SCHOOL OF ENGINEERING AND TECHNOLOGY ASSIGNMENT COVER SHEET

COURSE: NET1014 – Networking Principles

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

ACADEMIC SESSION: February 2025 Semester

DEADLINE: 28th Mar 2025 – 11:59PM

#	Name	Student ID	Percentage of contribution
1	TEE YU QING	23077787	16.66
2	DING YEE QING	23080732	16.66
3	LEE HUI WEN	23079692	16.66
4	LIM SHAN EN	23080690	16.66
5	SIN SHEN NEE	23050024	16.66
6	DASHVIN KUMAR A/L SURESH KUMAR	24112070	16.66

I. Comprehensive Analysis of OSI Protocol Stack

Introduction

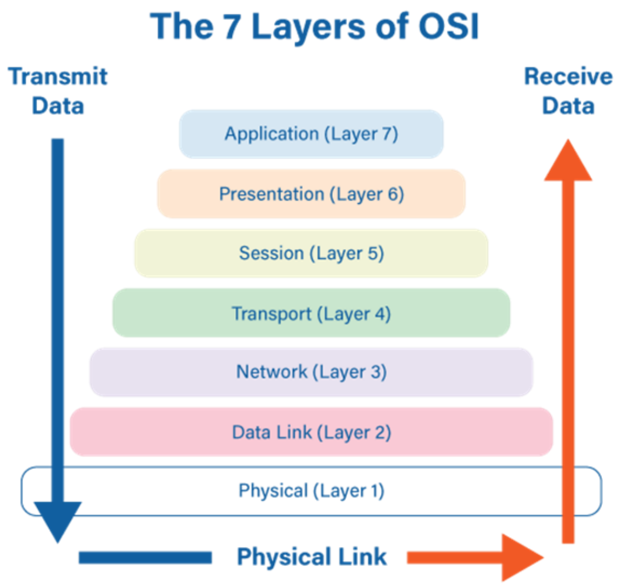


Figure 1.1 *shows the process of data transmission (client) and reception (server) through the 7 layers of the OSI model. (Source: Profitap)*

The Open Systems Interconnection (OSI) Model is a conceptual framework that helps us understand how devices communicate over a network. It was created by the International Organization for Standardization (ISO) to establish a universal standard for network communication. It divides network communication into seven layers, where each layer has a specific function. These layers work together to ensure smooth data transmission from one device to another.

This analysis will explain each of the seven layers, their functions, real-world examples, advantages, and challenges.

Layer 1: Physical Layer

Figure 1.2 *shows the transmission of raw binary data (bits) over physical media between two devices*. (Source: Imperva)

The Physical Layer transmits raw data bits over a physical medium to ensure proper data transfer between devices. It supports various transmission media, including copper cables for wired connections, fiber optics for high-speed data transfer, and wireless signals for communication without physical cables. A common example is a Wi-Fi router, which transmits data using radio waves, while fiber optics uses light pulses for high-speed internet transmission.

Layer 2: Data Link Layer

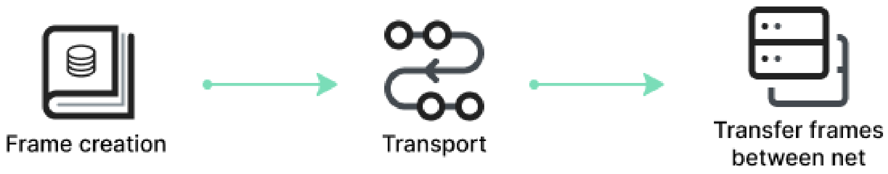


Figure 1.3 *illustrates how data is organized into frames, transmitted, and transferred between local networks.* (Source: Imperva)

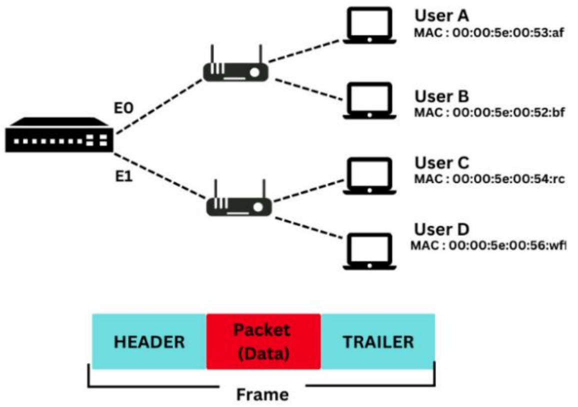


Figure 1.4 *displays how devices use MAC addresses for communication and how data is framed with headers, packets, and trailers.* (Source: DarkRelay)

The Data Link Layer manages physical addressing through MAC addresses, handles error detection, and controls data flow to ensure smooth communication between devices within the same network. It operates using protocols such as Ethernet, ARP, PPP, and VLAN to facilitate data transmission. In local area networks (LANs), Ethernet frames help devices communicate effectively by organizing data into structured packets.

Layer 3: Network Layer

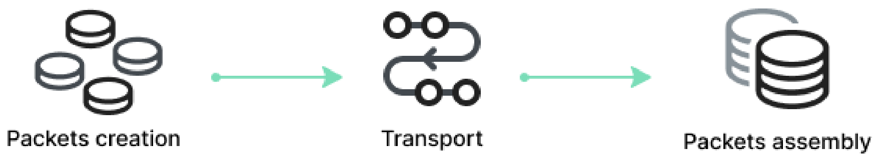


Figure 1.5 *demonstrates packet creation, routing, and delivery across different networks.* (Source: Impreva)

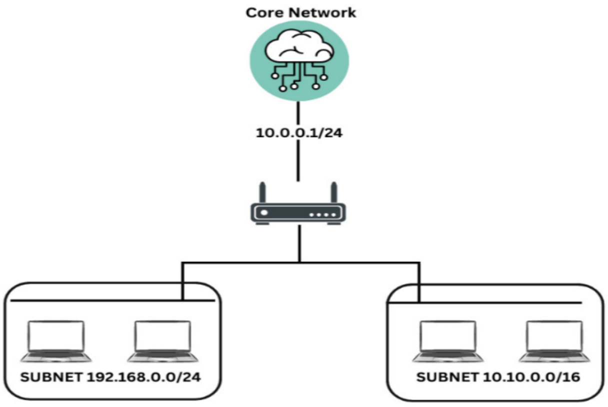


Figure 1.5 *how a core network connects to different subnets through IP addressing and routing.* (Source: DarkRelay)

The Network Layer determines the best path for data transmission and assigns logical addresses (IP addresses) to devices, allowing communication across multiple networks. It uses protocols such as IP, ICMP, RIP, and OSPF to route packets efficiently. For example, IP addresses enable devices to send and receive data over the internet, while routing protocols like OSPF help select the most optimal path for transmission.

Layer 4: Transport Layer

Figure 1.6 *shows the process of segmenting data, transporting it across the network, and reassembling it at the destination.* (Source: Impreva)

The Transport Layer ensures end-to-end communication, manages error detection, and maintains data integrity to ensure reliable data delivery. It operates using two main protocols: TCP (Transmission Control Protocol), which guarantees that all packets arrive correctly and in order, and UDP (User Datagram Protocol), which prioritizes speed over accuracy. A real-world example is TCP's role in email transmission (SMTP) to ensure complete message delivery, while UDP is used in live streaming, where speed is more important than perfect accuracy.

Layer 5: Session Layer

Figure 1.7 *demonstrates how the Session Layer establishes, manages, and secures communication sessions between clients and servers.* (Source: Impreva)

The Session Layer manages communication between source and destination applications. It establishes, maintains, and terminates session connections to ensure an efficient data exchange. It also handles session recovery and checkpointing, allowing sessions to continue after interruptions. Notable protocols in this layer include NetBIOS and Remote Procedure Calls (RPC). For example, RPC can be used in remote desktop applications and audio/video conferencing tools to perform tasks on remote servers.

Layer 6: Presentation Layer

***Figure 1.8** represents the key functions of Layer 6, which performs data encryption, compression, and translation, to ensure data is in a readable and secure format.* (Source: Impreva)

The Presentation Layer translates data from the source device into a compatible format for the destination device. It involves data compression to reduce size and ensures it can be decompressed by destination devices, using formats such as JPEG for images, MPEG for videos, and MIME for emails. It also encrypts data before transmission and decrypts it upon arrival through SSL and TLS protocols. A good example is secure data transmission during online banking and e-commerce, where this layer ensures data is encrypted and properly formatted for communication between users and servers.

Layer 7: Application Layer

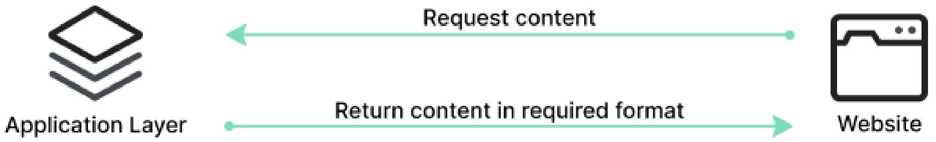


***Figure 1.9** illustrates how user applications request and receive content from a website in the required format.* (Source: Impreva)

The Application Layer provides the interface between applications used to communicate and the underlying network over which messages are transmitted. Standard protocols used include HTTP (Hypertext Transfer Protocol), DNS (Domain Name System), and FTP (File Transfer Protocol). For example, HTTP is used to access and exchange multimedia content, including text, audio, images, and video on the World Wide Web.

Advantages & Challenges of OSI Protocol Stack

Advantages:

Figure 1.10*: Advantages of OSI – Security.* (Source: PNGTree)

•**Standardization**: OSI provides a universal structure for network communication

•**Modularity**: Each layer works independently, making troubleshooting easier

•**Security**: Encryption at the Presentation Layer (TLS/SSL) and Transport Layer (TCP security features) improves security.

•**Interoperability**: Devices from different manufacturers (Cisco, HP, Dell) can communicate using the same protocols.

Challenges:

- **Complexity**: Some layers (like Session & Presentation) are rarely used separately in real-world networking.
- **Performance Overhead**: Passing data through seven layers can slow down processing.
- **Outdated Model**: Many modern networks use the TCP/IP model, which simplifies the OSI structure into four layers.

Figure 1.11*: Disadvantages of OSI – Performance overhead.* (Source: Freepik)

Conclusion

The OSI model remains a foundational framework in networking, offering a clear, seven-layer approach to understanding how data is transmitted across networks. While modern networks often simplify models like TCP/IP, the OSI model is a valuable educational tool and reference for designing, troubleshooting, and maintaining interoperable communication systems over networks. Its focus on standardization, modularity, and security helps simplify complex network processes and improve compatibility between different devices. Although some layers, such as the Session and Presentation Layers, are less prominent in practice, the OSI model still plays an essential role in explaining how reliable and secure data transmission works in today's complex networking environments.

II. Design and Implementation of a Network

Part A: Design

List of Required Equipment

Type	Equipment	Justification
Router	Cisco ISR4331/K9 (SU_Router)	Serves as a core router and main gateway for the network, providing maximum bandwidth and connecting additional routers or switches to the network. It interconnects different labs and handles the main traffic flow in the network. This model allows for high performance and ensures that data transmission is smooth throughout the network in multiple labs. It also has advanced security features like firewall, VPN and threat protection to protect the entire network.
	Cisco 2911 (SET_Router)	Serves as a distribution router. Used to segregate the network within the SET building to reduce congestion in the core router. It connects SET labs together and handles communication between them. This model has a lower cost and power consumption compared to the core router and is more suitable for small-scale routing tasks like offloading traffic and backup routing.
Switch	Cisco 2960-24TT Switch	Main function of the switch is to provide wired connectivity to the end devices. Each lab has a switch to ensure efficient traffic management and reduce congestion in the router. They allow for local communication within each lab network without overloading the routers. Furthermore, the switch has 24 ports, which is enough to accommodate and connect all required devices in each lab. The Cisco 2960-24TT Switch model is also cost-effective for the network as it is affordable yet sufficient since most end devices, namely the PCs, laptops, and printers, use Fast Ethernet.
End Device	PC	PCs function as workstations for staff and students to access the network in the labs. They can use it for general computing and lab work, such as coding, simulation, and networking tasks. While they are not portable like laptops, PCs possess higher processing power and stability, making them suitable for fixed workspaces such as lab environments where students perform intensive tasks, all whilst connected to the network.

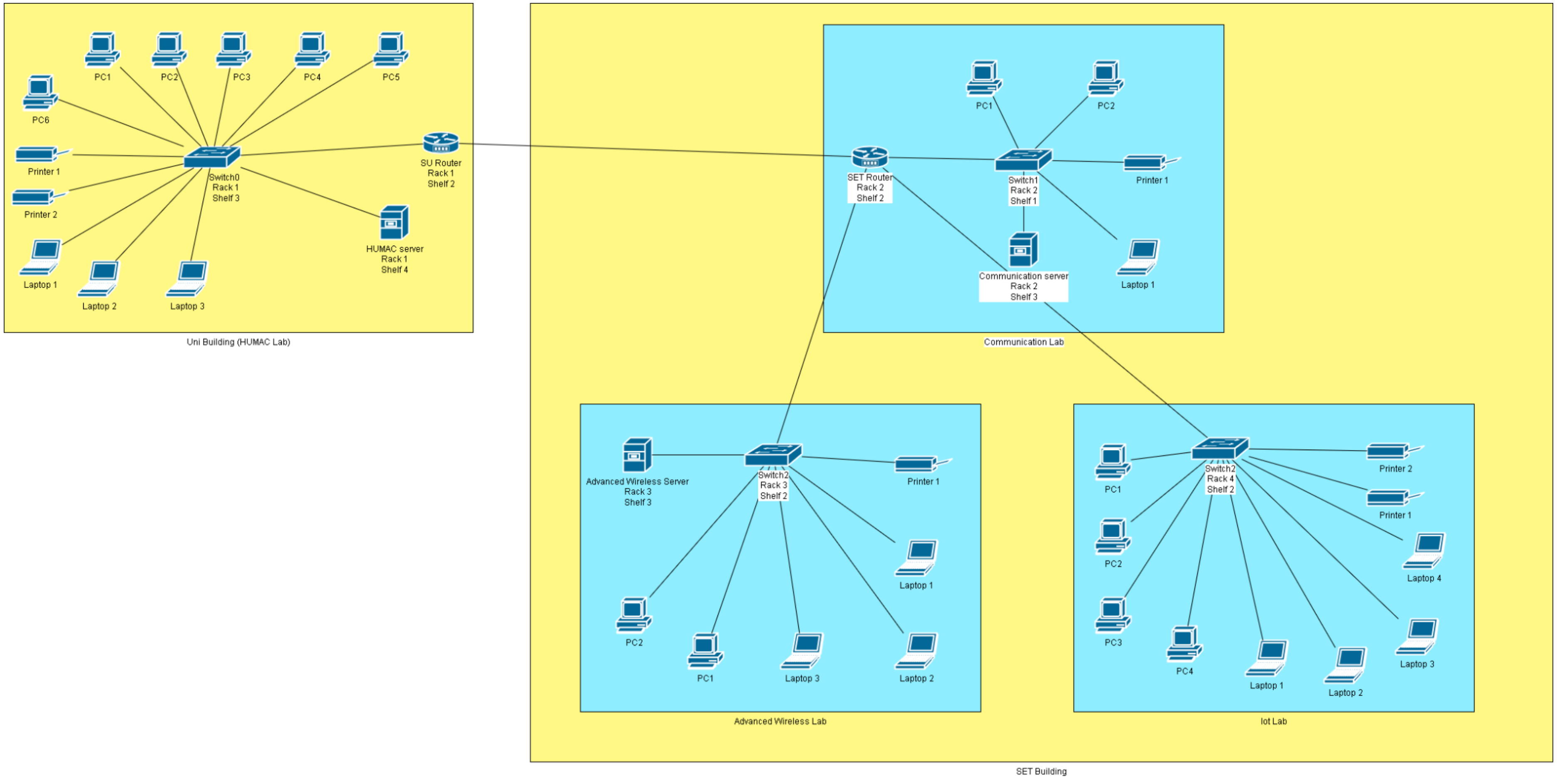
	Laptop	Laptops also function as workstations for both staff and students but are more portable than PCs. This enables them to carry out tasks on the go as it is able to connect to the network wirelessly when necessary. They are essential in labs where mobility is required, such as the Advanced Wireless Lab and IoT Lab, where wireless testing for networking experiments may be conducted. In other labs, they are useful for when students may work remotely and collaborate.
	Server	Servers function as centralised data storage, processing, and network resource management. Each lab, except the IoT Lab, has a dedicated server to handle specific tasks. For example, the server in the HUMAC Lab centralises file storage and user authentication, the Communications Lab's server manages communication software and file sharing, and the Advanced Wireless Lab's server runs network simulations and experiments. Whereas the IoT Lab does not require a server because many IoT applications process data in the cloud rather than on local servers.
	Printer	Used for printing hard copies of reports, academic materials, network designs, and documentation. The printers are connected to the network via switches, which allows easy file sharing for efficient printing. Increase convenience by having one in every lab to ensure quick access to physical documents for presentations and tests for both staff and students.
Cable	Copper Straight-though	Used to connect end devices such as PCs, printers, laptops, and servers to switches, as they operate at different network layers, that being Layer 3 and Layer 2, respectively. This allows end devices to access the network via the switch. It is also used to connect switches to routers as they are different device types, ensuring smooth packet forwarding between different subnets.
	Serial DCE	Used to connect router to router to form a WAN connection. This allows communication between both buildings and different subnets in the network.

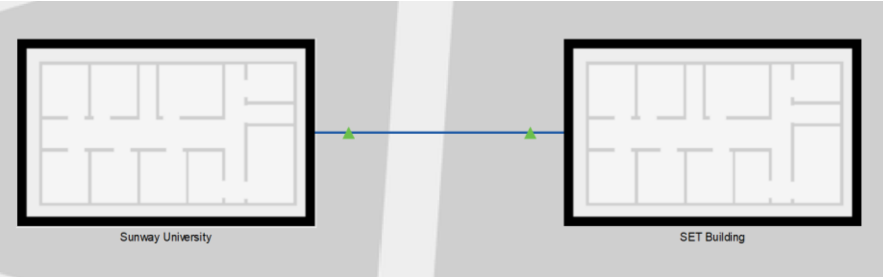
Estimated Cost of Equipment

Item	Type	Brand	Quantity	Price / item (RM)	Subtotal (RM)	Source
ISR 4331	Router	Cisco	1	6800.00	6800.00	Router SU
NIM-2T	Module	Cisco	1	2068.80	2068.80	Module 1 Router SU
NIM-ES2-4	Module	Cisco	1	856.00	856.00	Module 2 Router SU
2911	Router	Cisco	1	971.00	971.00	Router SET
HWIC-4ESW	Module	Cisco	3	560.30	1680.90	Module 1 Router SET
HWIC-2T	Module	Cisco	1	905.10	905.10	Module 2 Router SET
2960-24TT	Switch	Cisco	4	471.00	1884.00	Switches
PC	End Device	HP	14	2599.00	36386.00	PCs
Laptop	End Device	HP	11	1397.00	15367.00	Laptops
Printer	End Device	HP	6	539.00	3234.00	Printers
Server	End Device	Dell	3	4700.00	14100.00	Servers
Serial DCE	Cable	Cisco	1	120.68	120.68	Cable 1
Copper Straight Through (3m)	Cable	Cisco	38	74.00	2812.00	Cable 2

Total (RM)	87185.48

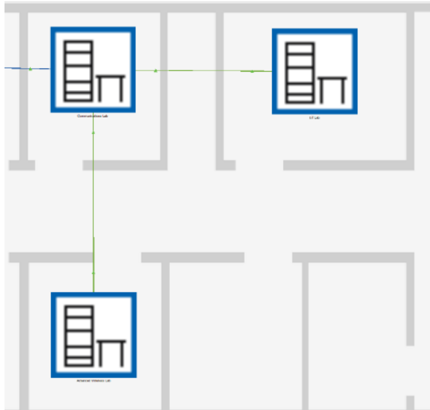
Physical Topology



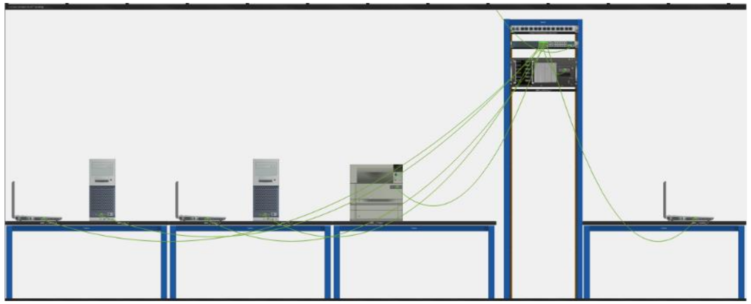


Router Connection from Sunway University to SET Building

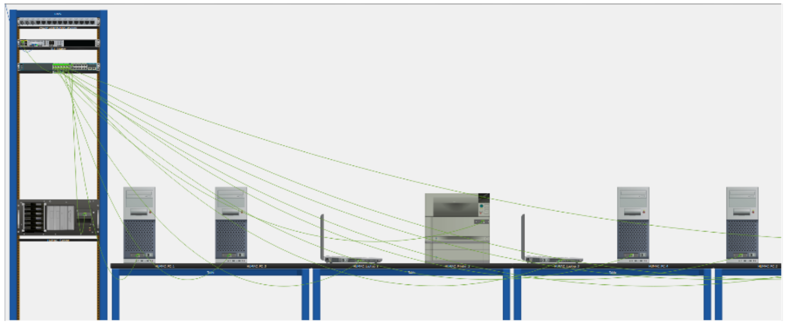
Communications Lab, SET Building



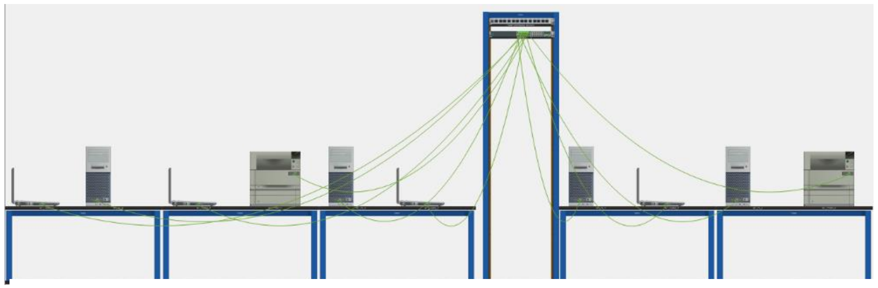
Labs in SET Building



Advanced Wireless Lab, SET Building

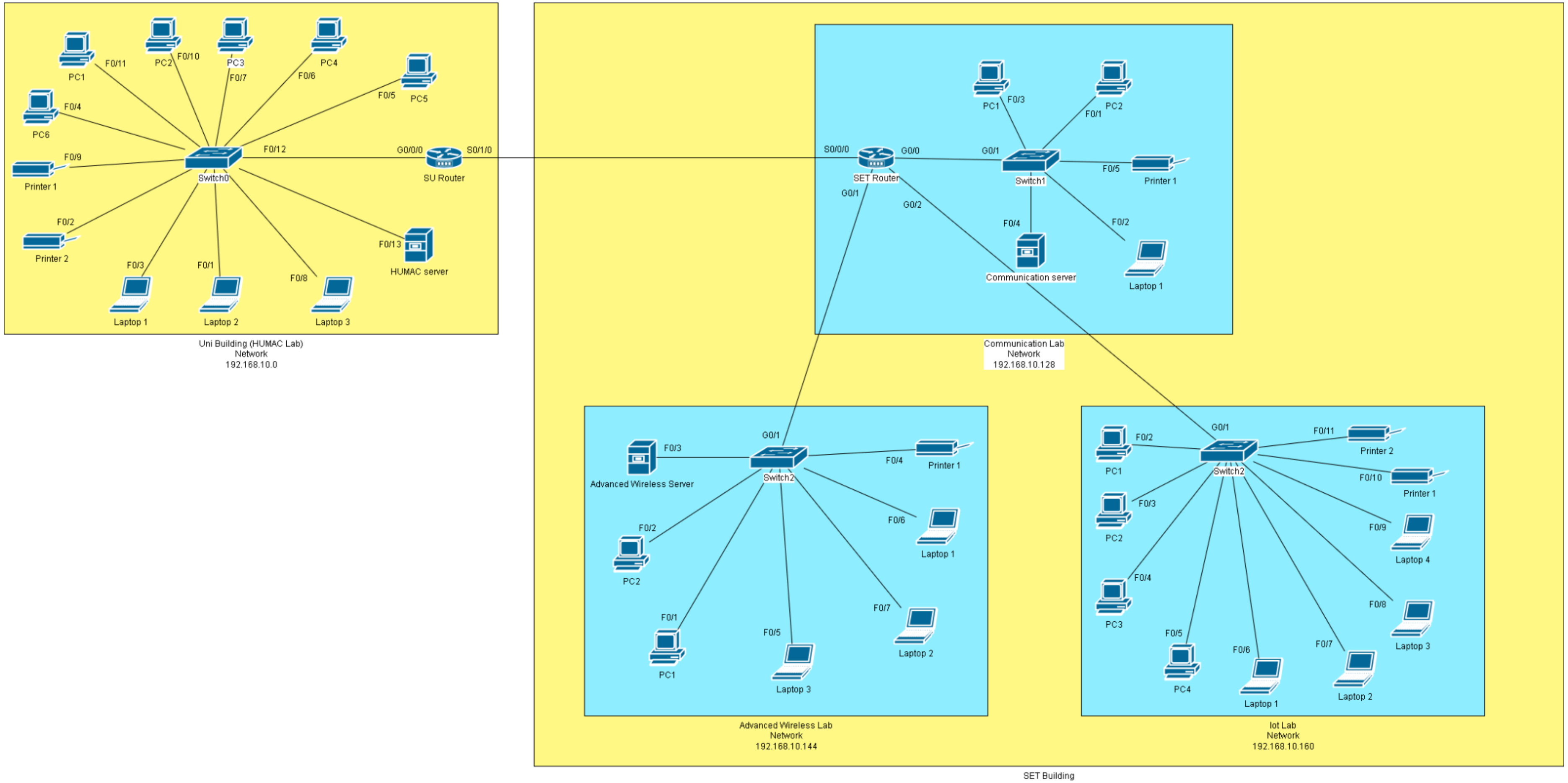


HUMAC Lab, Level 3, Sunway University Building



IoT Lab, SET Building

Logical Topology



Part B: Implementation

Addressing Table

Lab	Device	Interface	IPv4 Address	Prefix	Subnet Mask	Default Gateway
	SU router	G0/0/0	192.168.10.1	28	255.255.255.240	
		S0/1/0	192.168.10.201	30	255.255.255.252	
	SET router	G0/0/0	192.168.10.129	28	255.255.255.240	
		G0/0/1	192.168.10.145	28	255.255.255.240	
		G0/0/2	192.168.10.161	28	255.255.255.240	
		S0/0/0	192.168.10.202	30	255.255.255.252	
	Switch0	VLAN1	192.168.10.14	27	255.255.255.224	192.168.10.1
	Switch1	VLAN1	192.168.10.135	28	255.255.255.240	192.168.10.129
	Switch2	VLAN1	192.168.10.153	28	255.255.255.240	192.168.10.145
	Switch3	VLAN1	192.168.10.172	28	255.255.255.240	192.168.10.161
HUMAC	PC1	NIC	192.168.10.3	27	255.255.255.224	192.168.10.1
	PC2	NIC	192.168.10.4			
	PC3	NIC	192.168.10.5			
	PC4	NIC	192.168.10.6			
	PC5	NIC	192.168.10.7			
	PC6	NIC	192.168.10.8			
	Laptop1	NIC	192.168.10.9			
	Laptop2	NIC	192.168.10.12			
	Laptop3	NIC	192.168.10.10			
	Printer1	NIC	192.168.10.11			
	Printer2	NIC	192.168.10.13			
	Server	NIC	192.168.10.2			
Communication	PC1	NIC	192.168.10.130	28	255.255.255.240	192.168.10.129
	PC2	NIC	192.168.10.131			
	Laptop	NIC	192.168.10.132			
	Printer	NIC	192.168.10.134			
	Server	NIC	192.168.10.133			
Advanced Wireless	PC1	NIC	192.168.10.146	28	255.255.255.240	192.168.10.145
	PC2	NIC	192.168.10.147			
	Laptop1	NIC	192.168.10.148			
	Laptop2	NIC	192.168.10.149			
	Laptop3	NIC	192.168.10.150			
	Printer	NIC	192.168.10.151			
	Server	NIC	192.168.10.152			
IoT	PC1	NIC	192.168.10.162	28	255.255.255.240	192.168.10.161
	PC2	NIC	192.168.10.163			
	PC3	NIC	192.168.10.164			
	PC4	NIC	192.168.10.165			
	Laptop1	NIC	192.168.10.166			
	Laptop2	NIC	192.168.10.167			

	Laptop8	NIC	192.168.10.168			
	Laptop9	NIC	192.168.10.169			
	Printer1	NIC	192.168.10.170			
	Printer2	NIC	192.168.10.171			

Part C: Lessons Learned

In this project, our team collaborated to complete network design and deployment, focusing on network topology planning, router configuration, subnet division, and connection issues to ensure reasonable planning and efficient execution. To improve efficiency, we assigned tasks based on team members’ expertise, such as assigning network design responsibilities to those familiar with topology layouts. However, we still faced communication challenges. Since different members were responsible for different parts, poor communication could easily lead to issues such as IP conflicts and routing errors. To mitigate these problems, we scheduled regular meetings to clarify task deadlines, ensure smooth progress, discuss challenges, and adjust plans as needed.

During the implementation process, we encountered several technical challenges. First, in designing the physical topology, we aimed to meet the actual cabling requirements while considering accessibility and space constraints. To achieve this, we optimized the equipment layout and strategically placed routers, switches, and access points to ensure better coverage and accessibility. Simultaneously, to ensure network stability, we correctly selected the cable type based on the knowledge we learned in class. For instance, we used straight-through cables to ensure stable network connections between PCs and switches.

Secondly, in router configuration, some routers were unable to accurately forward data packets due to incorrect routing table entries, resulting in abnormal network connections. To solve this issue, we used Packet Tracer's simulation mode for troubleshooting and manually checked and adjusted the static routing configuration to ensure proper data transmission.

Third, we encountered problems with different protocol layers between router ports, which affected device communication. In response, we adjusted the encapsulation settings and ensured that IP addresses were correctly assigned to each port so that data could be transmitted stably.

Fourth, when dividing the network into four subnets, we initially made an error in the subnet mask configuration, resulting in an abnormal device connection. To correct this, we recalculated the subnet mask and optimized the allocation of IP addresses to align with the (192.168.10.0/24) network address.

Finally, since the HUMAC lab in the University building and the three labs in the SET building were located in different subnets, devices across subnets could not communicate, affecting overall network connectivity. To resolve this, we ensured smooth data transmission between subnets by implementing VLAN routing and correctly configuring the default gateway.

In summary, this project provided us with valuable hands-on experience in network design using Packet Tracer and effectively enhanced our practical skills in router configuration, subnet division, and troubleshooting network issues. The challenges we encountered deepened our understanding of network principles. Despite the difficulties, we successfully designed a fully functional and scalable network, significantly boosting our confidence in future network-related projects.

References

Bouchard, G. (2024, April 12). *OSI 7 layers explained the easy way*. https://insights.profitap.com/osi-7-layers-explained-the-easy-way

Darkrelay. (2024, January 30). What is OSI Model | 7 Layers Explained. *DarkRelay*. https://www.darkrelay.com/post/osi-model

Johnston, D. (2024, November 28). *What is OSI Model | 7 Layers Explained | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/osi-model/