CM2108: Secure Communication Networks

PORTFOLIO ON SECURE COMMUNICATION NETWORKS **(100%)**

Lakshmi Ksheeraja Sikha | 23112887 | 16th December 2024

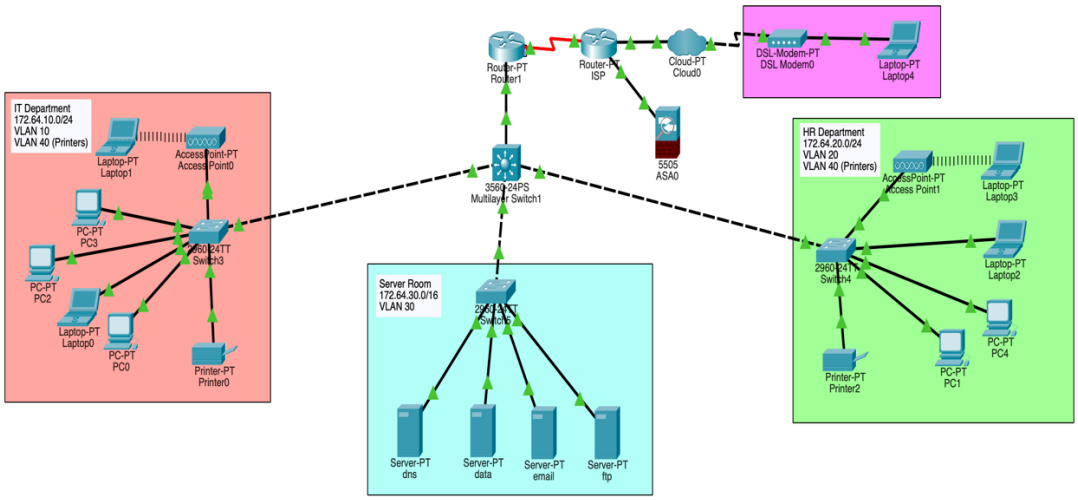
1. Network Design

a. Network Diagram and Justification

As part of the IT team at '**Teclyn'**, a mid-sized company with 150 employees spread across **two floors**, I have been tasked with designing an efficient network layout that meets the company's technical requirements. So below are the Components of the network along with the justification of the design choices:

- Red Section: IT Department (2960-24TT Switch3, AccessPoint0, Printer1, PC0, Laptop0, Laptop1, PC2, PC3)
- Blue Section: Server Room (DNS, DATA, EMAIL and FTP Servers)
- Green Section: HR Department (2960-24TT Switch4, AccessPoint1, Printer2, PC1, Laptop2, Laptop3, PC4)
- Home Network (Core Network): Multilayer Switch1, Router1, ISP router, Cloud0, ASA0 (Firewall), DSL Modem and Laptop 4

Network Diagram:



Design Justification: The requirements state a middle-sized company "Teclyn" with its layout over 2 floors and 150 employees which is designed accordingly to meet the requirements for efficiency, connectivity and stability. The key components of this network include:

- **Core Network (Home Network):**

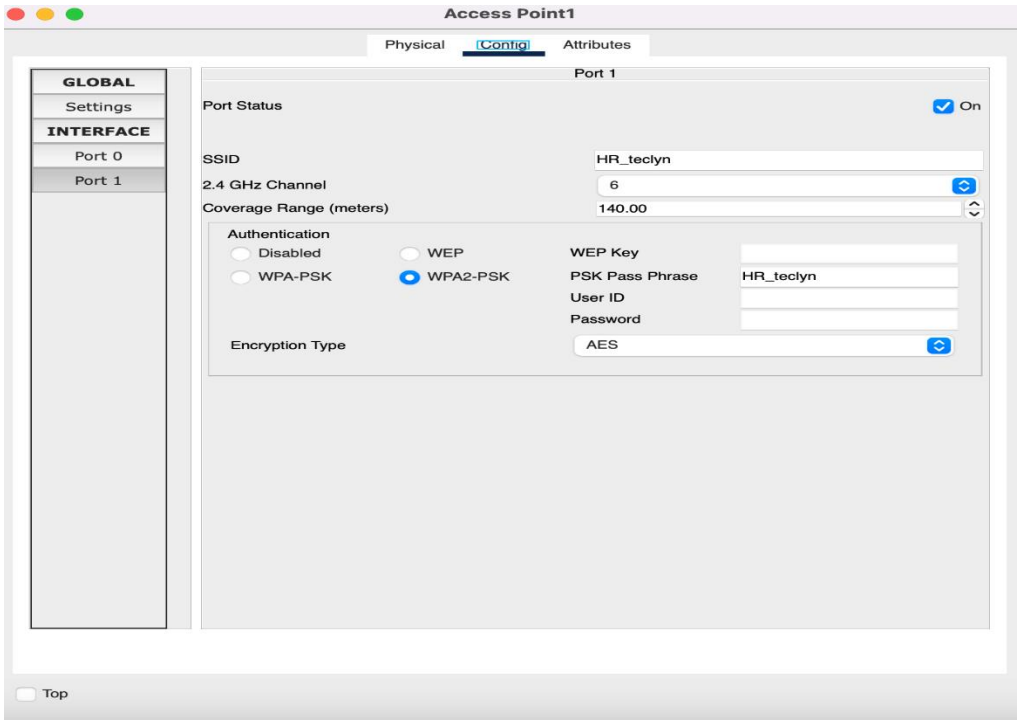
1. **ISP Router:** An ISP Router is used to connected Multiple devices of the network to the Internet. For this network I decided to choose an ISP due to the size of the network plus allowance of wireless and wired network services. Also, provides with security features and quality of service as it is connected to Firewall.

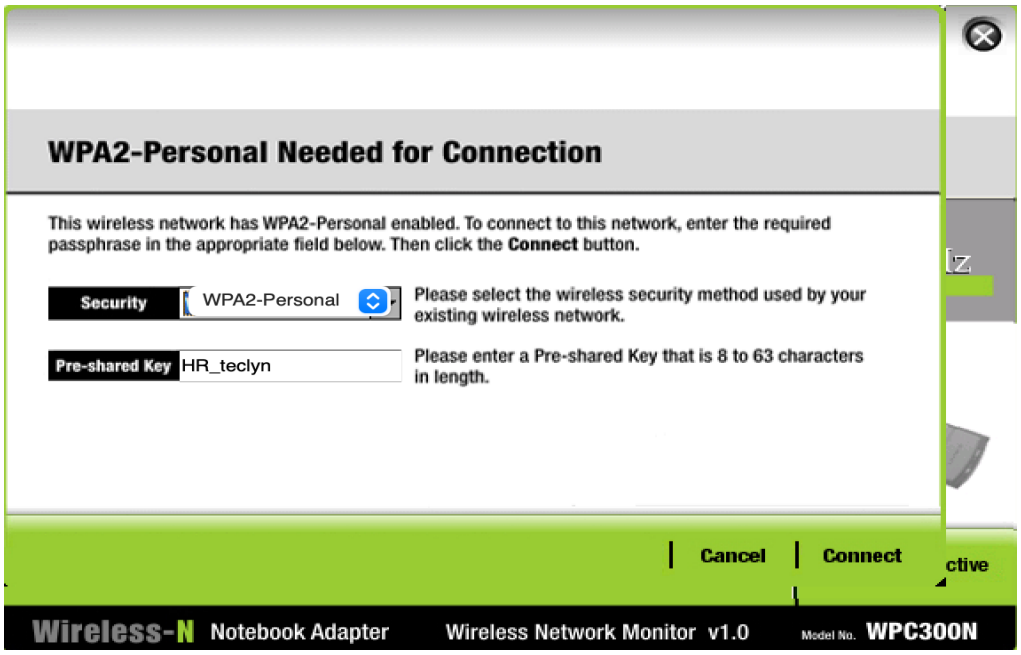
2. **Cloud:** Useful for providing the network with infrastructure, applications necessary for the workplace, Storage of databases for the company.
3. **ASA Firewall (ASA 5505):** Provides network security by filtering the unauthorised traffic throughout that enters or exits the network. It protects the Servers and the End Devices from external attacks such as viruses and malware, etc
4. **DSL Modem:** Acts as a bridge between the Laptop4 and the rest of the network as the Laptop4 is a connected to the remote network, i.e., the Home Network. Also helps check connectivity between laptop and the broader network.
5. **Laptop4**: Helps with checking the networks and day to day operations of the networks within the office.

- **Router (PT Router):** Handles Inter-network communication and connects the local networks (LAN) to the Internet Service Provider (ISPs). The router ensures that devices can access external resources and manages routing between subnets in the network
- **Multilayer Switch (3560-24PS Multilayer Switch**): Enables VLAN Configuration for traffic segmentation, improving network efficiency and reduces congestion. Also facilitates Inter-VLAN routing which allows communication between different departments. The VLANs set for the different networks (Departments within the network) are:

VLAN Routing for Teclyn's Design Layout	
Department	VLAN
Home Network (Core Network)	1
IT Department	10
HR Department	20
Server Room	30
Printers	40

- **Switches (2960-24TT Switches):** Connect end devices like PCs, printers, and servers, ensuring efficient LAN communication. Connect end devices like PCs, printers, and servers, ensuring efficient LAN communication.
- **Access Points:** Provides wireless connectivity for Laptops and other wireless devices and ensures that the employees have access to the network by typing in the PSK Pass Phrase and retrieving the wireless network. Below is an example on how easy it is to configure a wireless network through access points:





Through this, we are able connect wireless devices with extreme efficiency.

- **Servers (DNS, Email, Data, FTP):**

  DNS Server: Resolves domain names to IP addresses for internal devices.

  Data Server: Hosts files and shared resources for employees to access.

FTP Server: Facilitates file transfer services for uploading and downloading files securely.

Email Server: Manages email communication within the organization

- **End Devices (PCs, Laptops, Printers):** Workstations and peripherals for day-to-day operations.

b. Subnetting Scheme

Given Subnetting Scheme for the network: 172.64.0.0/16 To efficiently allocate into IP addresses, I divided the /16 network into /24 subnets:

Subnet	Subnet Mask	Network Address	Host Range	Purpose
Subnet1	/24	172.64.1.0	172.64.1.1-172.64.1.254	Home Network (Core Network)
Subnet2	/24	172.64.10.0	172.64.10.1-172.64.10.254	IT Department
Subnet3	/24	172.64.20.0	172.64.20.1-172.64.20.254	HR Department
Subnet4	/24	172.64.30.0	172.64.30.1-172.64.30.254	Server Room
Subnet5	/24	172.64.40.0	172.64.40.1-172.64.40.254	Printers

Dividing the /16 subnet into /24 subnet makes the IP allocation more efficient as it reduces the IP networks from 65,536 addresses to 256 addresses. This makes network segmentation better, management is easier. With limited addressing, it makes it much simpler, and limits issues and allows better security between networks.

VCCL Hosting, 2020. Unlock the power of /24 subnet: A comprehensive guide. Medium[online]

2. Network Simulation

The Simulation of the entire network is done using Cisco Packet Tracer

Connectivity Testing: Successfully tested the end-to-end communication between devices and networks using the Ping commands. The connection between the devices and the departments is given in detail in the video, proving the subnetting and the VLANs amongst these networks that can send packets of data throughout the network successfully.

3. Network Services and Protocols

As per the network, explaining through worked examples about how protocols are used to transfer data across the above network:

Using the OSI 7-Layer Model: The Open Systems Interconnection Model (OSI Model) is a framework that standardises the communications functions within a network. The communication within the network is divided into 7 layers, with each layer handling a specific part of this communications process. The 7 layers and its relation to my network are as follows:

1. **Application Layer:** The Application layer is the topmost layer and directly interacts with the user's applications. It provides services such as file transfer, email, and web browsing. Protocols like HTTP, FTP, SMTP, and DNS operate at this layer, enabling application-level communication. In a network, the Application layer ensures that data is formatted and presented in a way that applications can understand. For example, web browsers use HTTP to retrieve and display web pages, while email services use SMTP to send messages.
2. **Presentation Layer:** Converts data into a format readable by the application layer. Handles encryption, compression, and data translation. When a user uploads or downloads files from the server, this layer ensures data is compressed or encrypted if required. For secure communication (e.g., HTTPS), SSL/TLS encryption occurs at this layer to protect sensitive information.
3. **Session Layer:** Manages and maintains communication channels between devices. When a user accesses the file server, the session layer ensures the connection is established, managed, and terminated appropriately. For remote access to the network (e.g., via SSH), a session is created between the user and the network server.
4. **Transport Layer:** Provides end-to-end communication, ensuring data is delivered reliably and in the correct order. Protocols used within this layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). For reliable file uploads to the server, TCP ensures that all data packets are sent and acknowledged and tasks like video streaming or VoIP communication, UDP may be used because it prioritizes speed over reliability. Port numbers are used to differentiate services (e.g., port 25 for email via SMTP, port 80 for web traffic)
5. **Network Layer:** Handles logical addressing, routing, and packet forwarding to ensure data can travel between subnets or networks**.** Within this network, Protocols such as IP addressing and ICMP are used. Devices in the network are assigned IP addresses (e.g., 172.64.1.0/24). Routers are deployed to route data between different subnets, ensuring connectivity between servers, clients, and

VLANs. ICMP is used for connectivity checks; for example, a ping test will verify if devices like printers and servers are online.

6. **Data Link Layer:** Manages the reliable transfer of data frames between devices on the same local network. This layer includes MAC addressing and error detection.

- The Protocol used within this network is Ethernet which is used for communication between computers, printers, and servers within the network. Switches work at this layer to forward frames based on MAC addresses.

7. **Physical Layer:** Deals with the physical hardware connections, such as cables, switches, and signals that transmit raw data (bits). Within the network**,** the network uses Ethernet cables and Wi-Fi from Wireless access points to connect devices. Switches and routers serve as the backbone, allowing data transfer across different subnets or VLANs and when connected to Wi-Fi, the data is transmitted as radio waves to a wireless access point. The physical layer ensures the reliable transmission of bits across the network infrastructure.

Data Encapsulation in the OSI Model

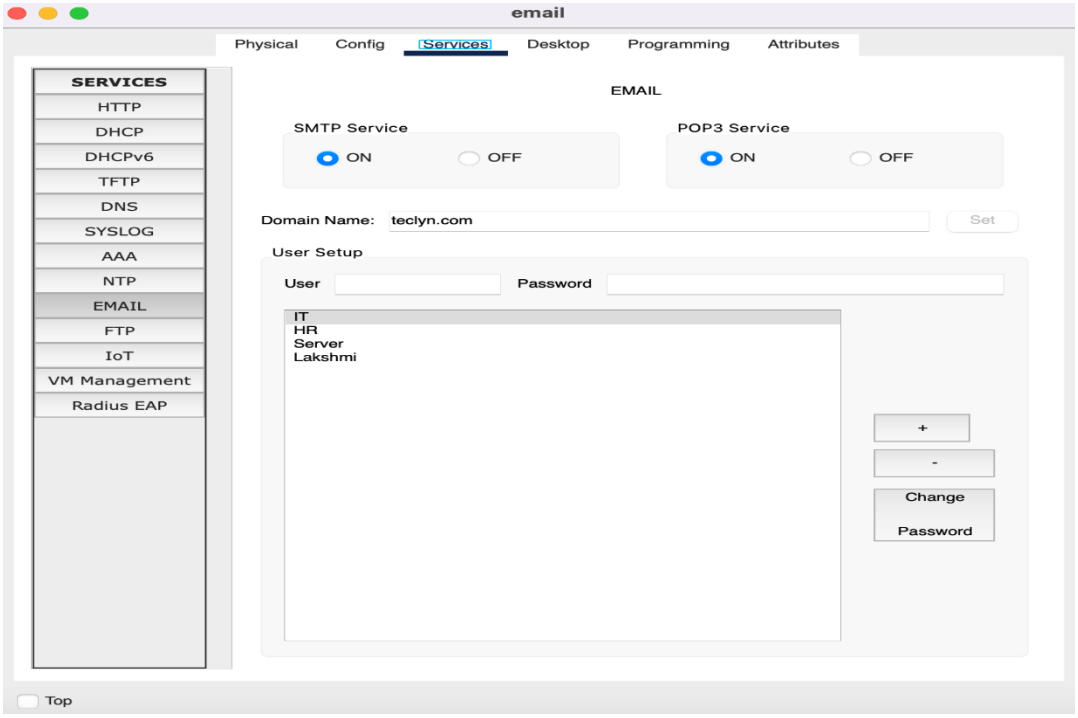
In the OSI model, data is **encapsulated** as it moves from the application layer (top) to the physical layer (bottom):

1. **Application Layer**: User data is generated (e.g., an email).
2. **Presentation Layer**: Data is formatted, compressed, or encrypted.
3. **Session Layer**: A session is established for communication.
4. **Transport Layer**: Data is segmented and assigned TCP/UDP port numbers.
5. **Network Layer**: Logical IP addresses are added, creating **packets**.
6. **Data Link Layer**: MAC addresses are added, creating **frames**.
7. **Physical Layer**: Frames are converted to electrical or optical signals and transmitted across the network.

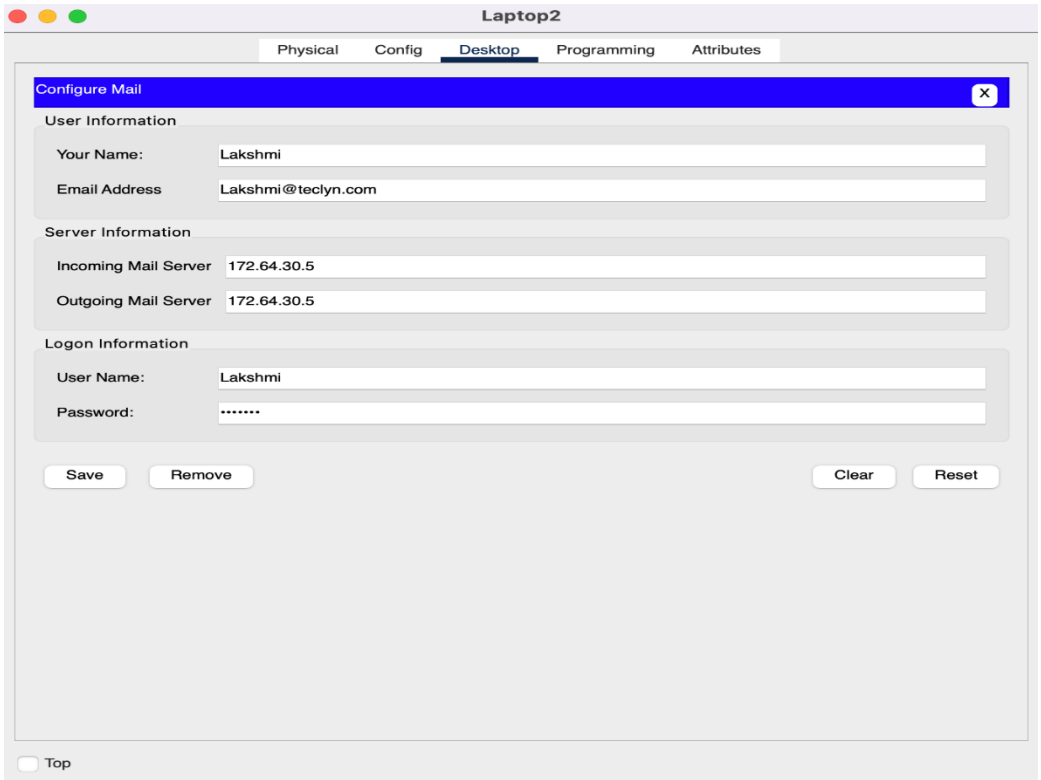
As the data reaches its destination, this process is reversed (de-encapsulation), ensuring the original message is reconstructed and delivered.

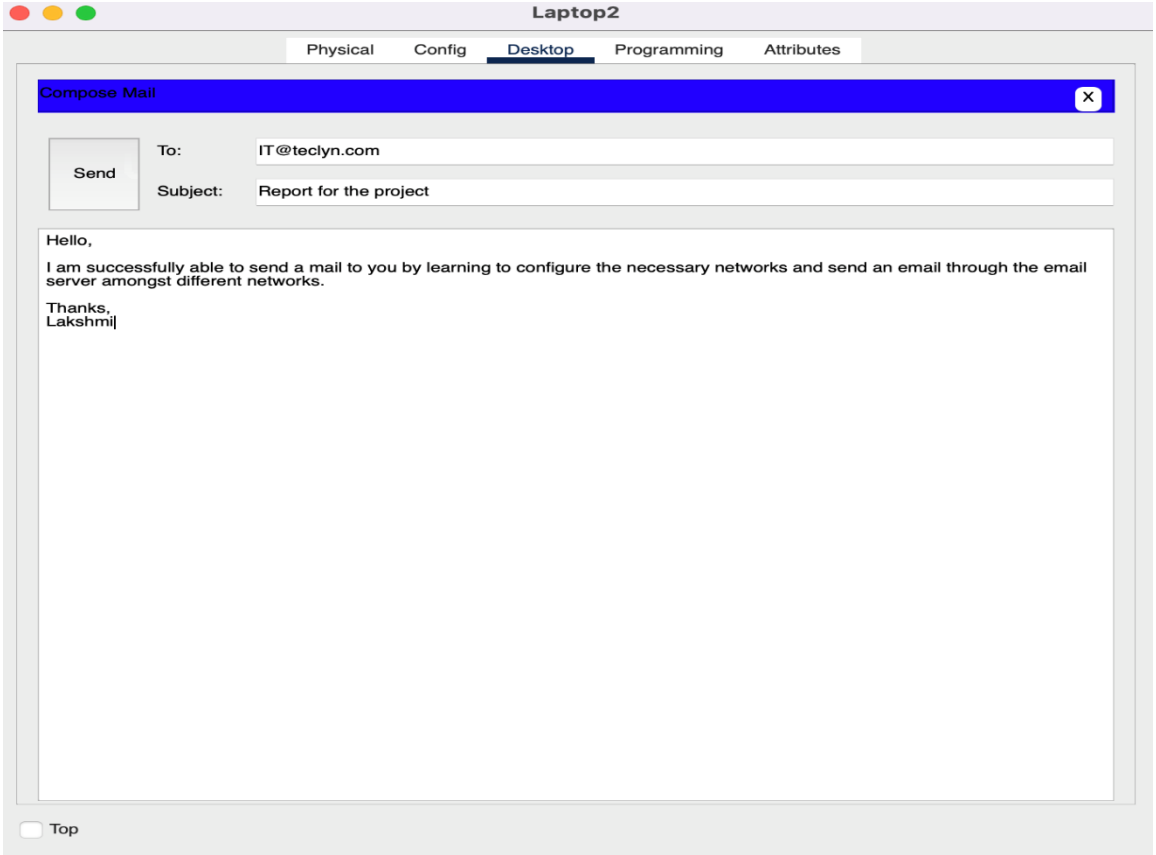
Example: Sending an Email Across the Teclyn Network

First, I ensured to set up the required usernames and passwords in the EMAIL Server.



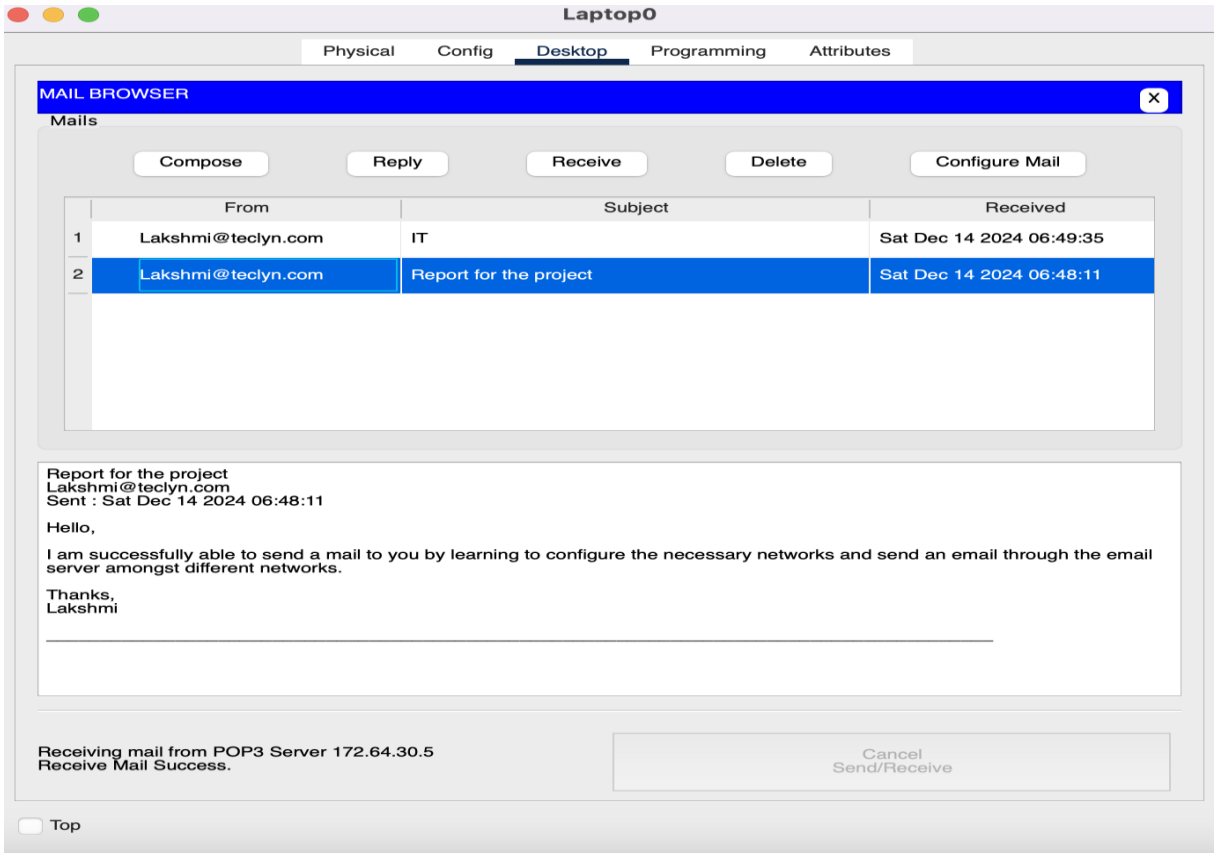
1. **Application Layer**: The user composes an email (SMTP).





2. **Presentation Layer**: The email is encrypted using SSL/TLS.
3. **Session Layer**: A session is established between the email client and the email server.
4. **Transport Layer**: TCP divides the email into segments and assigns a port number (port 25 for SMTP).
5. **Network Layer**: The IP address of the email server is added to the packet.
6. **Data Link Layer**: The packet is framed with MAC addresses and sent to the switch.
7. **Physical Layer**: The data is transmitted as electrical signals through Ethernet cables to the email server.

At the receiving end, this process is reversed, and the recipient successfully receives the email. The Mail that I sent from my username (Lakshmi) has finally come to the IT Department and I am able to access the email from any device in that department. The image below also shows how the EMAIL Server (172.64.30.5) successfully has sent through the server to different devices.



4. Network Security

Access control is fundamental to preventing unauthorized access to the network. To ensure security and proper resource management, I implemented VLANs to segment the network into distinct departments: IT, HR, and the Server Room. VLAN segmentation restricts access based on departmental roles, ensuring that employees can only interact with systems and data relevant to their responsibilities. For instance, HR systems are isolated from IT and server resources, preventing unauthorized access unless explicitly permitted through the PSK Pass Phrase as the other Department users will not be able to access files until they are given the Pass Phrase. This not only safeguards sensitive data but also reduces the risk of lateral movement within the network in case of a breach. By isolating network traffic, VLANs also improve performance and limit exposure to potential threats, ensuring each department operates within its designated boundaries. Additionally, I implemented a firewall (ASA0) to provide an additional layer of protection between the core network and the internet. The firewall filters incoming and outgoing traffic based on predefined security rules, blocking unauthorized access and ensuring that only legitimate traffic is allowed to pass through. This adds an extra

layer of defence, especially for the IT and Server Room segments, which house critical infrastructure. This layered approach aligns with the principle of least privilege, granting access strictly on a need-to-know basis, which is vital for mitigating risks and upholding security standards in a corporate environment like Teclyn.

My network design supports the three main principles of information security: **confidentiality, integrity, and availability.**

- To maintain **confidentiality**, I used VLANs (Virtual Local Area Networks) to separate different departments. This means that each department—like HR, IT, and the Server Room—has its own isolated section of the network. For example, HR staff can only access HR-related files and systems, and they can't access IT systems or servers. This helps keep sensitive HR data safe from unauthorized access and ensures that employees can only access what they need for their job.
- **Integrity** is protected by using a firewall (ASA0) between the network and the internet. The firewall acts like a security guard, only allowing safe and approved traffic into and out of the network. It helps stop malicious attacks like data manipulation or tampering. On top of this, encryption is used to protect data when it's being sent across the network. For example, we use SSL/TLS for web traffic, which secures data as it moves between the web browser and the server, and a VPN to protect remote access, ensuring that the data can't be altered by attackers during its journey.
- Finally, for **availability**, I ensured the network is designed to keep running smoothly, even if something goes wrong. The network is divided into different sections, and each server in the Server Room has a backup, so if one server fails, another can take over. The multilayer switch (Multilayer Switch1) helps make sure that the network in the core area stays available and can handle traffic efficiently. If one path fails, the system can automatically switch to another, minimizing downtime.

By using these methods, my network design helps ensure that sensitive information is kept safe, that data is accurate and unaltered, and that the network is always up and running

As an additional recommendation to further enhance the security of my network, I would consider implementing **Multi-Factor Authentication (MFA)** and utilizing **Wireshark** for continuous monitoring. I could employ **MFA** to secure access to sensitive resources, particularly in areas like the IT Department and Server Room. With MFA, users would need to authenticate using more than just a password—such as a combination of a password, a physical token, or biometric verification. This would

significantly reduce the risk of compromised credentials and add an extra layer of protection. Additionally, I could use **Wireshark** to capture and analyse network traffic in real-time. This would help me identify any unauthorized attempts to access restricted segments or detect unusual activity that might indicate a potential breach. Wireshark would also allow me to monitor the effectiveness of encryption protocols, ensuring that data remains secure during transmission. By integrating both MFA and Wireshark into the network, I would be able to create a more secure environment that not only restricts unauthorized access but also continuously monitors network traffic for any signs of vulnerabilities or malicious activity.

5. Network Performance

a. Network Performance: using examples of potential performance issues

My network upholds high performance using multiple strategies that address potential performance issues. One of the key components is the use of VLANs to segment network traffic based on department. This segmentation ensures that data traffic from one department, such as HR, does not interfere with traffic from another department, like IT. This division optimizes the performance within each department by reducing congestion and ensuring that bandwidth is used efficiently.

To further boost network performance, I have implemented a multilayer switch (Multilayer Switch1) in the core network, which helps route traffic more efficiently and minimizes delays. Additionally, the router (Router1) between the core network and external connections ensures fast and reliable access to the internet by managing traffic effectively.

For monitoring performance, network metrics like latency, throughput, and packet loss are important indicators of performance quality. These can be measured using network monitoring tools that track the performance of both internal and external connections. With the strategic placement of access points (AccessPoint0 and AccessPoint1), users can experience reliable wireless connectivity with minimal interference. Overall, these performance-enhancing measures reduce bottlenecks, ensuring that employees can complete tasks such as sending emails, uploading files, or accessing servers without delays.

b. Describing how my network upholds dependability:

My network design upholds dependability by ensuring high availability and fault tolerance. One of the strategies I used is incorporating redundant infrastructure, particularly in the server room. The DNS, DATA, EMAIL, and FTP servers are critical to

the company's operations, so having multiple servers for redundancy ensures that if one fails, another can take over seamlessly. This redundancy minimizes the risk of downtime and ensures that services remain operational even in the event of a hardware failure.

To further ensure dependability, I implemented a robust firewall (ASA0) that filters out malicious traffic and protects internal servers from cyberattacks that could cause service disruptions. Additionally, the network is designed with proper load balancing, ensuring that no single point of failure impacts overall network performance. This is particularly important for handling high-volume traffic and preventing slowdowns during peak usage times.

Network dependability can be measured through uptime metrics and the frequency of service disruptions. By using tools that track server availability and performance, I can proactively identify and resolve issues before they cause significant downtime. The combination of redundancy, load balancing, and firewall protection makes the network resilient and ensures that all systems remain available, supporting continuous business operations.