SUNWAY UNIVERSITY

SCHOOL OF ENGINEERING AND TECHNOLOGY

ASSIGNMENT COVER SHEET

COURSE: NET1014 – Networking Principles

LEVEL: BCNS, BIT, BCS, BSE, BDS - Year 1

ACADEMIC SESSION: September 2024 Semester

DEADLINE: 22th Dec 2024 – 11:59PM

GROUP NO: 1

#	Name	Student ID	Percentage of contribution
1	Mohamed Anan Abdul Samad Weerasinghe	23116718	20
2	Jaimelynn Wong Shin Yew	23113814	20
3	Fathima Nuha Nizar	23102676	20
4	Naila Nura Fabienne Raja	23129570	20
5	Ethan Yeng Ke Zhong	22089403	20

TASK I:

OSI PROTOCOL STACK

APPLICATION LAYER

The **Application Layer (Layer 7)** is implemented by network applications. These applications produce the data to be transferred over the network and act as a bridge between the user and the network.

Functions and Tasks

1. **Network Virtual Terminal (NVT):** Allows a user to log on to a remote host. This provides a standardized interface for communication across different systems.
2. **File Transfer, Access, and Management (FTAM):** Enables users to access, retrieve, and manage files on a remote host. It simplifies file sharing and control between systems.
3. **Mail Services:** Provides email services for sending, receiving, and managing messages.
4. **Directory Services:** Offers access to distributed databases containing global information about objects and services. Helps users locate resources and services efficiently.

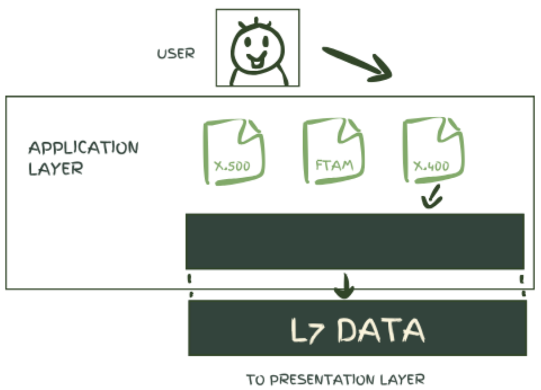
Examples such as :

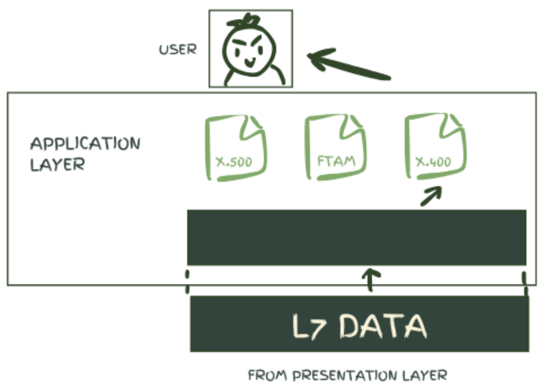
Email: Sending and receiving emails using services like Gmail or Outlook.
Web Browsing: Accessing websites via web browsers like Chrome or Firefox.
File Sharing: Transferring files using services like Dropbox or Google Drive.
Video Streaming: Streaming videos on platforms like Netflix or YouTube.

Real-World Protocols

HTTP/HTTPS (HyperText Transfer Protocol/Secure) : Enables web browsers to communicate with servers for accessing websites. Vital for everyday activities like browsing, online shopping, and accessing secure portals.
FTP (File Transfer Protocol) Enables file transfers between systems. Used for uploading and downloading large files, especially in web development and server management.
DNS (Domain Name System): Translates domain names into IP addresses.

An example for better understanding :
When you type a URL like www.example.com into a browser:
- DNS resolves the domain to an IP address.
- HTTP/HTTPS fetches the webpage from the server.
- TCP/IP (from lower layers) ensures reliable delivery of data packets.
- The browser displays the content for the user to interact with.





PRESENTATION LAYER

The **Presentation Layer (Layer 6)** ensures that data is presented in a format that both the sending and receiving systems can understand. It acts as a translator and manager of data formats.

Functions and Tasks

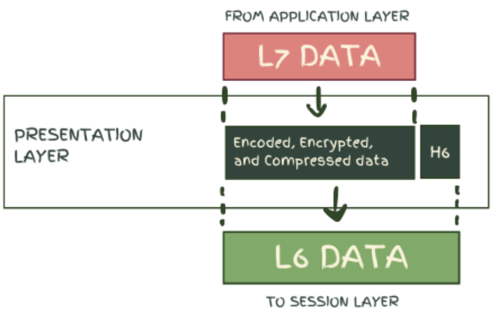
1. **Data translation**: Formatting, or presenting data at the source device into a compatible format for receipt by the destination device
2. **Data compression**: Compressing data in a way that can be decompressed by the destination device
3. **Data encryption**: Encrypting data for transmission and decrypting data upon receiving

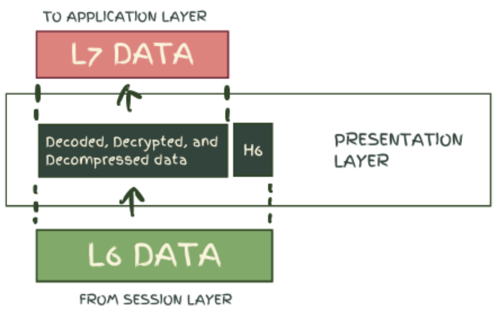
Real-World Protocols

SSL/TLS (Secure Sockets Layer/Transport Layer Security): Encrypts and secures data transmission over networks (e.g., HTTPS uses TLS).
MIME (Multipurpose Internet Mail Extensions): Encodes files like images and videos for email attachments.
JPEG, GIF, PNG: Standardizes image compression and encoding formats.
MP3, MP4: Used for audio and video compression.
ASCII/EBCDIC: Ensures text data uses a standardized encoding format.

Examples such as:

Video Streaming: The Presentation Layer compresses video files so platforms like Netflix can deliver them smoothly.
Secure Web Browsing: HTTPS encrypts data during online shopping or financial transactions.
Email Attachments: Email clients handle encoding (e.g., MIME encoding) to ensure attachments are transmitted properly.
File Conversion: When uploading a document, the Presentation Layer ensures it's converted into a compatible format (e.g., DOCX to PDF).





SESSION LAYER

The **Session Layer (Layer 5)** allows users on different machines to establish active communications sessions between them. This layer essentially coordinates communication between devices as well as as It manages sessions and synchronizes data flow.

Function and Tasks

1. **Dialog Control :** Enables communication between systems in either half-duplex or full-duplex mode, ensuring orderly data exchange.
2. **Synchronization :** Adds checkpoints (synchronization points) in data streams which allow resumption of communication from the last synchronization point in case of failures.
3. **Remote Procedure Calls (RPCs) :** Enables applications to execute procedures on remote systems as if its local.
4. **Data Flow :** Fetches or receives data from Transport Layer and sends it to Presentation Layer for smooth data flow

Real World Protocols and Relevance

RPC (Remote Procedure Call Protocol) : Allows one program to execute a procedure on another device over a network. It simplifies communication by abstracting the remote interaction details.

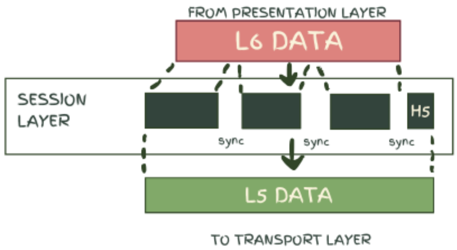
- **Key Features:** Client-server interaction, request-response communication.
- **Real-Life Application:** Cloud Services (e.g., AWS Lambda) – Enables distributed systems to process tasks seamlessly across multiple servers.

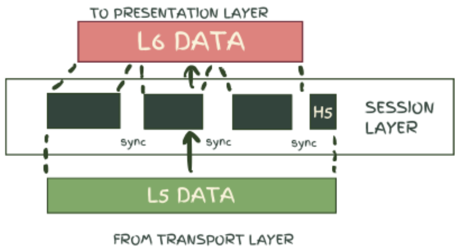
PPTP (Point-to-Point Tunneling Protocol) : Creates Virtual Private Networks (VPNs) by encapsulating PPP packets. It enables secure remote access by tunneling through networks.

- **Key Features:** Tunneling, encryption, and remote access support.
- Real-Life Application: Remote Work VPNs – Provides secure connections for employees accessing office resources from home.

Examples such as:

- **Video Conferencing (e.g., Zoom) –** Uses RTCP to synchronize audio and video for smooth communication.
- **VPNs (e.g., PPTP) –** Creates secure sessions for remote network access.
- **Remote Desktop (e.g., Windows RDP) –** Manages sessions for seamless remote control of a computer.





TRANSPORT LAYER

The **Transport Layer (Layer 4)** is responsible for end-to-end communication and data transfer management between devices on a network. It ensures reliable, error-free delivery of data across networks and supports multiplexing to allow multiple applications to share the same network connection.

Functions and Tasks

1. **Segmentation and reassembly:** The message is split up into segments and is given a unique sequence number. It then reassembles the message based on sequence numbers once it reaches its destination.
2. **Service-point addressing:** Data is also transmitted from source to destination from one process to another. As such, this layer adds the header that contains the address known as a service-point address or port address. The transport layer is in charge of sending the message to the appropriate process
3. **Connection control:**
- ***Connectionless service***: Each segment is handled as separate packet & take distinct paths
- ***Connection oriented***: Every packet follows the same path
4. **Flow control:** Manages end-to-end data transmission rates
5. **Error control:** Ensures that the data packet is received to the destination without any error.

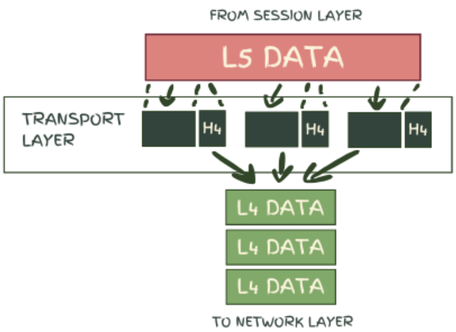
Real World Protocols and Relevance

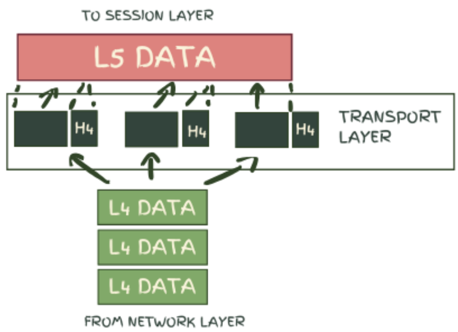
TCP (Transmission Control Protocol): a connection-oriented protocol that ensures reliable and ordered data delivery between devices. It establishes a connection via a handshake, monitors data flow with acknowledgments, and retransmits lost packets.

- **Key Features:** Reliable, ordered, error-checked delivery.
- **Examples such as:**
  - Email (SMTP) – Ensures the complete and correct transfer of emails between servers.
  - Text Communication (e.g. Whatsapp) – Ensures there is no discrepancy in texting between sender and receiver

UDP (User Datagram Protocol): a connectionless protocol offering fast, lightweight data transmission without guaranteeing delivery or order. It is used in applications where speed is prioritized over reliability.

- **Key Features:** Low latency, no acknowledgments, or retransmissions.
- **Examples such as:**
  - Video Streaming (e.g., Netflix) – Provides fast data transmission for uninterrupted viewing, even if some packets are lost.





NETWORK LAYER

The **Network Layer (Layer 3)** is primarily tasked with the management of routing and forwarding data to external receipients, mainly other servers, and checking for any data errors after the transfer.

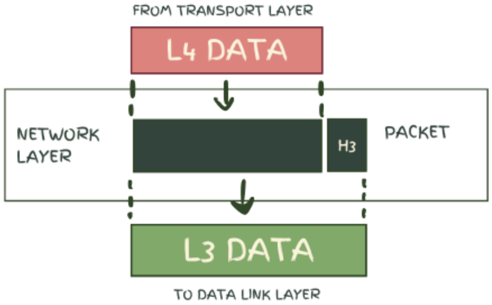
Functions and Tasks

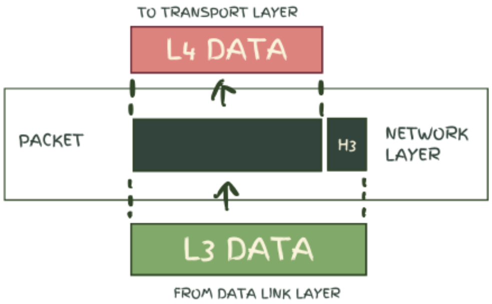
1. **Routing:** Determines the optimal path needed for data transmission from source to destination across multiple points in the network through the use of routing protocol
2. **Packet Forwarding:** The process of routing packets through various nodes in a computer network
3. **Addressing:** Assigns logical addresses to each device to identify each one individually and to confirm the data successfully reaching the intended destination
4. **Fragmentation and Reassembly:** Breaks down packets that are too big to be processed into smaller processable unit for the transmission process and reassembling them at the end point.

Real-World Protocols and Relevance

This layer of the OSI protocol ensures a smooth and efficient connection to whichever website that maybe connected to at a given time. It ensures the data packets are sent and received correctly after being sent through multiple routers across the internet before reaching the host's device where it is read and displayed or the site's server host. Some protocols used in this layer include:

IPv4 and IPv6: Acts as addresses between networks, allowing seamless transmissions.
ICMP (Internet Control Message Protocol): Checks for errors in the data transferred and gives a diagnostic based on it.





DATA LINK LAYER

The **Data Link Layer (Layer 2)** is mainly responsible for local communications between Network Interface Cards. It sequences data and encapsulates them into frames before sending them down to the physical layer. When it receives frames from the first layer, it de-encapsulates them, checks for errors and sends it up to the network layer.

Functions and Tasks

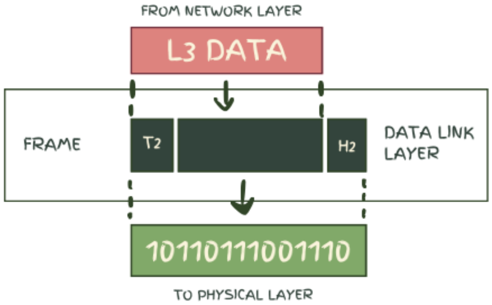
1. **Framing:** Encapsulation of network layer packets into frames
2. **Error checking:** Uses Cyclic Redundancy Check to detect, but not correct, errors.
3. **Physical addressing:** Assigns and uses MAC addresses to deliver frames within the same network segment
4. **Media Access Control (MAC):** Uses protocols like CSMA/CD and CSMA/CA to decide how devices share and access the network

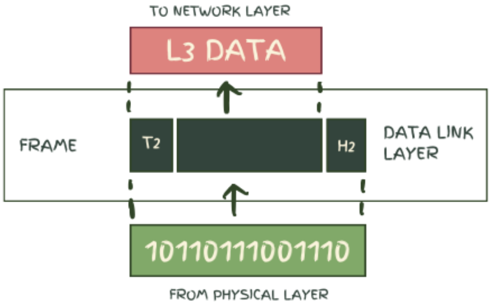
Real-World Protocols

Ethernet (IEEE 802.3): Provides connectivity in wired LANs, offers reliable framing, MAC addressing, and high-speed communication (such as Gigabit Ethernet)
Wi-Fi (IEEE 802.11): Provides connectivity in wireless LANs, helps mobile and IoT devices connect through CSMA/CA.
VLAN Tagging (IEEE 802.1Q): Tags Ethernet frames with IDs which segments network traffic, which helps security, scalability and isolation
MACsec (IEEE 802.1AE): Provides encryption for communication on this layer, which protects traffic between network devices.
Other examples of low-power wireless protocols: **Bluetooth, WiMax,** and **Zigbee/LoRa** for IoT use cases

Real world examples:

- Public WiFi- Hotels/cafes etc uses Wi-Fi to connect multiple users while managing access using media access control, same for home Wi-Fi
- IoT- Zibee is used in smart homes to power low-power items like light switches/thermostats etc
- VLAN- In enterprises, VLAN tagging isolates the employee networks from guest traffic for better security
- Office LANs- Printers, PCs, and servers are connected using Ethernet protocol for fast and reliable data transfer





PHYSICAL LAYER

The **Physical Layer (Layer 1)** consists of various network components such as power plugs, connectors, receivers, cable types, etc. Without the physical layer, there would be no network. It plays a crucial role in determining the data transfer rate, distance limitations, and signal quality to ensure efficient communication.

Functions and Tasks

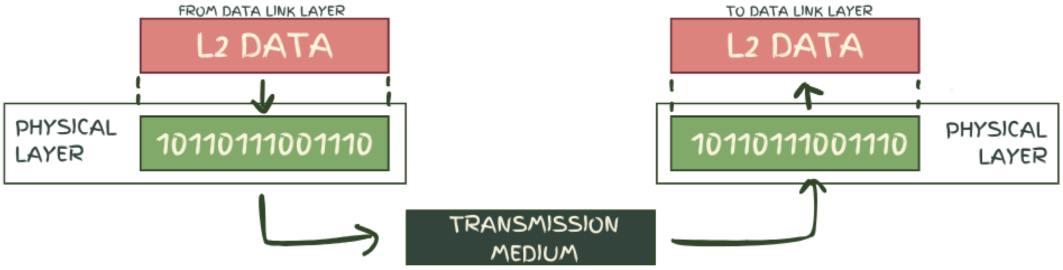
1. **Data Transmission:** Maintains the data rate (amount of bits sent per second) and performs the synchronization of bits.
2. **Transmission Medium and Selection:** Chooses the appropriate medium (e.g. copper wires, fiber optics) for data transfer based on factors like speed, distance, and cost.
3. **Physical Interface Specification :** Defines hardware-level standards like pin configurations, voltage levels, and connector types for device compatibility.
4. **Error Detection and Correction :** Aims to identify and minimize errors that occur during data transmission due to noise, attenuation, or interference.
5. **Signal Modulation and Encoding :** Uses signal modulation (AM, FM, PM) to embed data into a carrier signal and encoding (4B/5B) to convert digital data into suitable formats for transmission, ensuring effective data transmission and minimize errors.

Real-World Protocols and Relevance

Ethernet (IEEE 802.3): Connects devices in local networks using cables like twisted pairs or fiber optics to transmit data.
Wi-Fi (IEEE 802.11): Provides wireless internet access using radio signals, enabling device connectivity without cables.
Bluetooth (IEEE 802.15.1) : Allows short-range wireless connections between devices, like phones and headphones.

Examples such as:

- **Ethernet Cables:** Connects devices in a local network using for stable wired internet access.
- **Wi-Fi:** Accessing the internet wirelessly in homes, offices, or public places through Wi-Fi routers.
- **Fiber Optic Internet:** Provides high-speed internet connections for cities or businesses.



ADVANTAGES & CHALLENGES OF THE OSI PROTOCOL STACK

Advantages

Layered Architecture: The seven layers of OSI model simplifies troubleshooting and development by isolating issues within specific layers. The structured approach joins new technologies, supporting innovation and scalability.

Reduces Complexity: The OSI model simplifies technical processes by breaking down complex networking tasks into smaller and manageable layers for better understanding and implementation.

Enhanced Security: Security measures, like encryption at the presentation layer and firewalls at the network layer, applied to the different layers provides a multilayered defense approach.

Flexibility: The OSI model offers flexibility in development. For example, upgrades or updates to different layers can be done without affecting other layers.

Support Various Services: The OSI model supports connection-oriented services for reliable data delivery, and connectionless services for prioritizing speed and efficiency.

Challenges

Theoretical Nature: The OSI model is a conceptual framework, not a practical implementation, hence it is more complex and difficult to implement and maintain as it requires more hardware, software, and resources than the TCP/IP model.

Complexity for simple networks: For small, straightforward networks, the seven-layer design of OSI can be overly complex.
Example: Home Wi-Fi network primarily relies on physical connections, IP addressing (Network Layer), and application-level protocols (HTTP, DNS), ignoring many other OSI layers.

Ambiguity in Certain Layers: The Session and Presentation layers often overlap in functionality with the Application layer, making them less distinct in real-world applications.
Example: Video streaming protocols like RTSP(Real-Time Streaming Protocol) handle session management at the Application Layer, bypassing the Session Layer entirely.

Overhead in Error Handling: Error handling is an essential part of communication networks. However, multiple layers handling error detection and correction independently can result in time delays and redundant retransmissions.
Example: A video stream transmitted via RTP (Transport Layer) over Wi-Fi (Data Link Layer) might have retransmissions at both levels, causing unnecessary delays.

Incompatibility with Existing Technologies: The OSI model was developed after many protocols were already in use, causing a mismatch between the model and these protocols.
Example: The TCP/IP model, which predates OSI, doesn't have separate Presentation and Session layers, so these layers are effectively unused in practical implementations of modern networks.

Design and Implementation of a Network

Part A: Design

Lab No.	Location	Lab Name	No of hosts per lab
1	3rd floor, University Building	HUMAC	8
2	SET's new building	Communications Labs	6
3	SET's new building	Advanced Wireless Lab	4
4	SET's new building	IoT Lab	8

1. List of Required Equipment
    a. Router: used to handle inter-subnet communication between HUMAC (Subnet 1) and SET Labs (Subnet 2); routers are used to segment traffic between different subnets to ensure proper routing.
    b. 2960-24TT switch x4: one for each lab; switches are used to connect all devices (hosts) within each lab and facilitate local communication.
    c. Extension switch: to connect the switches at the SET labs to the main router.
    d. PCs x22: End devices to check wired connectivity between the labs
    e. Laptop x4: End devices to check wireless connectivity in the lab
    f. AP-PT: used in the wireless lab. Access points are used to extend the network in the wireless lab for wireless devices.
    g. WPC300N x4: adapter to upgrade the laptops for wireless connectivity
    h. NM-1FGE x2: to allow fiber cables to connect the router and the switch
    i. NM-1CGE: module for GigabitEthernet connection.
    j. NM-1CFE x3: module for FastEthernet connection.
    k. Cables:
        - Copper Straight Through: for shorter distance connections; in the labs, within the building
        - Fiber: for longer distance connections; connecting to another building
    l. Patch panels and Racks: to organise and manage network cables effectively in each lab

2. Estimated Cost of Equipment

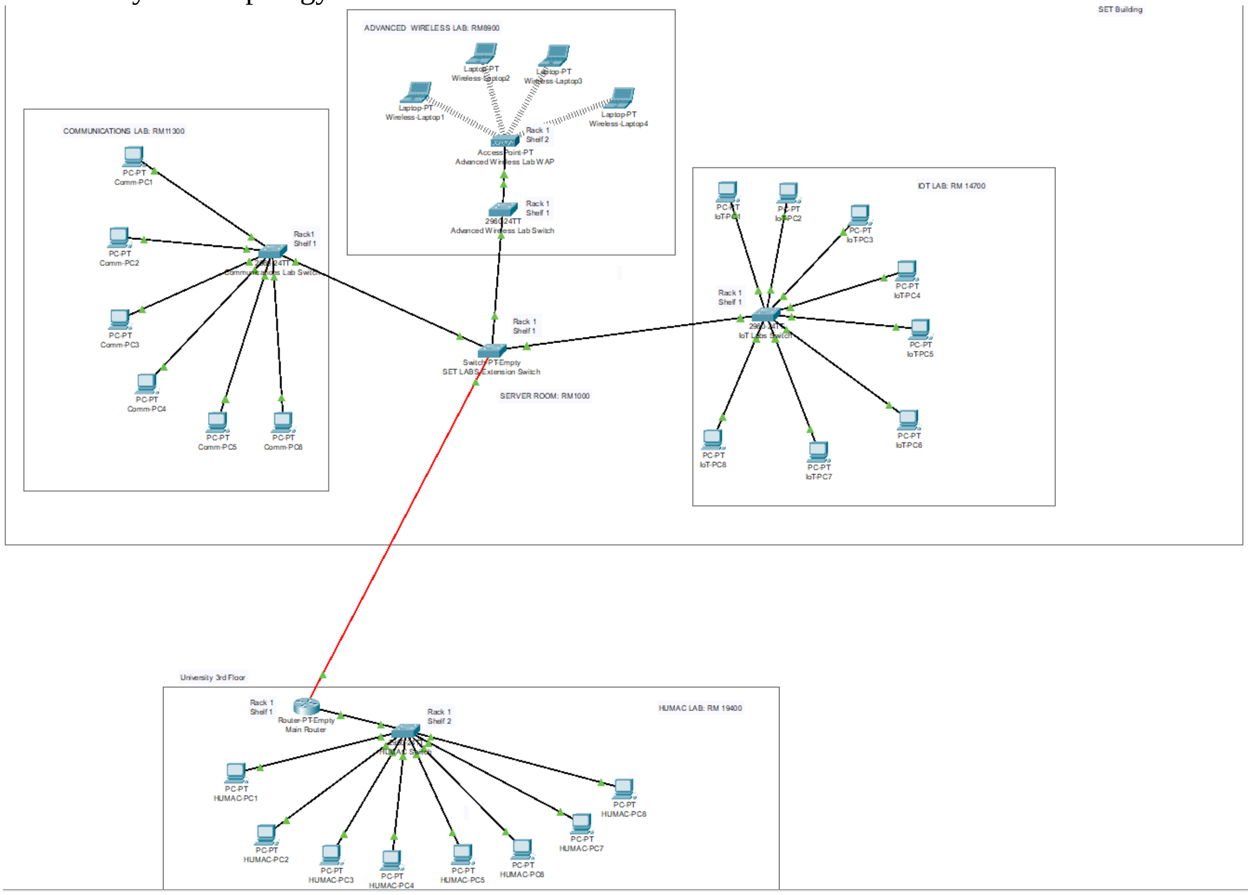
Equipment	Quantity	Unit Price (RM)	Total Cost (RM)
Cisco Router (e.g., ISR 1100)	1	4800.00	4800.00
Cisco Switch 2960-24TT (24-port)	5	1000.00	5000.00
Ethernet Cables (Cat6, 10m)	22	25.00	550.00
Fiber Cables (10 meters)	4	80.00	320.00
Access Points	1	600.00	600.00
Patch Panel and Rack	5	100.00	500.00
Access PC	22	1700.00	37400.00
Access Laptop	4	1800.00	7200.00

Total Estimated Cost **56370.00~++**

Source:
https://www.dell.com/en-my/shop/cty/pdp/spd/inspiron-3030-small-desktop/oid3030s700201mmy?tfcid=90375991&gacd=9654369-13065-5761040-272725660-0&dgc=ST&&gad_source=1&gclid=CjwKCAiA34S7BhAtEiwACZzv4aiJxEpM5Wkp-eH521Y2XbJq5IoAUNuqb2R_njh0-R7_o13Mn4_PrhoCtbMQAvD_BwE&gclsrc=aw.ds

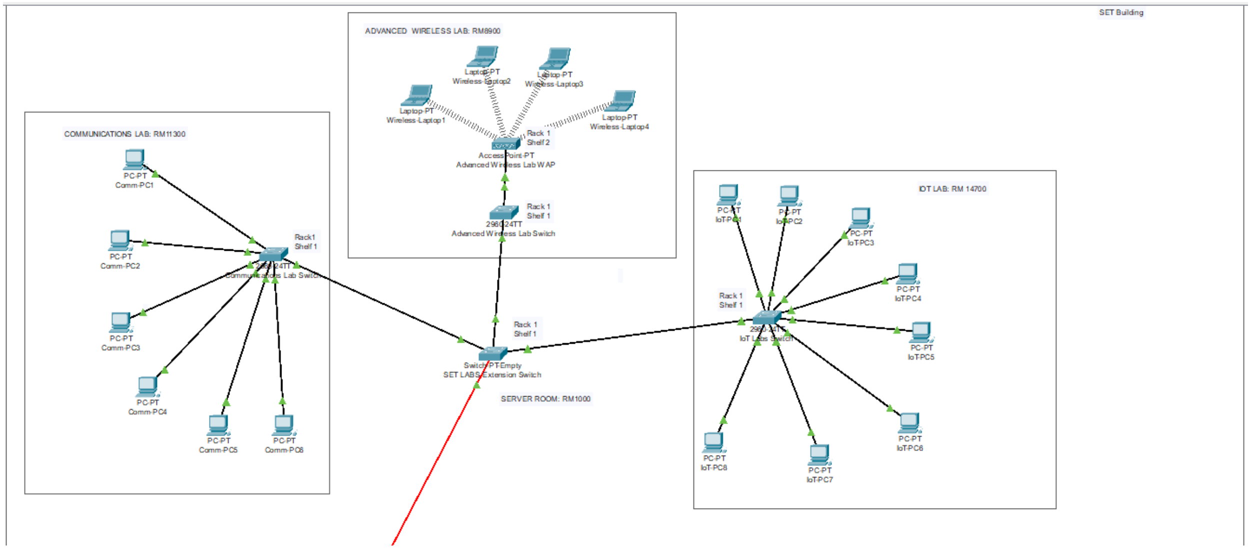
https://www.dell.com/en-my/shop/cty/pdp/spd/inspiron-15-3520-laptop/oin3520100201mmyh?tfcid=90375991&gacd=9654369-13065-5761040-272725660-0&dgc=ST&&gad_source=1&gclid=CjwKCAiA34S7BhAtEiwACZzv4ZFEi1TAAnRtlPIM0Q3iTmWlA9w98sysJ7UjtCVDwiZRI6Y1_3UOwhoCc-sQAvD_BwE&gclsrc=aw.ds

3. Physical Topology

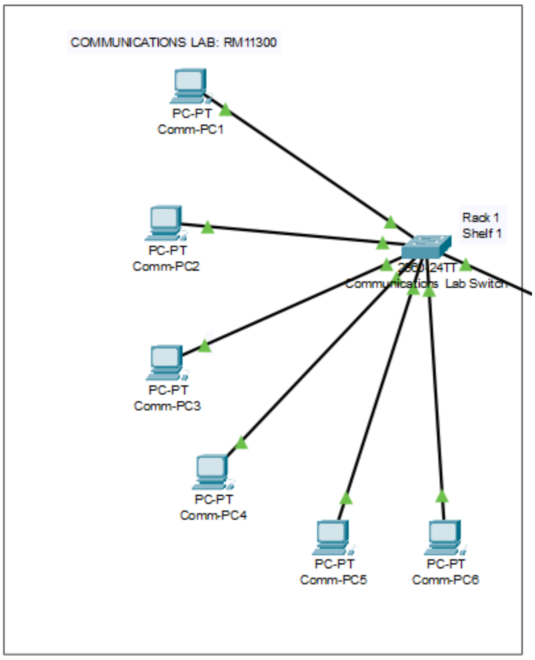


Topology of the entire network.

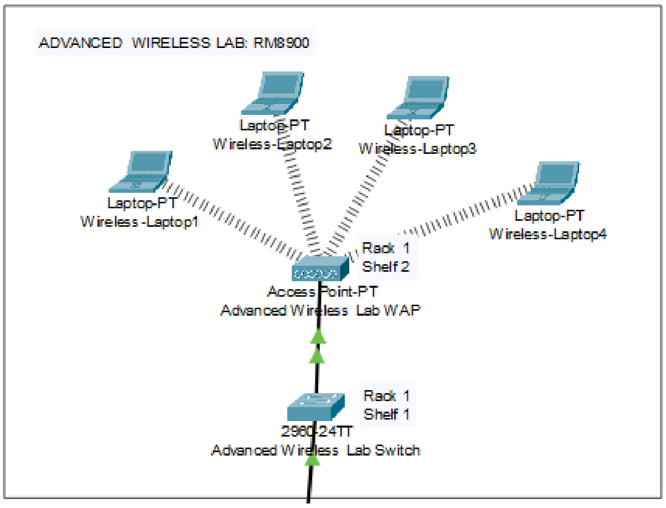
SET LABS BUILDING



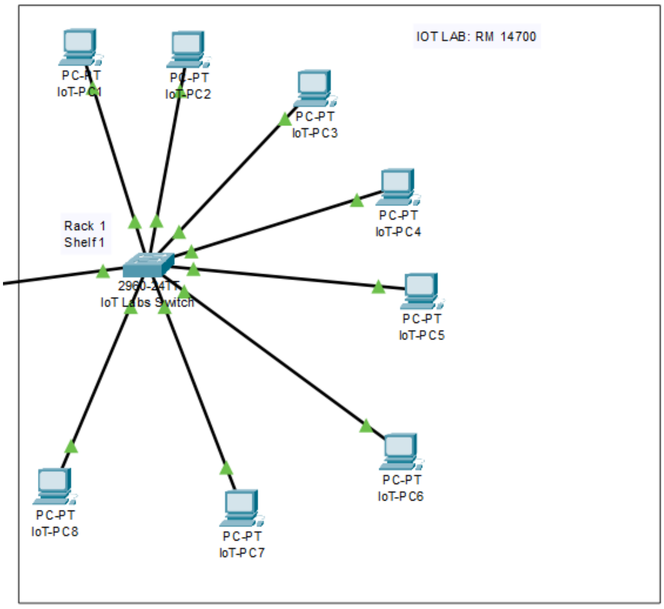
COMMUNICATIONS LAB



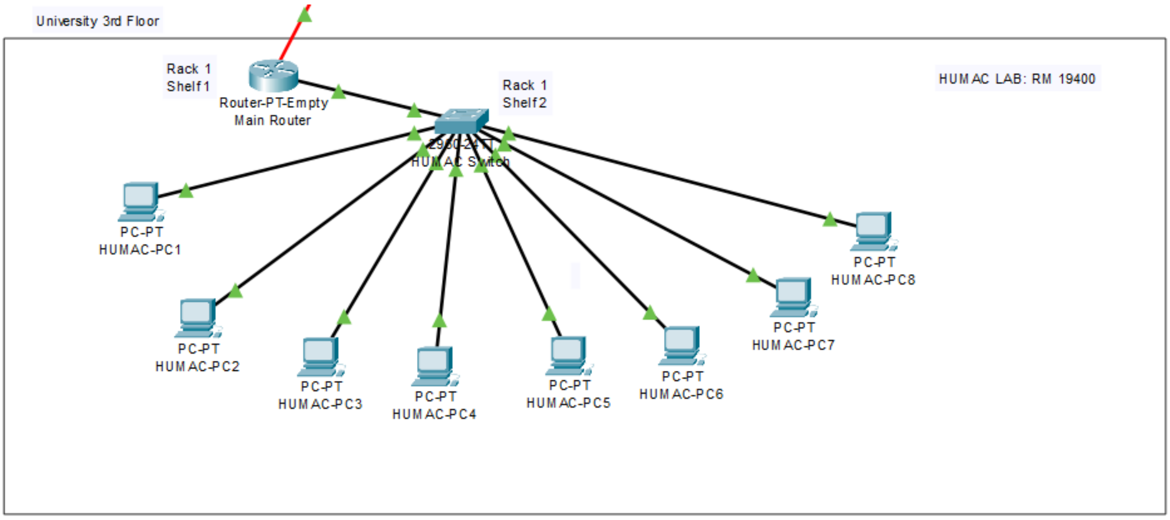
ADVANCED WIRELESS LABS



IOT LABS

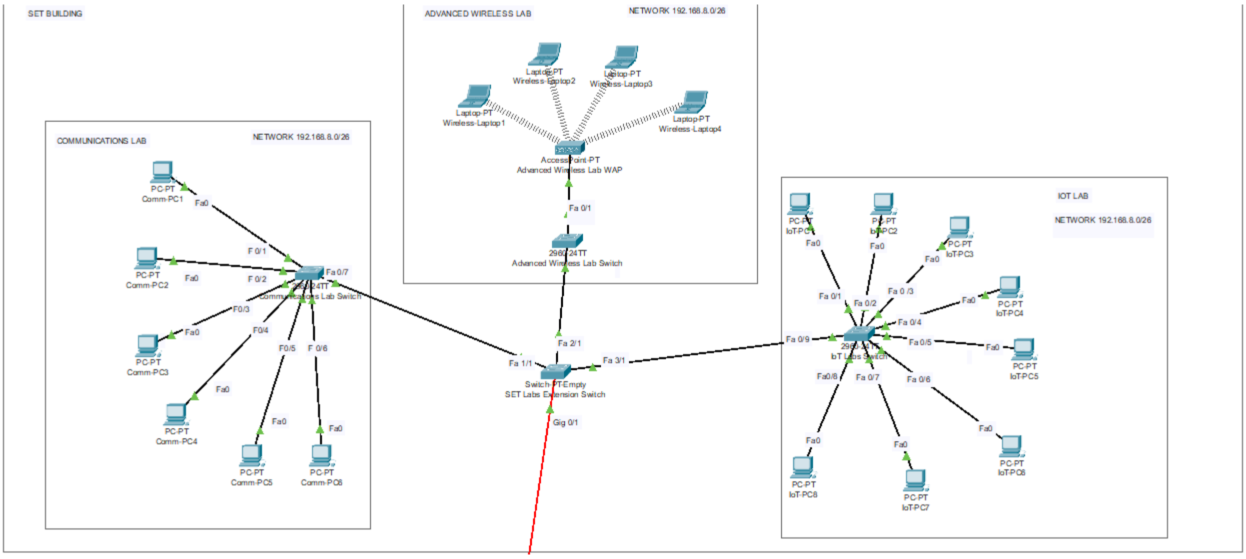


HUMAC LAB

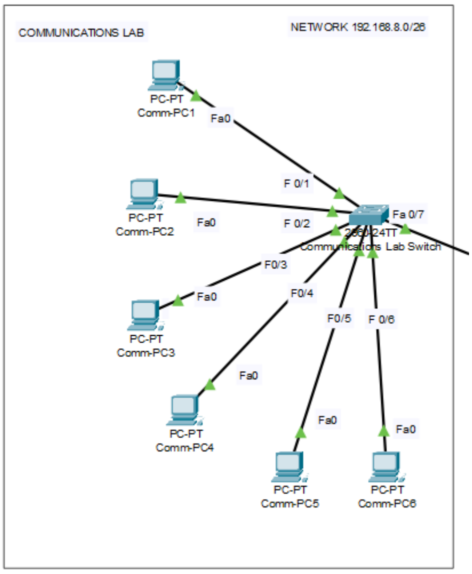

University 3rd Floor
Rack 1
Shelf1
Router-PT-Empty
Main Router
Rack 1
Shelf2
HUMAC LAB: RM 19400
HUMAC Switch
PC-PT
HUMAC-PC1
PC-PT
HUMAC-PC2
PC-PT
HUMAC-PC3
PC-PT
HUMAC-PC4
PC-PT
HUMAC-PC5
PC-PT
HUMAC-PC6
PC-PT
HUMAC-PC7
PC-PT
HUMAC-PC8

4. Logical Topology

SET LABS BUILDING

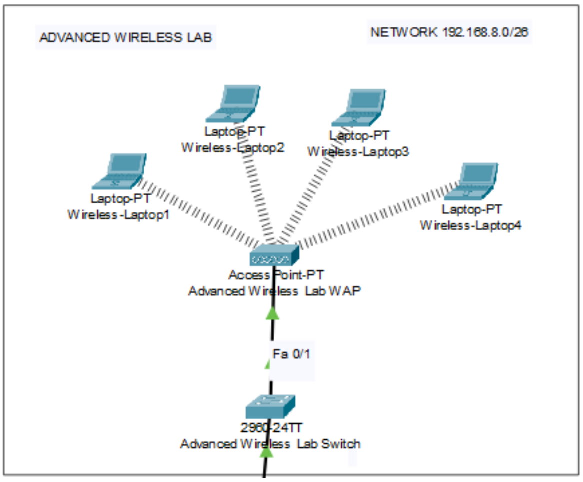


COMMUNICATIONS LAB



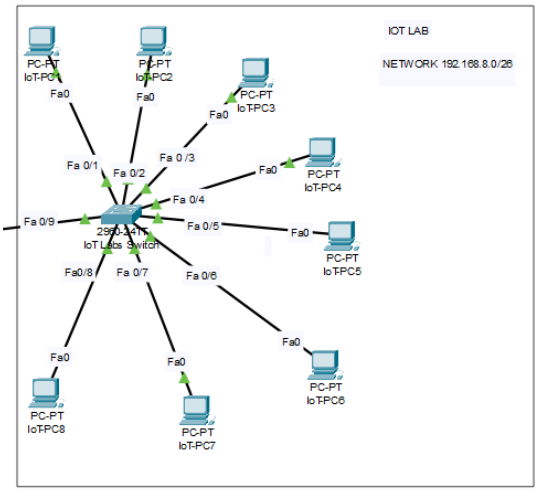
Device	IP address	Subnet Mask	Default Gateway
PC1	192.168.8.17	255.255.255.192	192.168.8.1
PC2	192.168.8.18	255.255.255.192	192.168.8.1
PC3	192.168.8.19	255.255.255.192	192.168.8.1
PC4	192.168.8.20	255.255.255.192	192.168.8.1
PC5	192.168.8.21	255.255.255.192	192.168.8.1
PC6	192.168.8.22	255.255.255.192	192.168.8.1

ADVANCED WIRELESS LABS



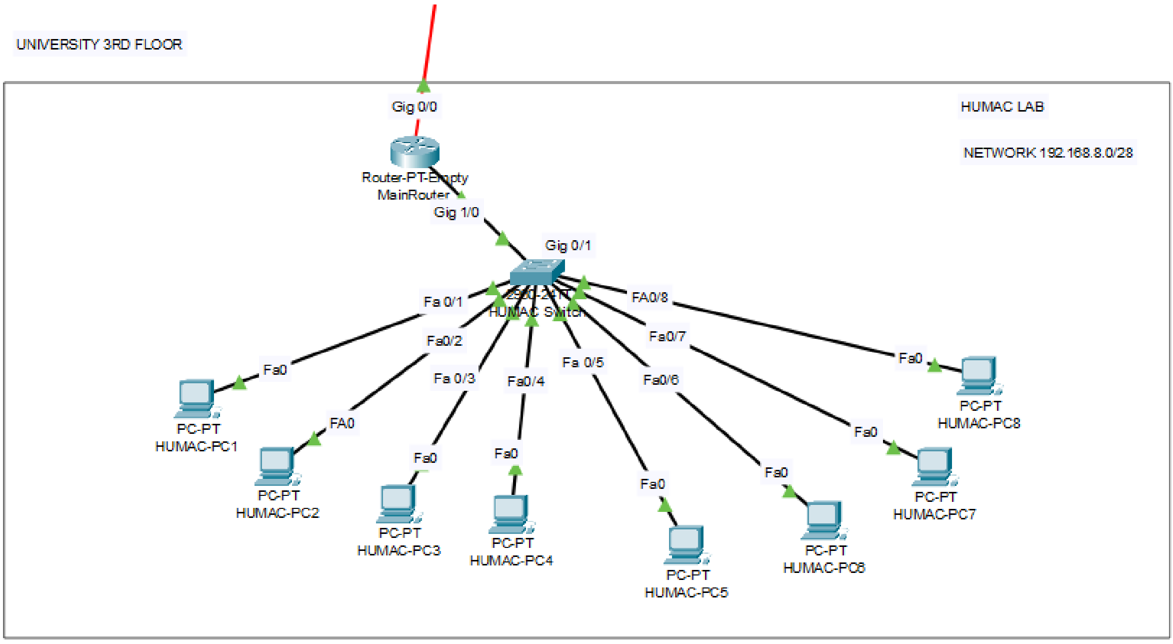
Device	IP address	Subnet Mask	Default Gateway
Laptop1	192.168.8.23	255.255.255.192	192.168.8.1
Laptop2	192.168.8.24	255.255.255.192	192.168.8.1
Laptop3	192.168.8.25	255.255.255.192	192.168.8.1
Laptop4	192.168.8.26	255.255.255.192	192.168.8.1

IOT LABS



Device	IP address	Subnet Mask	Default Gateway
PC1	192.168.8.27	255.255.255.192	192.168.8.1
PC2	192.168.8.28	255.255.255.192	192.168.8.1
PC3	192.168.8.29	255.255.255.192	192.168.8.1
PC4	192.168.8.30	255.255.255.192	192.168.8.1
PC5	192.168.8.31	255.255.255.192	192.168.8.1
PC6	192.168.8.32	255.255.255.192	192.168.8.1
PC7	192.168.8.33	255.255.255.192	192.168.8.1
PC8	192.168.8.34	255.255.255.192	192.168.8.1

HUMAC LAB



Device	IP address	Subnet Mask	Default Gateway
PC1	192.168.8.1	255.255.255.240	192.168.8.14
PC2	192.168.8.2	255.255.255.240	192.168.8.14
PC3	192.168.8.3	255.255.255.240	192.168.8.14
PC4	192.168.8.4	255.255.255.240	192.168.8.14
PC5	192.168.8.5	255.255.255.240	192.168.8.14
PC6	192.168.8.6	255.255.255.240	192.168.8.14
PC7	192.168.8.7	255.255.255.240	192.168.8.14
PC8	192.168.8.8	255.255.255.240	192.168.8.14

Part B: Implementation

Submission in pkt file

Part C: Lessons Learned

Teamwork Experience

Throughout the span of this assignment since it was released to us, it has highlighted the importance of effective and cohesive teamwork in order to achieve our goals, both in design and implementation of a mock network suited for the assignment's requirements. As such, we used a "split up" method to cover multiple parts concurrently, by dividing different areas of the assignment amongst the five members. We divided the work by having some members handle the setting up of each network between Set Labs and HUMAC Labs, while some handled the configuration and subnetting, and one more of us handled the report, cost calculation and topologies. With constant and clear communication being maintained throughout discussions and progress checkups, we managed to clarify any confusion effectively and dealt with any issues identified as soon as they appeared. Dividing the work as such has allowed all of us to stay motivated and feel supported by our groupmates, as seeing each other work hard makes us improve as well. Documenting each of our parts has also allowed us to pass on messages clearly whenever we send over a file for others to make any changes, reducing the chance of further confusion. Overall, working in a team has allowed us to grow and experience working in a team environment where we have to rely on each other to get work done.

Technical Challenges

Through the process of completing the assignment, a number of technical challenges came up, with the biggest issue being a subnet overlap, where two router interfaces with assigned overlapping subnets, leading to more configuration errors that took some time to pinpoint and solve. At the same time, in order for everything to flow smoothly, a lot of meticulous planning and checks had to be conducted to ensure proper connectivity between the numerous switches we had in place and each router interface. Apart from that, misunderstandings about the cable types and their intended use case also propped up to be a relevant point of problem which we had to figure out initially, alongside the need to adjust the IP addressing for the HUMAC Lab to avoid any unnecessary clashes with the addressings of the SET Labs. The configurations of the wireless access points and ensuring a stable inter-lab communications were also additional areas that required us to pay extra attention to.

Issue Resolution

After the ever so increasing number of issues kept popping up, the team had to approach each and every one of the issues individually in a systematic manner, leveraging both learnt problem solving techniques and networking knowledge passed to use throughout the semester. Something like the subnet overlap was resolved by redesigning the IP addressing plans, assigning individually distinct subnets to the HUMAC Lab and SET Labs. The testing tools provided such as the ping command and Packet Tracer's simulation mode played a big role in identifying and debugging such connectivity issues, with proper research and discussions leading to the most optimal configuration for the router interfaces and device IPs. The collaboration between team members undoubtedly played a key role in solving the problems of the wrong switch configurations and misunderstandings about the roles of each cable. Patience and iterative testing are the critical skills needed to achieve a smooth transition for the implementation.

Overall Experience

Through the process of completing the assignment, we have been given the opportunity to get valuable hands-on experience in designing and implementing a network with the key takeaways including the importance of proper subnetting, logical and efficient device placement, and the clear communication between teammates. Practical skills in networking such as router and switch configuration, IP addressing, and troubleshooting have also been particularly helpful and are important technical skills. It also highlighted the importance of careful and meticulous planning before beginning, multi phased implementations, and constant testing to ensure the successful creation of a network. Ultimately, this assignment has shown how hands-on learning is incredibly important for mastering real-world networking skills and concepts and to prepare for future challenges in the field.