10 ip 192.168.1.1
HQ-MLS2(config-if)#standby 10 priority 100
HQ-MLS2(config-if)#standby 10 preempt
HQ-MLS2(config-if)#exit
```

Figure (5.19): HSRP Configuration on HQ-MLS2

In **Figure (5.19)**, on HQ-MLS2, a standby group with the same group number as HQ-MLS1, which is 10, and the same virtual IP address within VLAN 10 is created. Next, the priority is set to 100, which is lower than HQ-MLS1's priority. Finally, the preemptive mode is enabled to allow HQ-MLS2 to take over as the active switch if HQ-MLS1 fails.

```
HQ-MLS2(config)#do sh standby br
P indicates configured to preempt.
|
Interface    Grp  Pri P State    Active        Standby        Virtual IP
Vl10         10   100 P Standby   192.168.1.1   local         192.168.1.1
Vl20         20   100 P Standby   192.168.2.1   local         192.168.2.1
Vl30         30   100 P Standby   192.168.3.1   local         192.168.3.1
Vl40         40   100 P Standby   192.168.4.1   local         192.168.4.1
Vl50         50   100 P Standby   192.168.5.1   local         192.168.5.1
Vl60         60   100 P Standby   192.168.6.1   local         192.168.6.1
```

Figure (5.20): HSRP Standby State on HQ-MLS2

In **Figure (5.20)**, after HSRP configuration on HQ-MLS2, it will be in the standby state, while HQ-MLS1 is already in the active state. This is because of the priority setting of 100 on HQ-MLS2, which is lower than that of HQ-MLS1.

4.2.14. Enabling STP PortFast and BPDU Guard on All Access Ports

```
D1-SW(config)#int range fa0/3-6
D1-SW(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/3 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
```

Figure (5.21): Enabling STP PortFast on All Access Ports

In **Figure (5.21)**, the access ports on all Layer 2 switches will first be configured with Spanning Tree PortFast. This feature cannot be enabled on trunking interfaces. It reduces delays by immediately transitioning access ports into the forwarding state.

```
D1-SW(config-if-range)#spanning-tree bpduguard enable
D1-SW(config-if-range)#exit
```

Figure (5.22): Enabling STP BPDU Guard on All Access Ports

In **Figure (5.22)**, after enabling STP PortFast, STP BPDU Guard will also be enabled. It prevents misconfigured switches from causing network problems by disabling ports when receiving unexpected BPDUs, maintaining network stability.

4.2.15. Configuring NAT ACL

```
HQ-R1(config)#interface range g0/0-1
HQ-R1(config-if-range)#ip nat inside
HQ-R1(config-if-range)#exit
HQ-R1(config)#interface se0/2/0
HQ-R1(config-if)#ip nat outside
HQ-R1(config-if)#interface se0/2/1
HQ-R1(config-if)#ip nat outside
HQ-R1(config-if)#exit
```

Figure (5.23): Configuring NAT Inside and Outside

In **Figure (5.23)**, the interfaces connected to the LAN are configured as NAT inside, translating multiple private IP addresses to a single public IP address. Conversely, the interfaces connected to the external network are configured as NAT outside, translating the single public IP address to multiple private IP addresses.

```
HQ-R1(config)#access-list 50 permit 192.168.1.0 0.0.0.255
HQ-R1(config)#access-list 50 permit 192.168.2.0 0.0.0.255
HQ-R1(config)#access-list 50 permit 192.168.3.0 0.0.0.255
HQ-R1(config)#access-list 50 permit 192.168.4.0 0.0.0.255
HQ-R1(config)#access-list 50 permit 192.168.5.0 0.0.0.15
HQ-R1(config)#access-list 50 permit 192.168.6.0 0.0.0.7
HQ-R1(config)#ip nat inside source list 50 interface se0/2/0 overload
HQ-R1(config)#ip nat inside source list 50 interface se0/2/1 overload
```

Figure (5.24): Configuring ACL for NAT and PAT

In **Figure (5.24)**, an access list numbered 50 permits traffic from all LANs, allowing NAT translation for outgoing traffic. PAT is then enabled, translating addresses from access list 50 to the public IP addresses assigned to serial interfaces 0/2/0 and 0/2/1.

4.2.16. Wireless LAN Controller Configuration

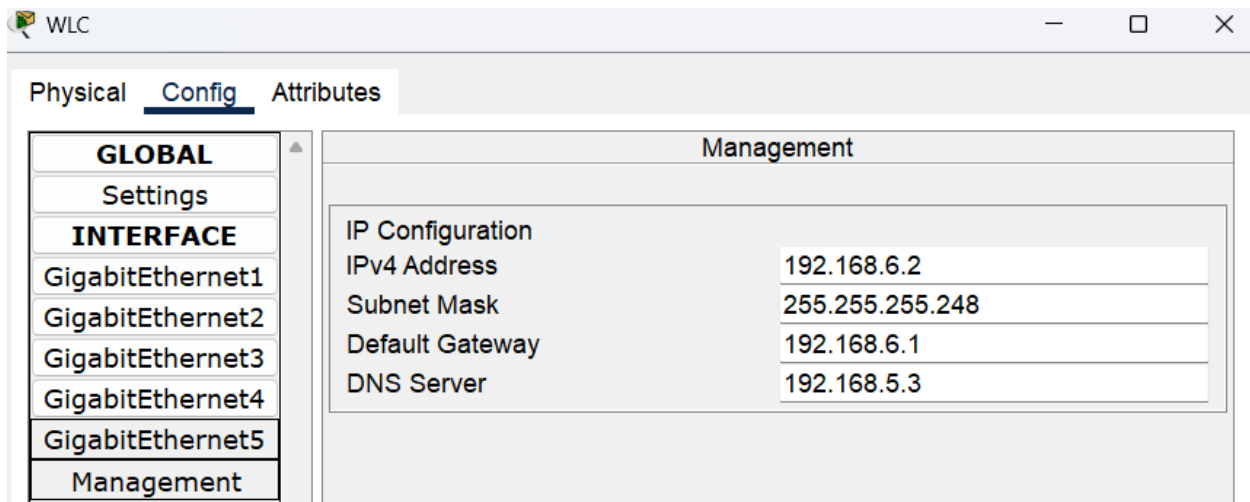


Figure (5.25): IP Configuration on WLC Management

In **Figure (5.25)**, first, the Wireless LAN Controller (WLC) is assigned a static IP address of 192.168.6.2/29. Then, the default gateway and DNS server addresses are configured.

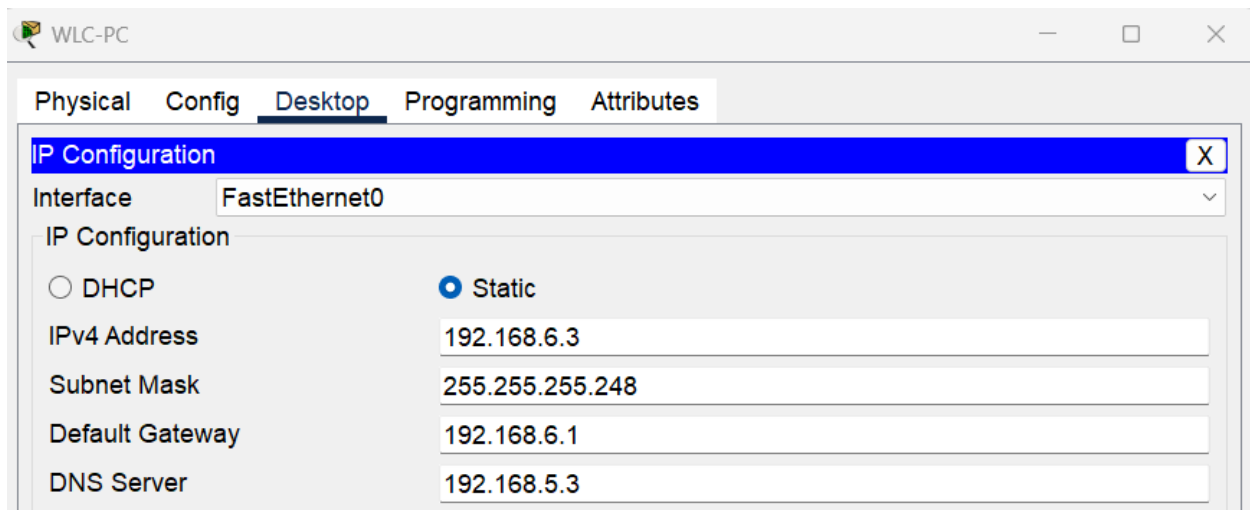


Figure (5.26): IP Configuration on WLC-PC

In **Figure (5.26)**, after configuring the IP address on the WLC, the WLC-PC is assigned a static IP address of 192.168.6.3/29. Then, the default gateway and DNS server addresses are configured.

The image displays two side-by-side screenshots from a Cisco 3500 Series Wireless LAN Controller (WLC) configuration interface. The left screenshot shows the 'Web Browser' window with the URL `http://192.168.6.2`. The page title is 'Cisco 3500 Series Wireless LAN Controller'. It features a blue background with a Cisco logo and a welcome message: 'Welcome! Please start by creating an admin account.' Below this, there are three input fields: 'Admin' (username), a password field (masked with asterisks), and another password field (masked with asterisks). A 'Start' button is at the bottom. The right screenshot shows the 'Config' tab with various system settings. The 'System Name' is 'WLAN'. The 'Country' is 'United States (US)'. The 'Date & Time' is '02/08/2024' and '22:19:49'. The 'Timezone' is 'Rangoon'. The 'NTP Server' is '(optional)'. The 'Management IP Address' is '192.168.6.2'. The 'Subnet Mask' is '255.255.255.248'. The 'Default Gateway' is '192.168.6.1'. The 'Management VLAN ID' is '0'.

System Name	WLAN
Country	United States (US)
Date & Time	02/08/2024 22:19:49
Timezone	Rangoon
NTP Server	(optional)
Management IP Address	192.168.6.2
Subnet Mask	255.255.255.248
Default Gateway	192.168.6.1
Management VLAN ID	0

Figure (5.27): Creating Admin Account and Setting Up Controller

In **Figure (5.27)**, after configuring the IP address on the WLC-PC, an admin account is created in the web browser for the WLC. The username and password must be entered whenever logging into the WLC. After that, the required management name and IP address are registered.

The figure consists of two side-by-side screenshots of the Cisco 3500 Series Wireless LAN Controller setup wizard.

The left screenshot shows the 'Employee Network' configuration page. It features a green toggle for 'Employee Network' and a grey toggle for 'Guest Network'. The configuration fields include:

- Network Name: D1
- Security: WPA2 Personal
- Passphrase: (masked with dots)
- Confirm Passphrase: (masked with dots)
- VLAN: Management VLAN
- DHCP Server Address: 0.0.0.0 (optional)

The right screenshot shows the 'Advanced Setting' page. It features a toggle for 'RF Parameter Optimization' (disabled). Below it are fields for:

- Virtual IP Address: 192.0.2.1
- Local Mobility Group: Default

 At the bottom are 'Back' and 'Next' buttons.

Figure (5.28): Creating the First Wireless Network and Completing the Setup

In **Figure (5.28)**, next, the first wireless network is created by specifying the network name, and security type of WPA2 Personal, and creating a password. Then, a virtual IP address is assigned to complete the WLC setup.

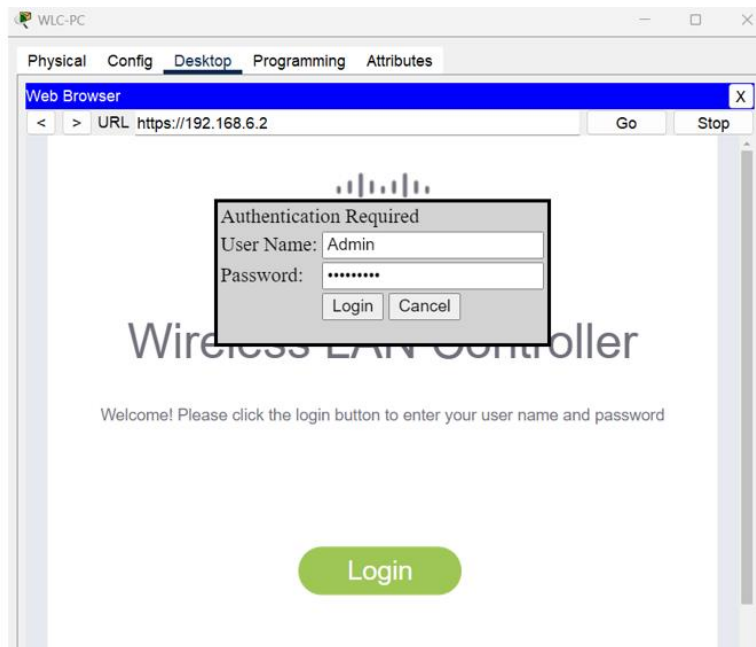


Figure (5.29): Accessing into WLC

In **Figure (5.29)**, after setting up the WLC, WLC-PC could use the created admin account to access the WLC and further configuration will be followed.

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
D1	10	192.168.1.2	Dynamic	Disabled	
D2	20	192.168.2.2	Dynamic	Disabled	
D3	30	192.168.3.2	Dynamic	Disabled	
D4	40	192.168.4.2	Dynamic	Disabled	
management	untagged	192.168.6.2	Static	Enabled	::128
virtual	N/A	192.0.2.1	Static	Not Supported	

Figure (5.30): Configuring VLANs for Interfaces of APs from D1, D2, D3, and D4

In **Figure (5.30)**, VLANs must be configured for access points from D1, D2, D3, and D4. VLAN 10 is assigned to D1-AP, VLAN 20 to D2-AP, VLAN 30 to D3-AP, and VLAN 40 to D4-AP. Each VLAN is assigned an appropriate IP address, and the IP address of the DHCP server is added. Also, each link from the department switch to each Access Point is configured as a trunk link to carry VLAN.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	D1	D1	Enabled	[WPA2][Auth(PSK)]
2	WLAN	D2	D2	Enabled	[WPA2][Auth(PSK)]
3	WLAN	D3	D3	Enabled	[WPA2][Auth(PSK)]
4	WLAN	D4	D4	Enabled	[WPA2][Auth(PSK)]

Figure (5.31): Creating WLANs

In **Figure (5.31)**, WLANs for D1, D2, D3, and D4 are configured by assigning SSID, VLAN ID, and WPA2 security with a Pre-Shared Key (PSK).

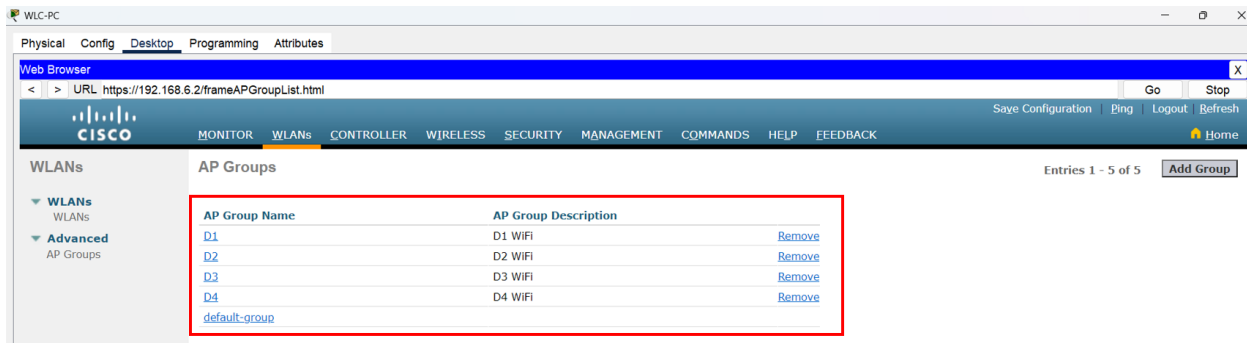


Figure (5.32): Adding AP Groups

In **Figure (5.32)**, next, each access point (AP) is assigned to its corresponding departmental group, such as D1-AP in the D1 AP group. Wireless devices from specific departments can only connect to their designated AP using the appropriate SSID and PSK. For example, laptops and mobile phones from D1 can connect to D1-AP by entering the correct SSID and PSK.

4.2.17. Setting Up DNS Server

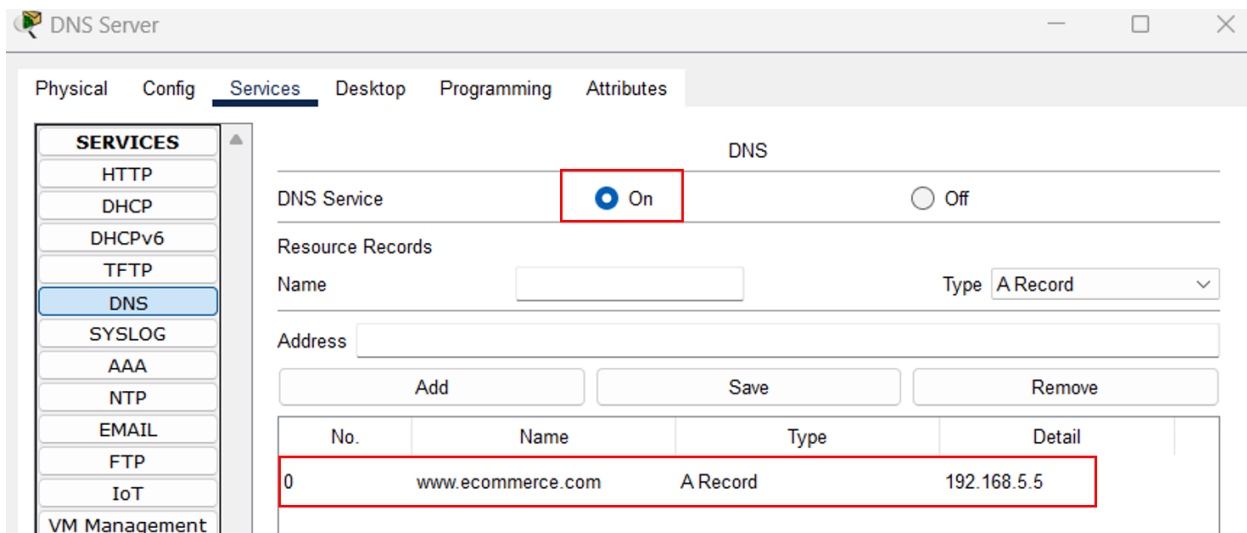


Figure (5.33): Setting Up DNS Server

In **Figure (5.33)**, in the DNS server, the DNS service is first enabled, and then an organizational website is created. In the figure, an example website named www.ecommerce.com is created by assigning the IP address 192.168.5.5.

4.2.18. Setting Up WEB Server

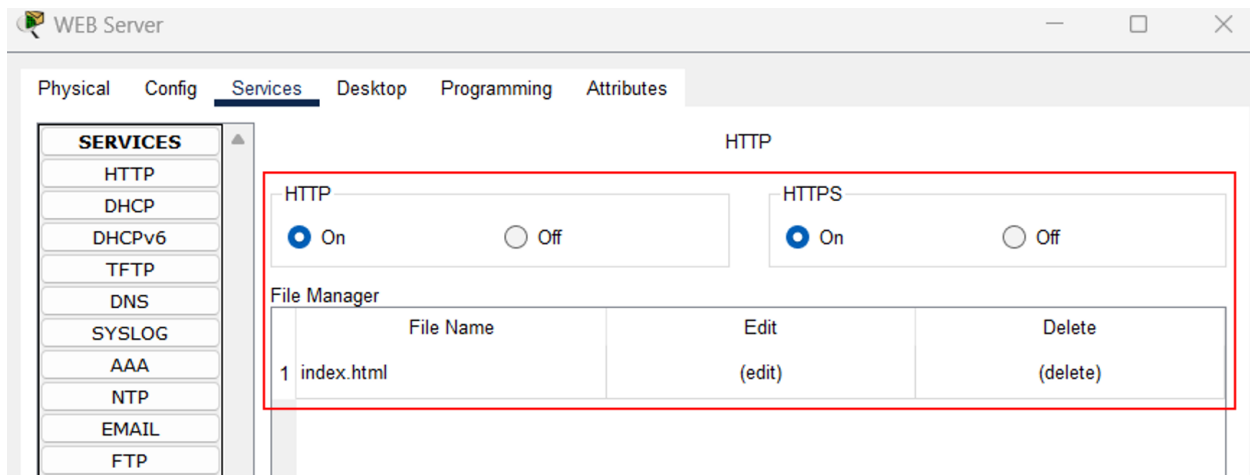


Figure (5.34): Setting Up WEB Server

In **Figure (5.34)**, first, the HTTP and HTTPS services are enabled, and then the HTTP file for the website is created in the web server.

4.2.19. Setting Up EMAIL Server

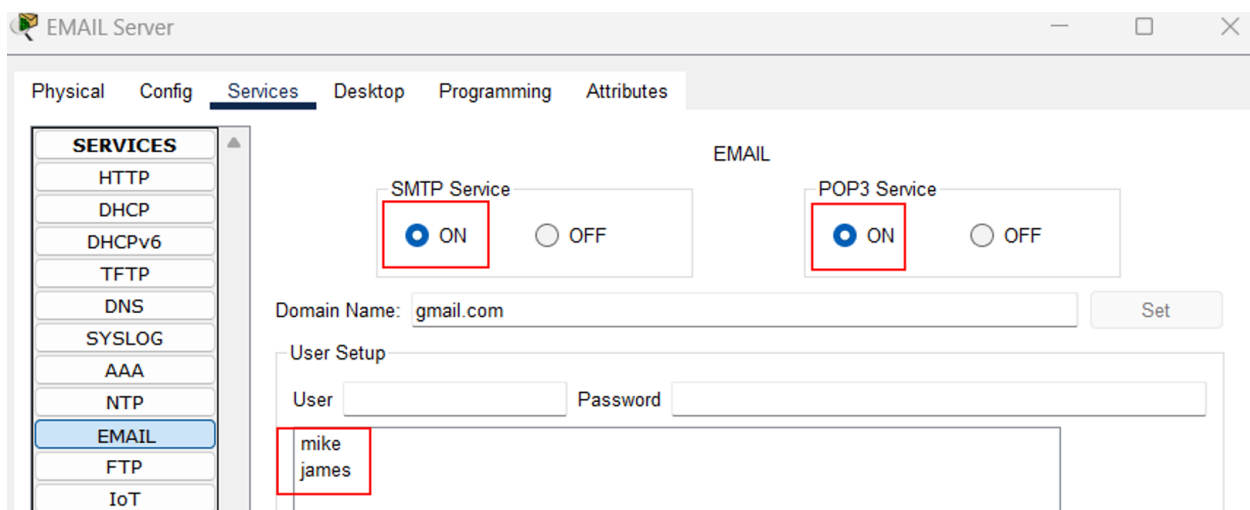


Figure (5.35): Setting Up EMAIL Server

In **Figure (5.35)**, SMTP and POP3 services are enabled in the EMAIL server. The domain name "gmail.com" is provided as an example. Then, two users and passwords are created.

D1-Laptop

Physical Config **Desktop** Programming Attributes

Configure Mail X

User Information

Your Name: Mike

Email Address: mike@gmail.com

Server Information

Incoming Mail Server: 192.168.5.4

Outgoing Mail Server: 192.168.5.4

Logon Information

User Name: mike

Password: ****

Save Remove Clear Reset

Figure (5.36): Configuring Mail on D1-Laptop

In **Figure (5.36)**, after setting up the EMAIL server, the created email address from the EMAIL server is added, along with the name. Then, incoming and outgoing mail server IP addresses, and login information are configured on D1-Laptop and D2-Laptop.

4.3. Testing and Evaluation

Testing ensures that every aspect of the hierarchical design functions correctly, addressing any issues and ensuring the design's reliability in reflecting real-world scenarios.

4.3.1. Password Testing

```
NO UNAUTHORISED ACCESS!!!

User Access Verification

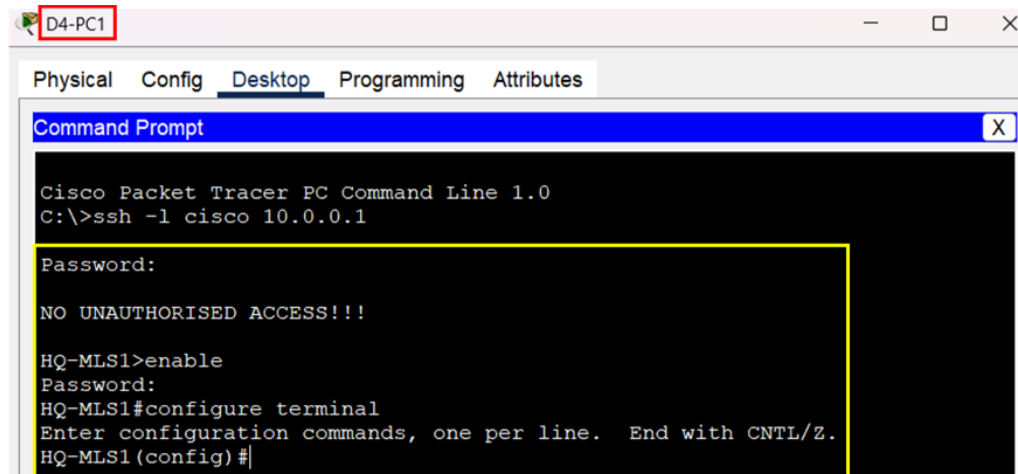
Password:

HQ-R1>enable
Password:
HQ-R1#|
```

Figure (5.37): Result of Initial Security Configuration

In **Figure (5.37)**, when accessing the Cisco network devices, a login banner will be displayed, requesting the password to access the device twice: once for privileged access and once for console port access. Once the correct password is entered, access to the network device is granted.

4.3.2. Testing Secure Remote Access for Only PCs from D4



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l cisco 10.0.0.1

Password:

NO UNAUTHORISED ACCESS!!!

HQ-MLS1>enable
Password:
HQ-MLS1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
HQ-MLS1(config)#
```

Figure (5.38): Secure Remote Access to the Multilayer Switch from D4-PC1

In **Figure (5.38)**, PC1 from Department 4, D4, can remotely access the multilayer switch by entering commands from the command prompt. It requests a password for access, ensuring

user authenticity. Only D4 is authorized for remote access. Devices from D1, D2, and D3 are not authorized for remote access.

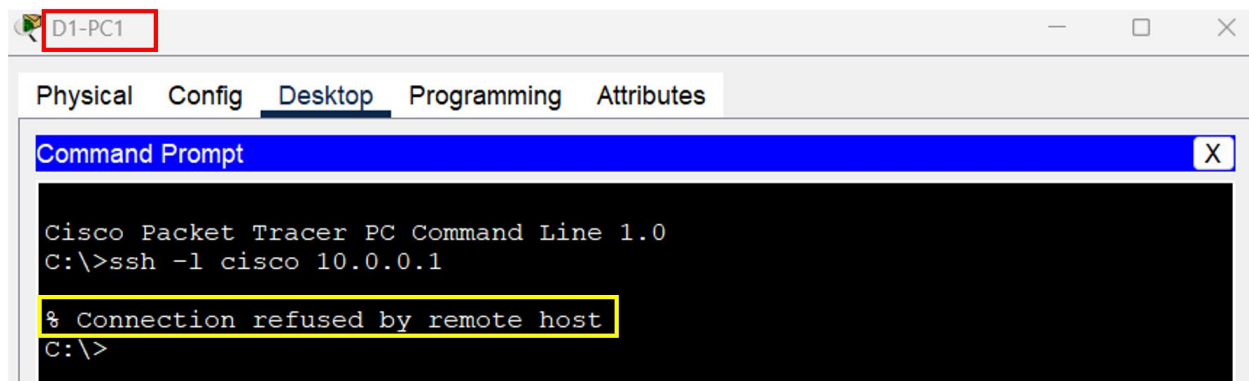


Figure (5.39): Rejection of Remote Access from D1-PC1 to the Multilayer Switch

In **Figure (5.39)**, when a PC from Department 1, D1-PC1, tries to access the multilayer switch remotely, the remote host will reject that connection.

4.3.3. Testing DHCP Requests Provided by the DHCP Server

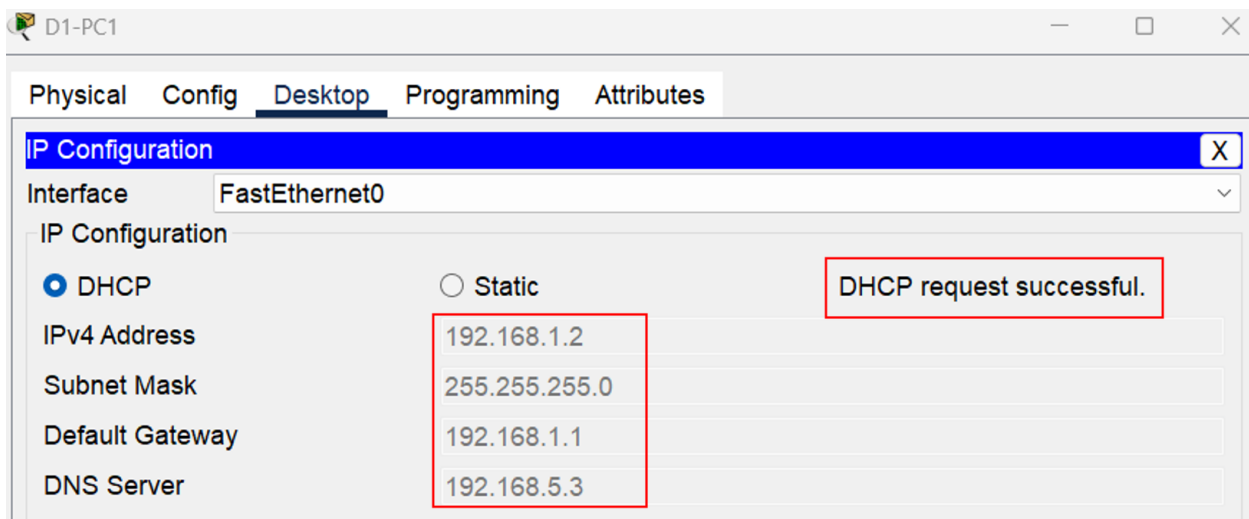


Figure (5.40): Successful DHCP Request from D1-PC1

In **Figure (5.40)**, after configuring DHCP for all departments, devices such as PCs, printers, and access points from any department can choose IP configuration as DHCP to automatically obtain an IP address from the DHCP Server. In the figure, the DHCP request from PC1 in D1 is successful and the IPv4 address within the correct IP range is displayed.

4.3.4. Testing Wi-Fi Functionality

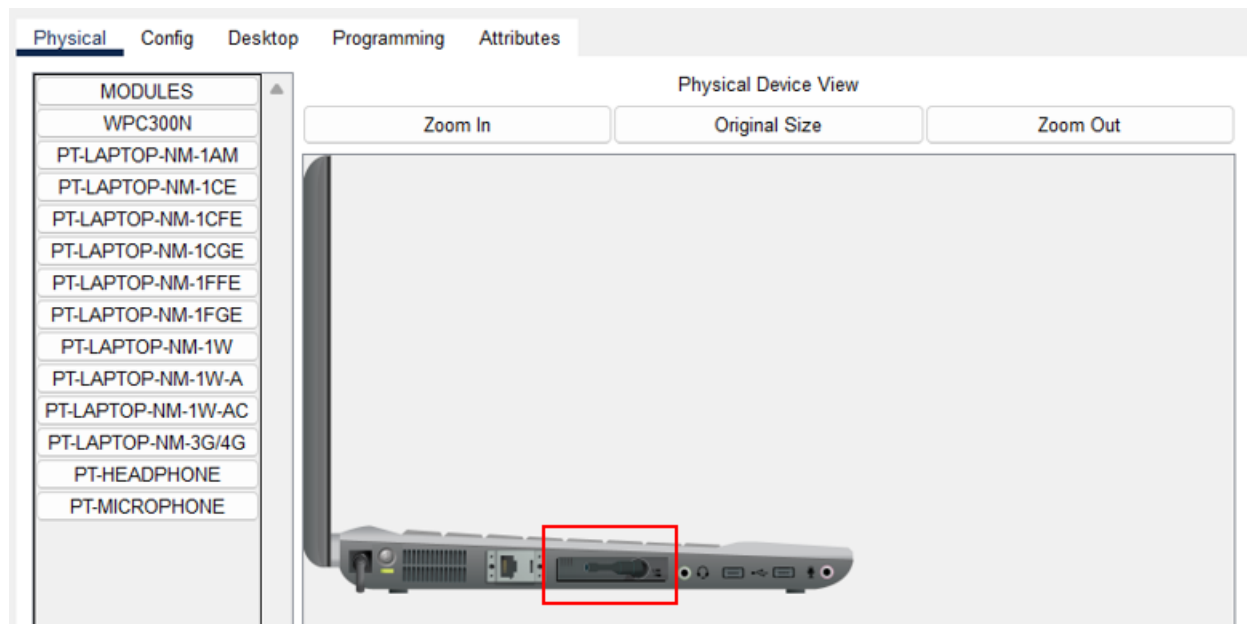


Figure (5.41): Adding WPC300N Module to all Laptops

In **Figure (5.41)**, the WPC300N is a wireless network adapter designed for laptops, enabling wireless connectivity to Wi-Fi networks. First, the laptop must be powered off. Then, the WPC300N module is added to the laptop. Finally, the laptop is powered on again.

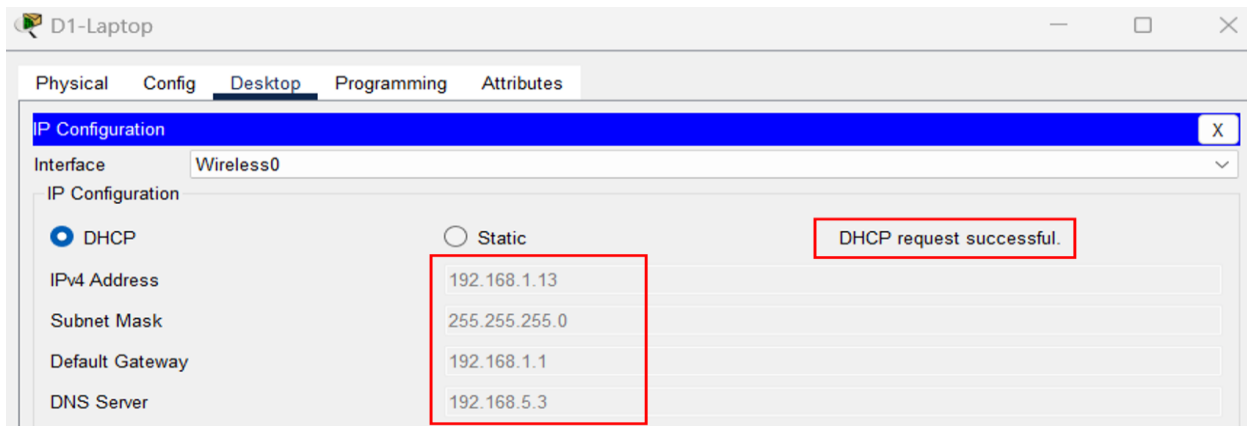


Figure (5.42): Successful DHCP Request of D1-Laptop

In **Figure (5.42)**, next, enable the DHCP option on the D1-Laptop to obtain an IPv4 address from the DHCP server. Upon a successful DHCP request, a message confirming a successful connection is displayed. Finally, the D1-Laptop is successfully connected to the Wi-Fi Network of D1-AP.

4.3.5. Testing the DNS and WEB Servers Via Wi-Fi

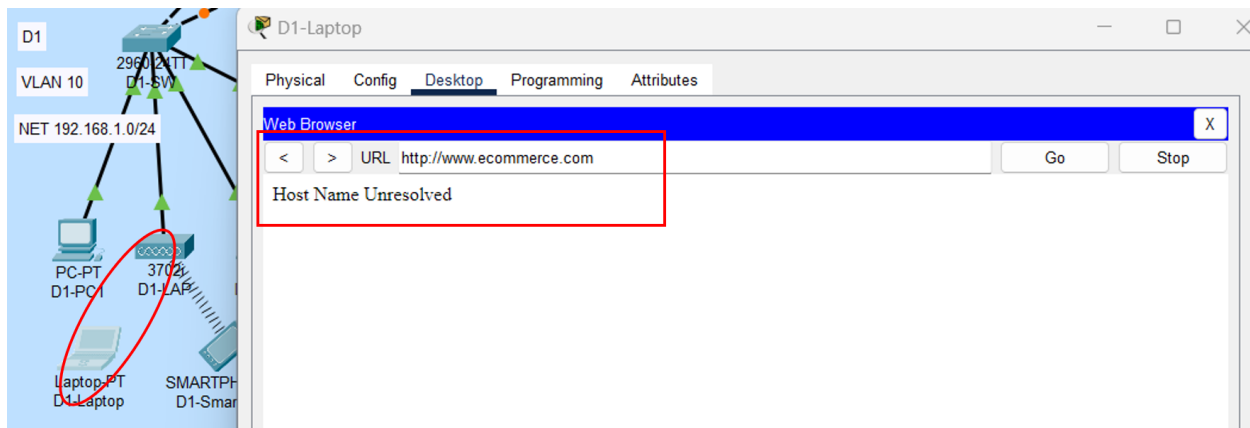


Figure (5.43): No Wireless Connection of D1-Laptop

In **Figure (5.43)**, after setting up the DNS and WEB servers, attempting to visit the created website is made. However, when the D1-Laptop is not connected to Wi-Fi, it cannot browse websites through the web browser.

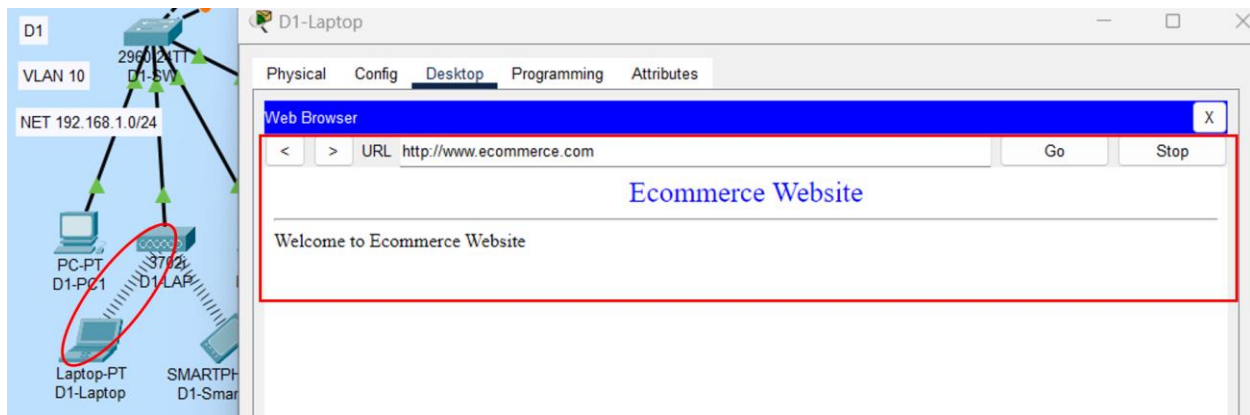


Figure (5.44): After D1-Laptop Connects to the D1-AP

In **Figure (5.44)**, after the D1-Laptop connects to the D1-AP by selecting DHCP and entering the SSID and PSK, it can browse the created website through the web browser.

4.3.6. Testing EMAIL Server by Sending Mails

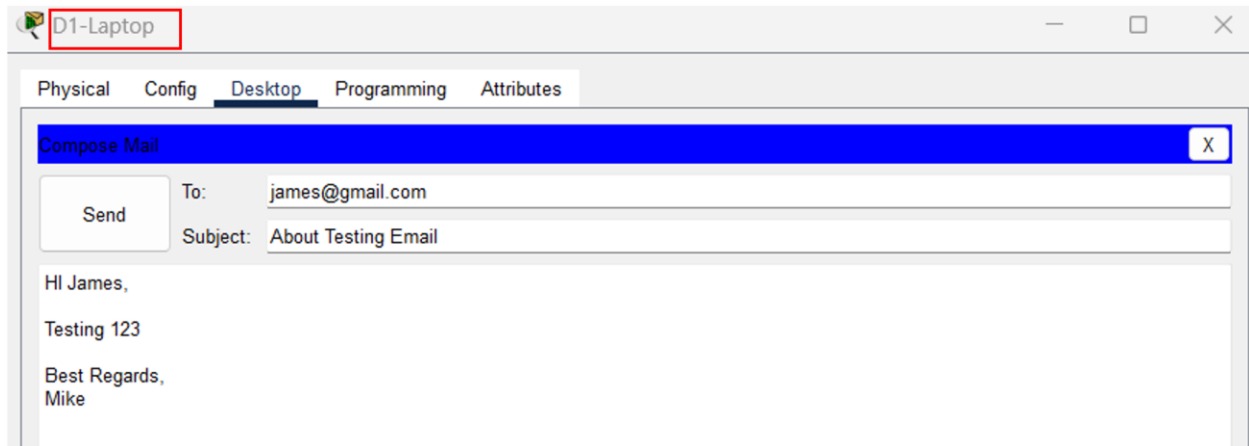


Figure (5.45): Composing Mail from D1-Laptop

In **Figure (5.45)**, next, send an email from D1-Laptop, which has the email address mike@gmail.com, to D2-Laptop's email address, which is james@gmail.com.

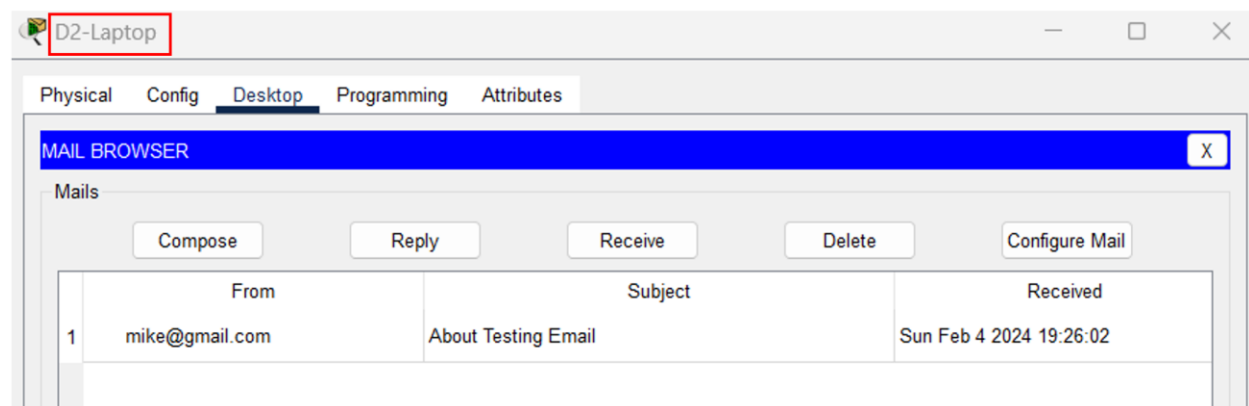


Figure (5.46): D2-Laptop's Received Mail

In **Figure (5.46)**, after sending the email, check the mail browser on D2-Laptop, where an email from mike@gmail.com will be waiting.

4.3.7. Testing HSRP

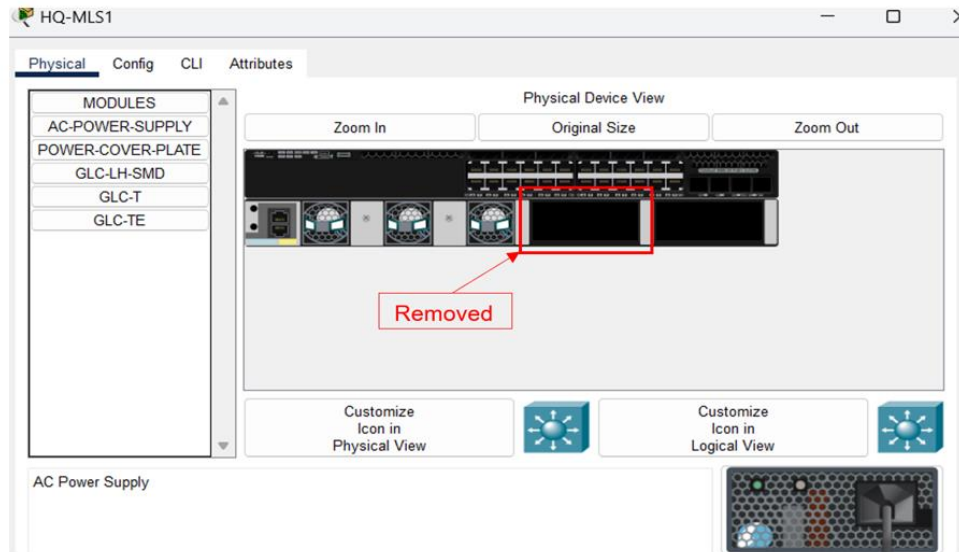


Figure (5.47): Remove AC Power Supply from HQ-MLS1

In **Figure (5.47)**, first, the AC power supply is removed from HQ-MLS1 to consider it as a failure. After that, the state of HQ-MLS2 will be checked to see if it is active or not working.

```
HQ-MLS2(config)#do sh standby br
P indicates configured to preempt.
|
Interface    Grp  Pri  P State    Active      Standby      Virtual IP
Vl10         10   100  P Active   local       unknown     192.168.1.1
Vl20         20   100  P Active   local       unknown     192.168.2.1
Vl30         30   100  P Active   local       unknown     192.168.3.1
Vl40         40   100  P Active   local       unknown     192.168.4.1
Vl50         50   100  P Active   local       unknown     192.168.5.1
Vl60         60   100  P Active   local       unknown     192.168.6.1
HQ-MLS2(config)#
```

Figure (5.48): Checking Active State in HQ-MLS2

In **Figure (5.48)**, when the HQ-MLS1 fails, HQ-MLS2 becomes active because of the correct HSRP configuration.

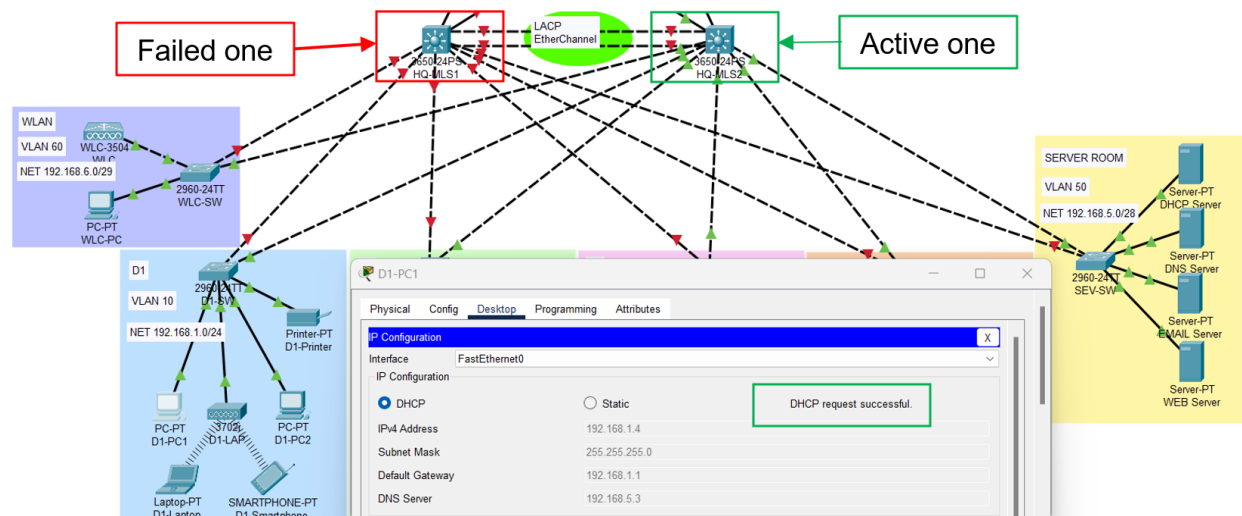


Figure (5.49): Successful DHCP Request from D1-PC1 When HQ-MLS1 Fails

In **Figure (5.49)**, D1-PC1 successfully obtains an IP address from the DHCP server. This indicates that HQ-MLS2 has successfully taken over from HQ-MLS1, restoring the entire network to its normal functioning state.

4.3.8. Verifying EtherChannel Status

```
HQ-MLS1(config)#do show etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1 (SU)          LACP       Gig1/0/8 (P) Gig1/0/9 (P)
```

Figure (5.50): EtherChannel Summary

In **Figure (5.50)**, a port-channel group 1 is created. Interfaces g1/0/8 and g1/0/9 both show 'p', indicating they are members of the port-channel group 1, and the protocol is LACP.

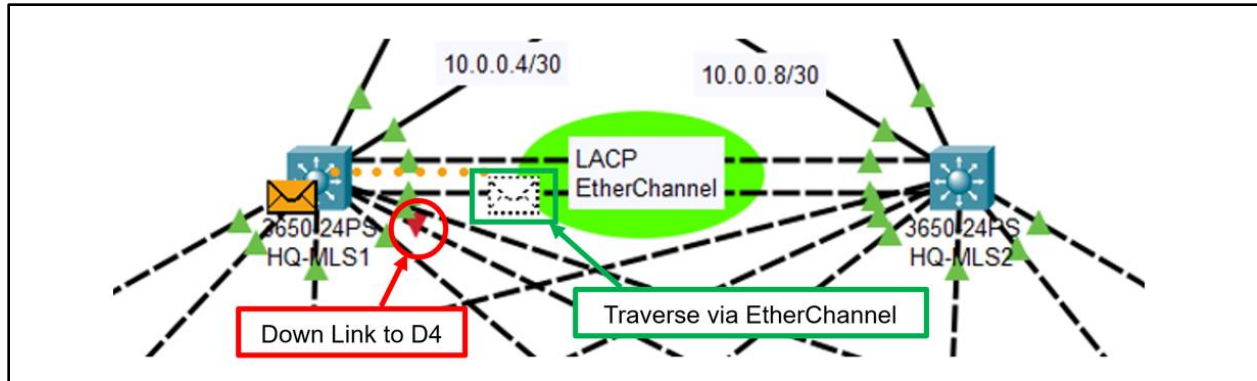


Figure (5.51): Providing Redundancy

In **Figure (5.51)**, the link from HQ-MLS1 to D4 is considered a failure. When D1-PC1 sends packets to D4-PC1, they traverse the EtherChannel to reach D4-PC1, utilizing redundancy.

4.3.9. Testing Conclusion

Through testing, password security, remote access, Wi-Fi connectivity, HSRP, EtherChannel, DHCP, WEB, DNS, and EMAIL servers are tested. After testing the whole design, it can be confidently concluded that all configurations were successfully implemented, and the expected results were obtained without encountering any issues.

5. Project Conclusion

As a conclusion, this project focuses on designing a hierarchical network, an enterprise-level design widely used in various industries. Throughout the project, current networking technologies, topologies, network simulation tools, and components of hierarchical network design have been researched using various internet sources such as academic papers, textbooks, and networking-related websites. The design is planned to meet the standards of hierarchical network design. It took several weeks to plan the design initially, involving extensive research. Initially, a firewall was considered for implementation at the top of the design, but encountered difficulties during implementation, leading to its removal from the design. In the real world, firewalls are essential for filtering unauthorized access and preventing cyber-attacks. However, this project aims to design a hierarchical network with three main benefits which are modularity, scalability, and flexibility. These benefits can be found in this project design. Building a network design project has provided advanced insights into network technologies and topologies. Moving forward, the aim is to continue researching more advanced technologies and gaining practical experience to further improve networking skills and support the networking industry.

6. References

- Academy, C. N. (2014). Connecting Networks Companion Guide: Hierarchical Network Design. In C. N. Academy, *Connecting Networks Companion Guide* (pp. 1-28). Indianapolis: Cisco Press.
- advantages-and-disadvantages-of-bus-topology*. (n.d.). Retrieved from www.javatpoint.com: <https://www.javatpoint.com/advantages-and-disadvantages-of-bus-topology>
- Borthakur, J. (2022). A comparison study of single area OSPF Network to multiple area OSPF Network implementation in a Campus area Network. *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. Kharagpur, India: IEEE.
- Bouchard, G. (2020, April 30). *OSI 7 Layers Explained the Easy Way*. Retrieved from www.insights.profitap.com: <https://insights.profitap.com/osi-7-layers-explained-the-easy-way>
- BrainKart. (n.d.). *Wired Technologies and its types*. Retrieved from BrainKart.com: https://www.brainkart.com/article/Wired-Technologies-and-its-types_36827/
- Brennan, L. L., & Johnson, V. E. (2004). *Social, Ethical and Policy Implications of Information Technology*. Information Science Pub.
- Chandramouli, R., & Rose, S. (2013). *Secure Domain Name System*. NIST.
- Forouzan, B. (2012). *Data Communications & Networking ed 5*. McGraw-Hill Education.
- Forouzan, B. A. (2009). *TCP/IP protocol suite*. McGraw-Hill Education.
- GeeksforGeeks. (2023, December 12). *what-is-routing*. Retrieved from www.geeksforgeeks.org: <https://www.geeksforgeeks.org/what-is-routing/>
- GeeksforGeeks. (2023, June 28). *what-is-switching*. Retrieved from www.geeksforgeeks.org: <https://www.geeksforgeeks.org/what-is-switching/>
- GeeksforGeeks. (2024, February 6). *network-layer-protocols*. Retrieved from www.geeksforgeeks.org: <https://www.geeksforgeeks.org/network-layer-protocols/>
- GeeksforGeeks. (2024, January 25). *protocols-application-layer*. Retrieved from www.geeksforgeeks.org: <https://www.geeksforgeeks.org/protocols-application-layer/>
- HO. (2018, October 25). *6 Leading Types of IoT Wireless Technologies and Their Best Use Cases*. Retrieved from behrtech.com: <https://behrtech.com/blog/6-leading-types-of-iot-wireless-tech-and-their-best-use-cases/>
- Insider, I. B. (n.d.). *Enhancing Network Security: A Comprehensive Guide for Organizations*. Retrieved from itbusinessinsider.com: <https://itbusinessinsider.com/enhancing-network-security-a-comprehensive-guide-for-organizations/>
- Jim Kurose, K. R. (2020). IPv4 Addressing. In K. R. Jim Kurose, *Computer Networking: A Top-Down Approach* (8th ed., pp. 333-344). Pearson Education.

Kurose, J., & Ross, K. (2018). *Computer Networking: A Top-Down Approach, Global Edition*. Pearson Education.

Misra, S., & Goswami, S. (2014). Fundamental Routing Protocols. In S. Misra, & S. Goswami, *Network Routing: Fundamentals, Applications, and Emerging Technologies* (pp. 59-87). Wiley Telecom.

packet-tracer. (n.d.). Retrieved from www.netacad.com:
<https://www.netacad.com/courses/packet-tracer>

Perez, A. (2014). *Network Security*. Wiley Data and Cybersecurity.

Rajput, A. K., Tewani, R., & Dubey, A. (2016). The helping protocol "DHCP". *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 634-637). New Delhi, India: IEEE.

Secgin, S. (2023). Seven Layers of ISO/OSI. In S. Secgin, *Evolution of Wireless Communication Ecosystems* (pp. 41-50). Wiley-IEEE Press.

Stallings, W. (2018). Network Access Control. In W. Stallings, *CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE GLOBAL EDITION* (7th ed., pp. 520-523). Pearson Education.

Tanenbaum, A. S., & Wetherall, D. (2011). *Computer Networks*. Pearson Prentice Hall.

Tanenbaum, A. S., & Wetherall, D. J. (2010). The OSI Reference Model. In A. S. Tanenbaum, & D. J. Wetherall, *Computer Networks* (5th ed., pp. 41-45). Boston: Pearson Education.

Tanenbaum, A. S., & Wetherall, D. J. (2010). The TCP/IP Reference Model. In A. S. Tanenbaum, & D. J. Wetherall, *COMPUTER NETWORKS* (5th ed., pp. 45-48). Boston: Pearson Education.

the-internet-protocols. (n.d.). Retrieved from www.khanacademy.org:
<https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:the-internet-protocol-suite/a/the-internet-protocols>

three-layer-hierarchical-model-in-cisco. (n.d.). Retrieved from www.geeksforgeeks.org:
<https://www.geeksforgeeks.org/three-layer-hierarchical-model-in-cisco/>

what-is-a-ring-topology. (n.d.). Retrieved from www.javatpoint.com:
<https://www.javatpoint.com/what-is-a-ring-topology>

what-is-mesh-topology. (n.d.). Retrieved from www.javatpoint.com:
<https://www.javatpoint.com/what-is-mesh-topology>

what-is-star-topology. (n.d.). Retrieved from www.javatpoint.com:
<https://www.javatpoint.com/what-is-star-topology>

7. Appendix

7.1. Proposal Overview

In modern times, network technology has become an essential part of accomplishing daily tasks in every organization. The organizations rely mainly on network technology for communication, data access, and the exchange of data resources. Therefore, all organizations must possess a well-designed network infrastructure to operate their daily tasks efficiently.

In the study of hierarchical network design, the design can be a 3-layer design or a 2-layer design. Large businesses can choose the 3-layer design, which is more reliable, while the 2-layer design remains an option for small businesses. The 3-layer design consists of three layers: the access layer, the distribution layer, and the core layer. The 2-layer design consists of two layers: the access layer and the distribution layer, or aggregation layer. This 2-layer design is also called the collapsed core design.

The access layer allows end devices such as computers, printers, and mobile phones to access the network. The distribution layer controls policy-based connectivity, firewalls, and ACL (Access Control List) rules. The core layer serves as the backbone of the network design. It is responsible for high-speed switching, which means packets are switching between the distribution switches as fast as possible.

The hierarchical network design provides the benefits of scalability, effective management, and efficient performance. Plus, it provides ease of network growth, reducing network complexity while increasing overall reliability. This project focuses on the design and implementation of the hierarchical network using a simulation tool. The simulated outcome is expected to match the real-world applicability nearly.

7.2. Aims and Objectives

Aims

This project aims to design and implement the 3-layer hierarchical network using the simulation tool.

Objectives

The following objectives are considered for researching, designing, implementing, and testing the hierarchical network to complete the project. The objectives are:

1. Research [3. 2]

- 1.1. Research on current network technologies [1. 0]
- 1.2. Research on network designs [1. 0]
- 1.3. Discussion with supervisor [1. 0]
- 1.4. Title approval by the supervisor [0. 2]

2. Research approach [5. 0]

- 2.1. Literature review on current network technologies [3. 5]
- 2.2. Literature review on existing network designs [3. 2]
- 2.3. Hierarchical network design approach [1. 2]

3. Design and implementation [12. 3]

- 3.1. Review of simulation tools [2. 0]
- 3.2. Design and configuration [9. 2]
- 3.3. Testing and evaluation [1. 3]

4. Documentation and project conclusion [2. 4]

- 4.1. Review of the whole project [0. 6]
- 4.2. Validation and verification [0. 6]
- 4.3. Finalize the documentation [0. 6]

7.3. Legal, Ethical, Social, and Professional Issues

Legal Issues

This project comprises implementing a hierarchical network design using a simulation tool and a report. By understanding the applicable laws and regulations, all the sources used in this entire project have added citations and references respectively. Moreover, this project includes IETF and IEEE standards to ensure the project's integrity.

Ethical Issues

This demonstrated that network design complies with the network standards by understanding the ethical principles. This project does not include offensive features and is not intentionally violating user rights. This project is not breaching any person's or organization's privacy or security measures.

Social Issues

This demonstrated network design project contributes to positive social issues. The network infrastructure is designed to meet society's requirements with legitimate resources. This project seeks to advance network technology while considering social responsibility.

Professional Issues

This project is demonstrated and utilized according to industry standards, such as IEEE, to support professionalism. The design is considered to maintain the quality of the network by providing confidentiality, integrity, and a reputation to support professionalism. This design guarantees a standard network that can be applied to every industry.

(Brennan & Johnson, 2004)

7.4. Research Approach Overview

The research approaches the best practices of designing the 3-layer hierarchical network. This design approach consists of studies in VLAN (Virtual Local Area Network) technologies, concepts of routing protocols, network services such as DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System), and so on. The studies are applied in the simulation tool to perform the best practices in the network. The overall design approach will consider systematic studies of literature and technologies.

7.5. Project Planning

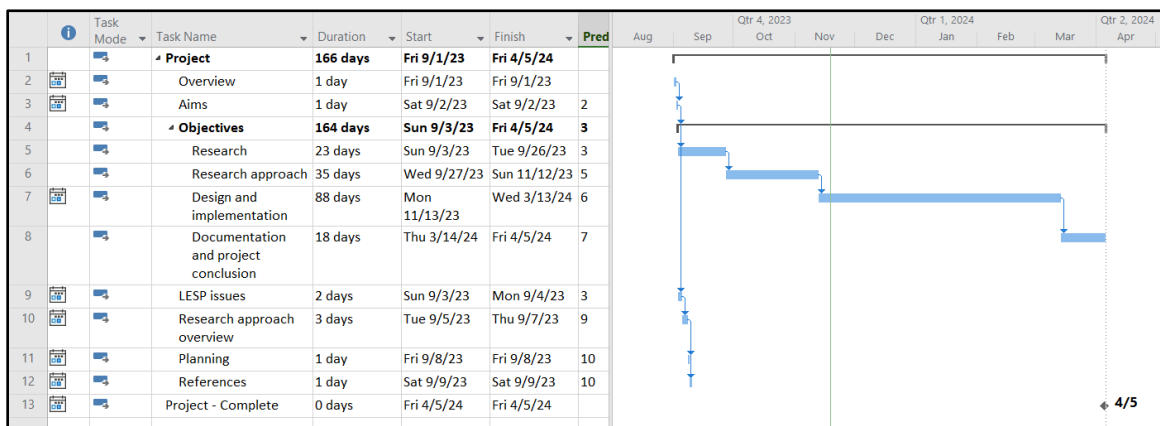


Figure (1): Overall Project Plan

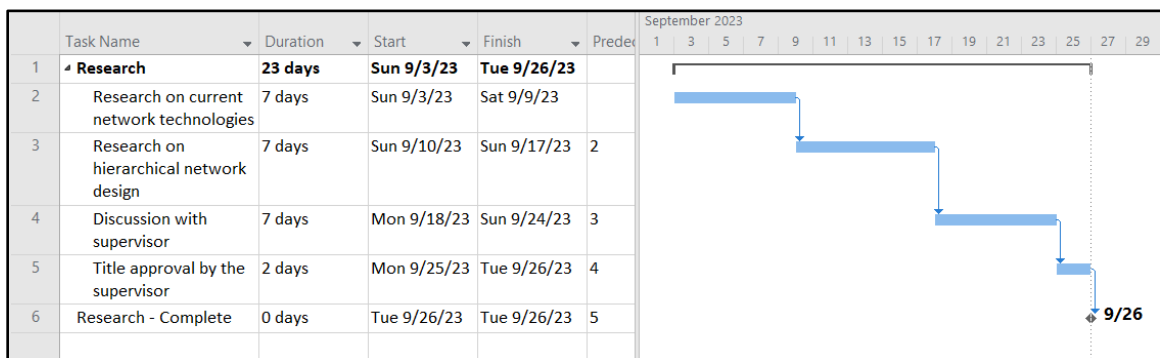


Figure (2): Research Plan

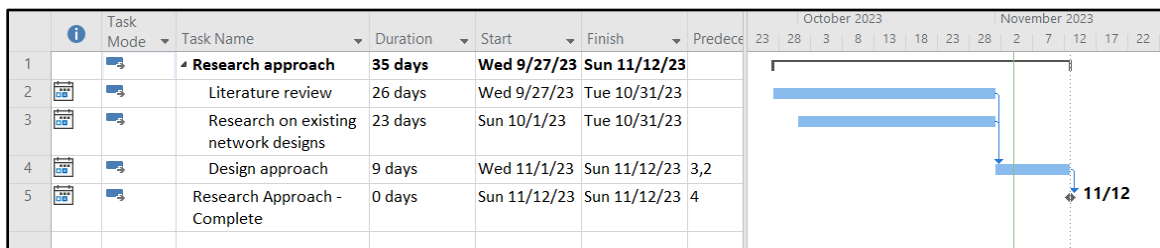


Figure (3): Research Approach Plan

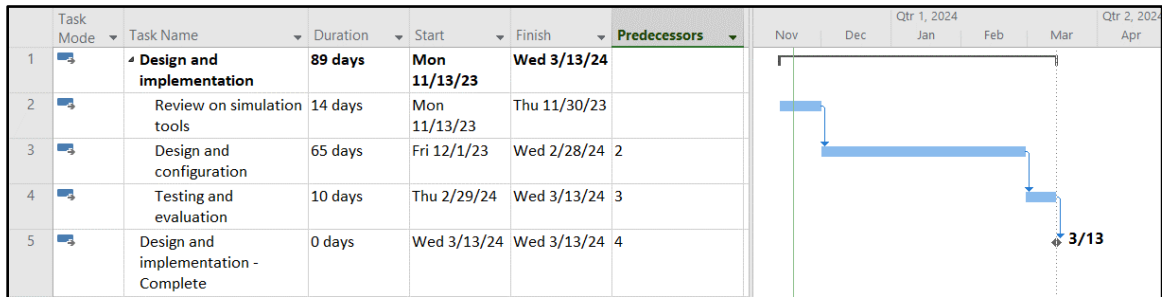


Figure (4): Design and Implementation Plan

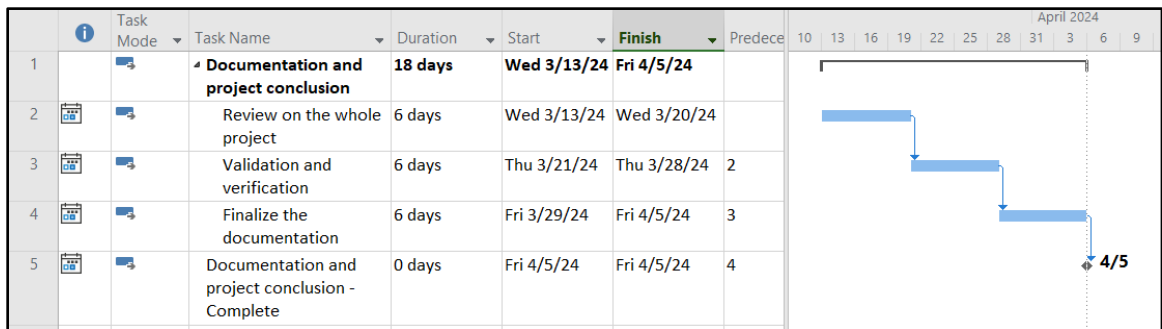


Figure (5): Documentation and Project Conclusion Plan