SCHOOL OF ENGINEERING AND TECHNOLOGY

ASSIGNMENT COVER SHEET

COURSE: NET1014 – Networking Principles

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

ACADEMIC SESSION: January 2024 Semester

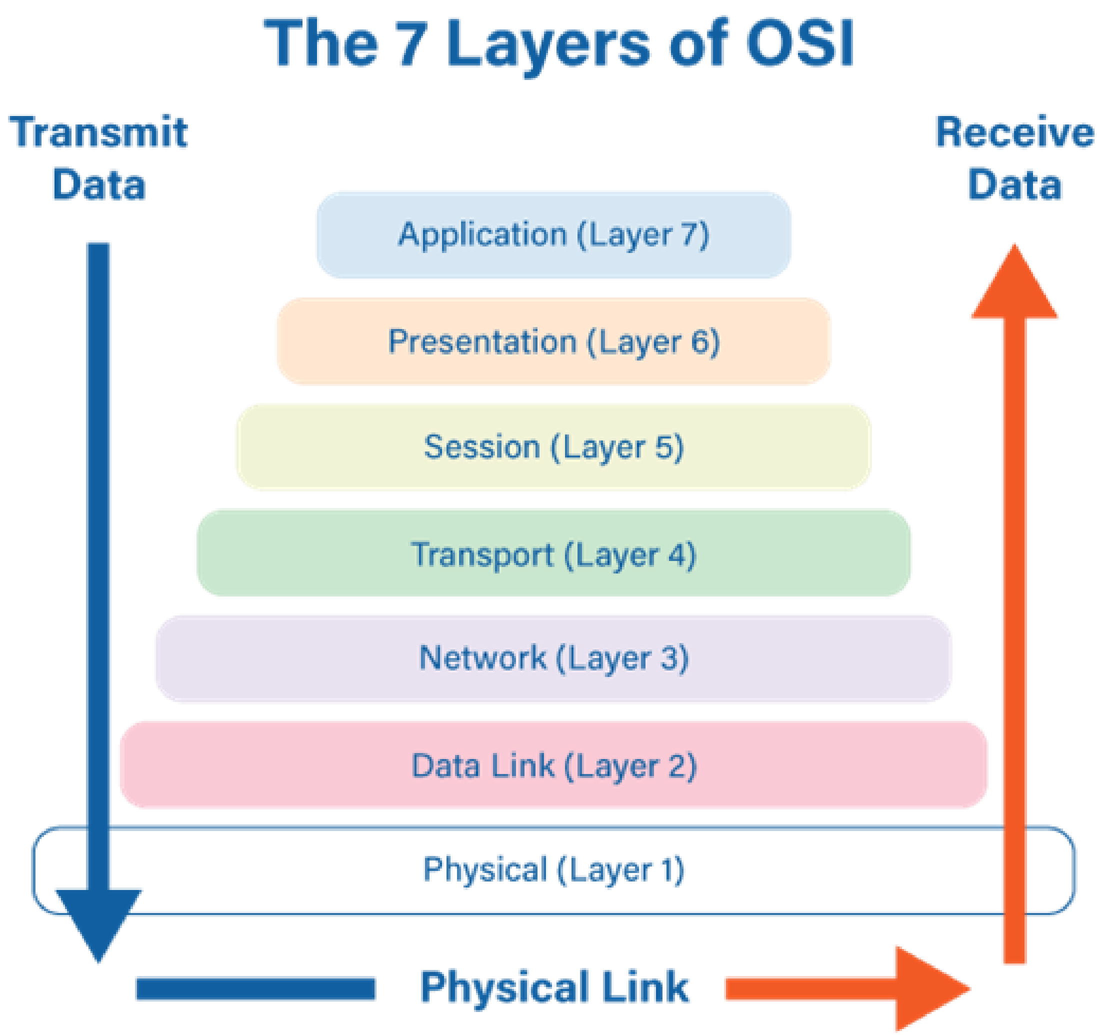
DEADLINE: 17th Mar 2024

GROUP NO: 5

#	Name	Student ID	Percentage of contribution
1	Wayne Kan Kah Weng	21099403	20 %
2	Goh Ci Yun	22017503	20 %
3	Lam Chee Hiew	22035455	20 %
4	Pu Xinyi	23026610	20 %
5	Ryan Ng Xu Yang	22025670	20 %

Table of Contents

I. Comprehensive Analysis of IOS Protocol Stack



OSI Layer	Function
OSI Layer 1: The Physical layer (managing the transmission of binary data)	It sets standards for voltage, signal timing, and modulation techniques, enabling the seamless exchange of information between devices and fostering compatibility across different networking technologies.
OSI Layer 2: Data Link layer (managing data transfer between physical transmission mediums and higher-layer protocols.)	It frames data into manageable units called frames, incorporating error detection, addressing, and control information. Governed by MAC sublayer coordinates access to the shared network medium. CRC enhances data reliability while assigning unique MAC addresses for efficient data delivery.
OSI Layer 3: The Network Layer (Facilitates data sharing across networks among end devices)	Configuration with end devices requires unique IP addresses for identification. Transforms PDUs from the transport layer into packets and inspects the IP header. Routing determines the optimal path for packet delivery to the destination host.
OSI Layer 4: Transport Layer (Manages logical communication between applications on different systems.)	Track individual conversations and data segments, Reassemble segments, and apply header information. Port Numbers identify target applications. Segmentation multiplexing and error checking occur in this layer.
OSI Layer 5: Session Layer (Establishes communication sessions between users across different machines.)	Session initiation, transfer of data and synchronization occur among end-user applications and ensure uninterrupted sessions between systems. When errors occur, data streams will be verified and allow selective retransmission in case of failure.
OSI Layer 6: Presentation Layer (Provides for common representation of the data transferred between application layer services.)	Handles data translation, encryption, compression, and formatting. Translates data between the application layer and network format. Encrypts data for security and compresses data for efficiency. Format data with headers, footers, or other information for presentation to the application layer.
OSI layer 7: Application Layer (Manages file transfer, access, and email services.)	Contains protocols for process communication, exchange messages and network management. Serves as the interface to the user to applications. Provides directory services like DNS/ LDAP.

Real-world examples of protocols used at each layer.

Physical layer: fiber-optic cable
- Fiber-optic cables transmit data signals in high-level data security fields of military and aerospace applications.

Data link layer: Point-to-point (PPP)
- establishing connections between a computer and an ISP to connect between a branch office and a central office.

Network Layer: IP
- IP addresses help identify the location of a device by accessing the connected internet.

Transport layer: Transmission Control Protocol (TCP)
- Used in applications that require guaranteed delivery of data, such as WhatsApp, Instagram, iMessage and more.

Session layer: NetBIOS
- It allows resource sharing such as files and printers, easier in local area networks.

Presentation layer: Secure Sockets Layer (SSL)
- provide encryption, data integrity, and authentication services to ensure that data transmitted between clients and servers remains confidential and secure.

Application layer: HTTP
- send hypermedia documents such as HTML files over the Internet.

Advantages of the IOS protocol stack and Challenges of the IOS protocol stack

Advantages	• High scalability. It is capable of overseeing thousands of devices and ensuring constant network performance. • Strong security measures to shield networks against malware, illegal access, and data breaches, among other threats. • Broad management capabilities. It provides graphical user interfaces (GUIs) for simpler management and a command-line interface (CLI) for configuration. • High reliability and stability, goes through extensive testing and development procedures.
Challenges	• High complexity, configuring and managing the IOS protocol stack can be difficult for inexperienced users. • High cost - IOS-based network implementation and maintenance can be quite expensive for small and medium-sized enterprises. • Time consuming, it takes specific training and certification courses for network administrators. • Security vulnerabilities - Cisco IOS is susceptible to security flaws and exploits even with its strong defenses.

II. Design and Implementation of a Network

Part A: Design

1. List of Required Equipment

No.	Equipment	Quantity
1.	Layer 3 Router	2
2.	Layer 2 Switch	5
3.	PC	11
4.	Laptop	9
5.	Wireless Access Point	3
6.	Printer	2
7.	HTTP Server	1
8.	DNS Server	1
9.	Tablet	1
10.	Smartphone	1

2. Estimated Cost of Equipment

No.	Equipment	Unit price (MYR)	Qty	Total price (MYR)
1.	Layer 3 Router (CISCO2911/K9 Cisco 2911 Router ISR G2)	6,603.53	2	13,207.06
2.	Layer 2 Switch (Cisco WS-C2950T-24 Catalyst 2950 24 Port Switch)	2,389.81	5	9,559.24

3.	PC (HP Slim Desktop PC S01-pF3006d)	2,599	11	28,589
4.	Laptop (ASUS ZenBook 14 OLED - UX3402)	4,799	9	43,191
5.	Wireless Access Point (Cisco Aironet 2802I Series Access Point Wireless AIR-AP2802I-K-K9)	2,309.99	3	6,929.97
6.	Printer (Sharp MX-M5654N A3 Mono Laser Multifunction Printer)	13,120.80	2	26,241.60
7.	HTTP Server	2000	1	2000
8.	DNS Server	2000	1	2000
9.	Tablet (Xiaomi Pad 6)	1,299	1	1,299
10.	Smartphone (Samsung - Galaxy A25 5G)	1,299	1	1,299
11.	Copper Straight-Through Cable	25.72 per meter	83	2,134.76
12.	Copper Cross-Over Cable	31 per meter	177	5,487
13.	Serial DCE Cable	37.05 per meter	184	6,817.20

Estimated Total Cost: RM 148,754.83

3. Physical Topology

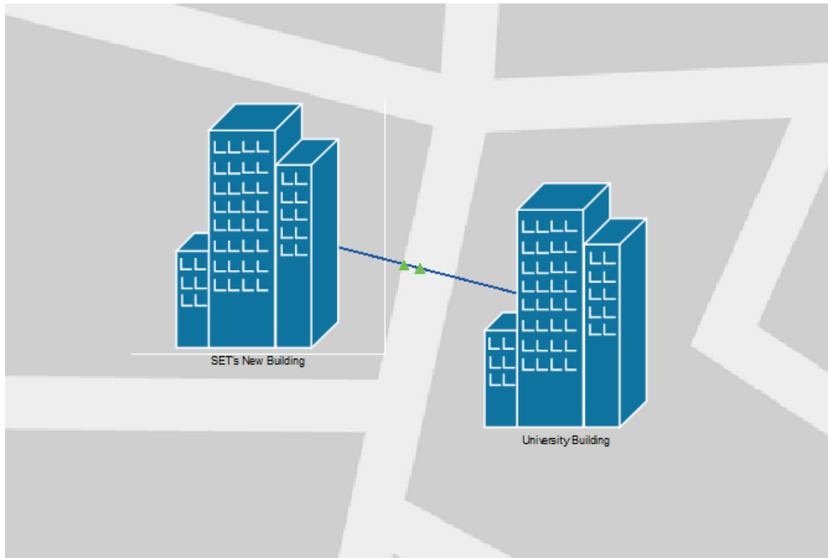


Figure 1 – SET's New Building and University Building

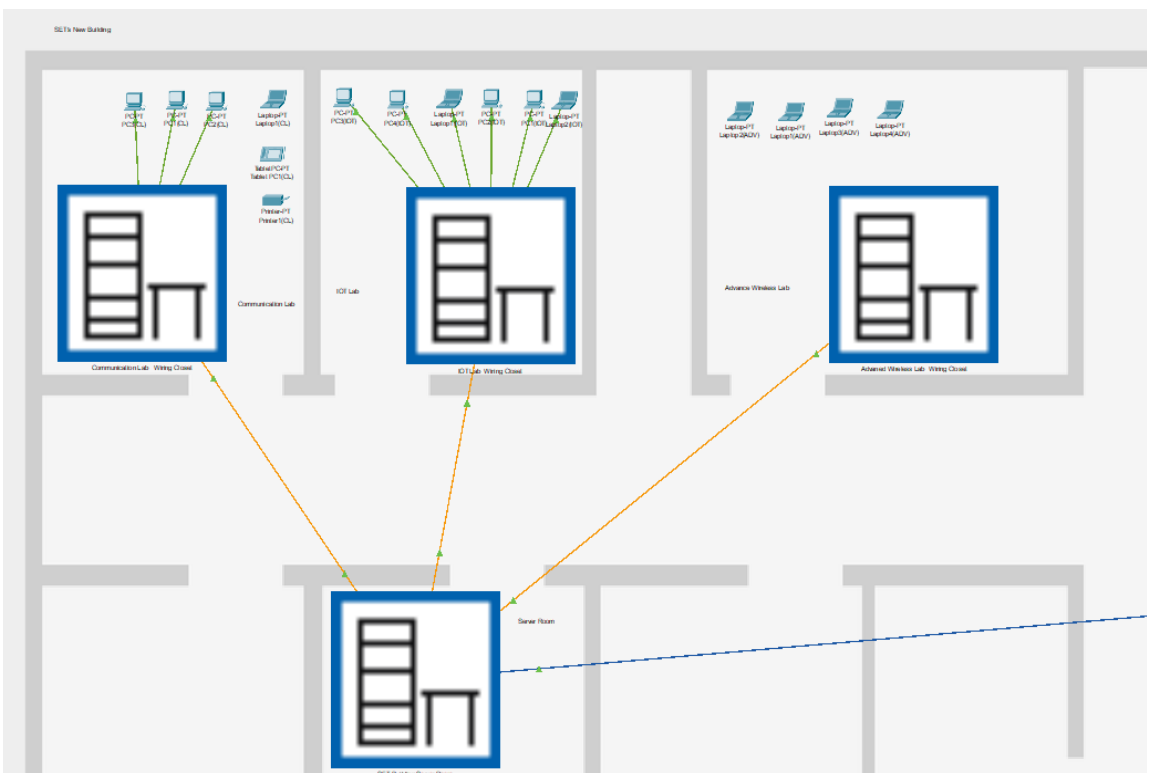


Figure 2 – SET's New Building Floor Plan

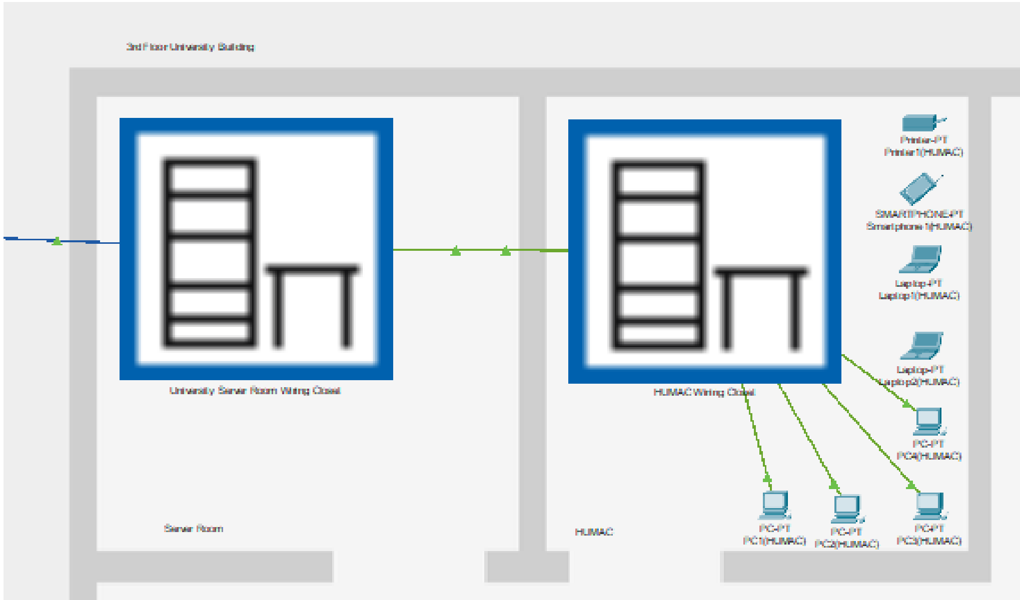


Figure 3 – University Building Floor Plan

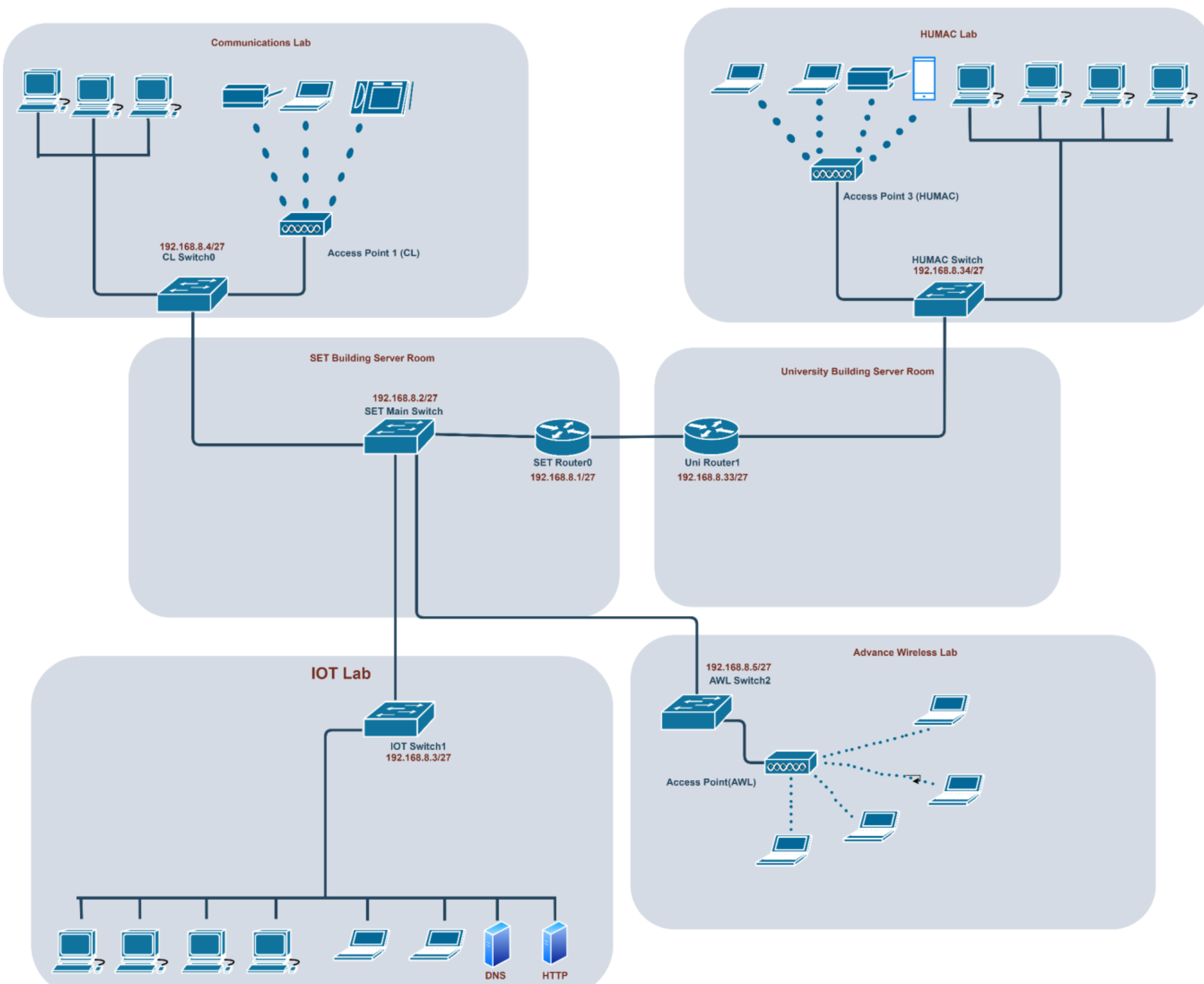


Figure 4 – Physical Topology of the Network Design

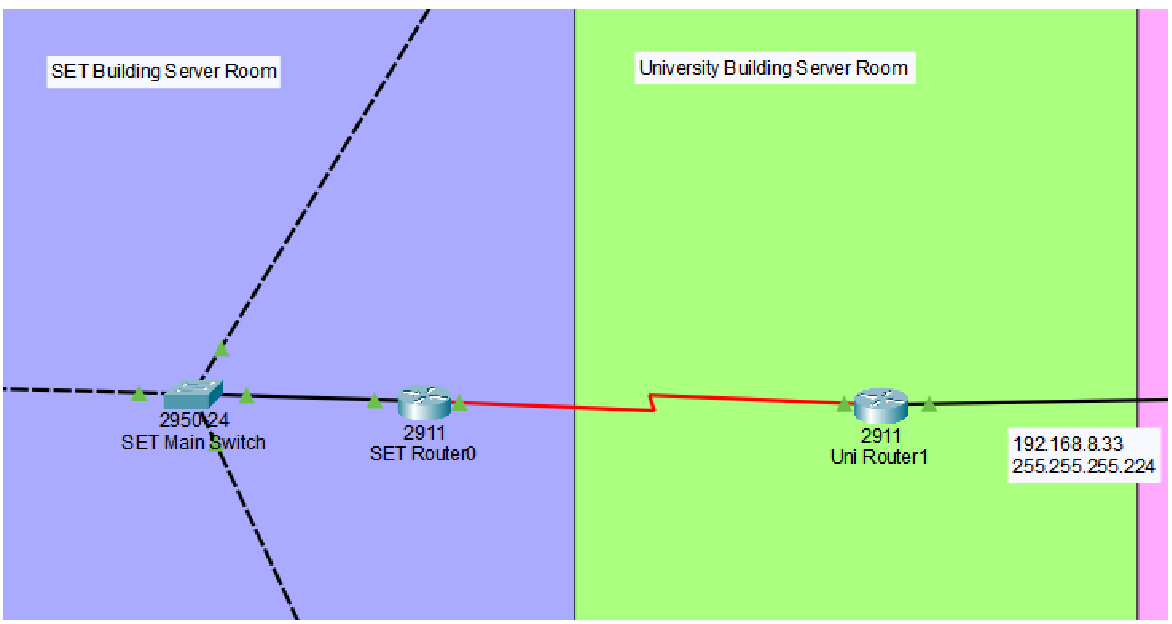
The physical topology (Figure 4) of the network comprises six rooms: the IOT Lab, Communication Lab, Advanced Wireless Lab, HUMAC, SET Server Room, and University Building Server Room. The IOT Lab, Communication Lab, Advanced Wireless Lab, and SET Server Room are situated in the SET New Building (Figure 2), while the HUMAC and University Building Server Room are located on the 3rd floor of the University Building (Figure 3). Physical access to network equipment is strictly controlled, with locked server room doors and access restricted to authorized personnel only.

Each building features a router positioned in the server room to oversee network connectivity. Additionally, a main switch in the SET Building Server Room interconnects the three labs in the SET New Building. All network devices, including routers, switches, and access points, are mounted on racks to optimize space utilization and ensure equipment safety.

Cable management is meticulously maintained, with cables organized in cable trays and secured with ties to prevent tangling and ensure easy identification. Each cable is labeled with its respective destination to facilitate troubleshooting and maintenance.

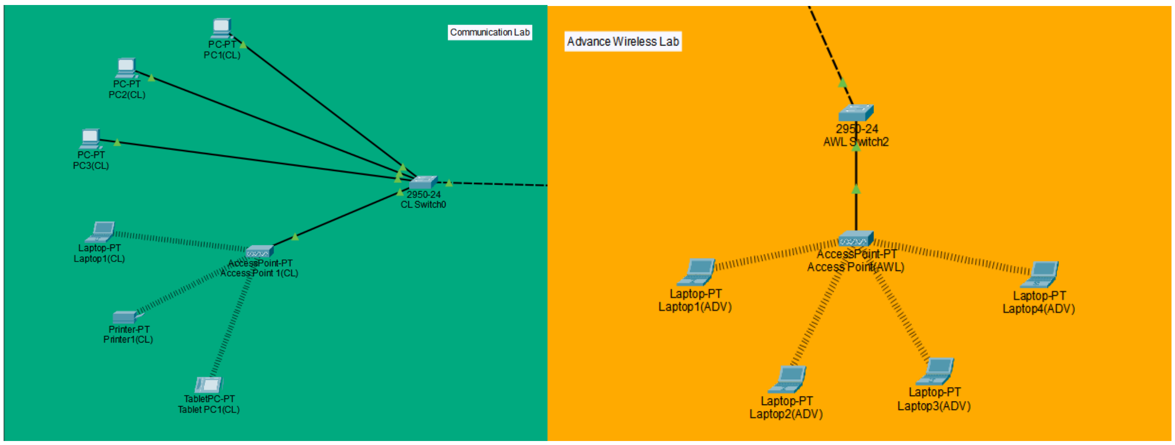
Overall, the network's physical layout is designed to deliver efficient connectivity and accessibility while prioritizing the safety and organization of network infrastructure. The comprehensive design considerations ensure that the network is not only reliable and secure but also scalable to accommodate future technological advancements and growth.

4. Logical Topology



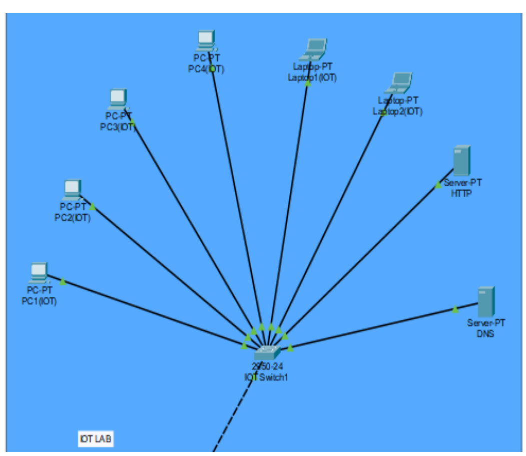
<u>Switch and Routers</u>

The main switch serves as a central hub connecting to various components of our network. It is responsible for interconnecting the switches for the labs in SET building. SET router configured with the subnet mask 255.255.255.224 to manage IP addressing within our internal network and establish connections with Uni Router and the main switch. Besides, Uni Router connects the HUMAC location to the internal network. It uses the same subnet mask (255.255.255.224) as the other locations to maintain consistency in IP addressing and facilitate communication between subnets.



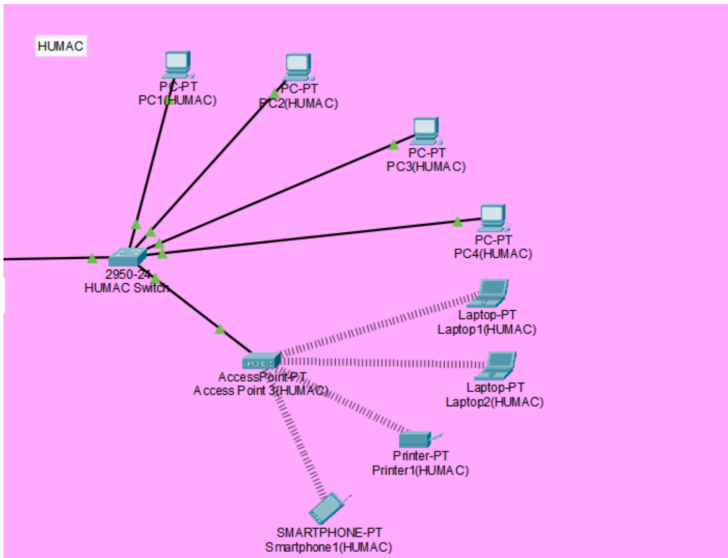
<u>Advanced Wireless Lab and Communication Lab Subnets</u>

These locations are configured with the subnet mask 255.255.255.224. However, unlike the IoT Lab, both the Advanced Wireless Lab and Communication Lab utilize DHCP for IP address assignment. DHCP offers dynamic IP allocation to devices in these labs, providing flexibility and scalability in accommodating various wireless devices and workstations. Besides that, the use of wireless access points increases scalability and flexibility, allowing for seamless integration of new devices or changes in device configurations, particularly between different semesters or projects.



IoT Lab

IoT Lab are configured with the subnet mask 255.255.255.224 as well, allowing for efficient management of IP addresses and network segmentation. Password-protected access ensures secure management of devices within each location and their respective switches. In the IOT lab, we have implemented a server that allows users to access the web browser by inputting the domain name of the website.



HUMAC

HUMAC operates in a separate subnet with the subnet mask 255.255.255.224, it maintains secure connectivity to the internal network through Uni router. Password protection adds an extra layer of security to device management and configuration within HUMAC.

Building	**Lab Name**	**Network Address**	**Switch Address**	**Usable Host Range**	**Broadcast Address**	**Subnet Mask**
SET’s New Building	Communication Labs	192.168.8.0	192.168.8.4	192.168.8.1-192.168.8.30	192.168.8.31	255.255.255.224
	Advanced Wireless Lab		192.168.8.5			
	IOT Lab		192.168.8.3			
3rd floor University Building	HUMAC	192.168.8.0.32	192.168.8.34	192.168.8.33-192.168.8.60	192.168.8.61	

Part C: Lessons Learned

Teamwork Experience:

To complete our first network design as a team, we had to make sure all the members were on the same page. Thus, we had everyone look through the instructions of the assignment before scheduling a meeting to enhance coordination. We effectively communicated with each other through discussions online and in person, sharing our thoughts on how we should approach. We used the internet extensively for research and also sought guidance from our practical class teacher to ensure that our design and implementation were aligned with the project's objectives. To tackle challenges such as conflicting opinions or uncertainty regarding the project's direction, we dedicated time to openly discussing these issues as a team and collaboratively work towards finding a solution. We had a member to lead the team and divided the tasks to enhance our teamwork and coordination.

Technical Challenges:

Some of the technical challenges we faced during the process included the inability of devices from the HUMAC lab to communicate with the lab in SET's new buildings. Additionally, we encountered issues where devices connected to a wireless access point were unable to communicate with other devices connected to a different wireless access point in another lab.

Issue Resolution:

We had been actively finding solutions such as checking the IP address, subnet mask, and default gateway for each router and devices. Not only that, but we have also tried testing the connectivity by pinging the IP address of other devices within the same subnet to note any "Request Timed Out" or "Destination Host Unreachable" messages. After countless Google searches, we were able to troubleshoot and resolve the network connectivity issues between the HUMAC lab and SET's new buildings.

Overall Experience:

Throughout the process of designing and implementing the network, our team gained invaluable experience and practical skills that have significantly enriched our understanding of networking principles and technologies. The collective journey provided us with a comprehensive learning opportunity such as problem solving and critical thinking where we learned to analyze complex network issues, identify root causes, and develop effective solutions through logical reasoning and experimentation. In conclusion, it is important to have hands-on learning in the field of networking as theory alone is insufficient, without practical application we may not be available to develops skills and competencies necessary for success in the dynamic field of networking engineering.