FACULTY OF COMPUTING

SECR1213 - NETWORK COMMUNICATIONS

NETWORK DESIGN FOR FACULTY OF COMPUTING BLOCK N28B

LECTURER:

DR. RAJA ZAHILAH BINTI RAJA MOHD RADZI

GROUP 3: THE PHOENIX

GROUP MEMBER:

NAME	MATRIC NO.
HARCHANA A/P ARULAPPAN	A21EC0028
LEE RONG XIAN	A21EC0043
LU QI YAN	A21EC0049
YUSRA NADATUL ALYEEA BINTI YUSRAMIZAL	A21EC0151

ABSTRACT

In this project, we planned to design our own floor plan of a double-storey building with actual size. The ground floor will consist of an IOT lab, a Network lab and 2 General Purpose labs, toilets, a lift and a staircase. On the first floor, there was a video conferencing room, student lounge, lift, staircase and toilet. Our building was designed in a rectangular shape. We also did a preliminary analysis of current and future requirements and devices to be used. This portion was done through research and meetings. After that, we determined the feasibility of the project. Not only that, we also chose the appropriate LAN devices by referring to the information that we research on the internet. Then, we identified the work area on our floor plan and determined the number of connections, patch cords and switch ports that were needed. We also identified the cable types and lengths. We decided to use a CAT6 cable to connect the router, switch, PC and access point. In the end, we are also required to develop an addressing scheme that every host can connect to the network without a conflict of addresses. We also did the subnetting and IP assignment for each lab and room. Last but not least, we would like to express our gratitude to Dr. Raja Zahilah binti Raja Mohd Radzi who guided us through the project. Not forgetting, we would like to thank our team members who gave cooperation throughout the project.

TABLE OF CONTENTS

TABLE OF FIGURES

1.0 INTRODUCTION

This Network Communication project is a group project with individual review. The objective is to bring out what we have learned in class how things are in the real world. We were assigned to build a small network with all appropriate components such as understanding user/customer needs and planning them according to given budget, planning and designing network infrastructure for current and future needs, research and application of network device availability, usability, cost and service, calculating and using addressing Network IP and finally report our work to the client.

There are six tasks that require us to complete them within a predetermined time period. In Task 1, we were required to make our own layout and design of the additional building based on the requirements where it required us to draw a floor plan of a two-story building that has four labs, a video conference room and a student lounge according to the given size. Next, in Task 2 we need to do a preliminary analysis of the current and future needs and devices that will be used. We need to generate at least 10 questions and get answers from interviewing users. From the answer, we need to determine whether the project is feasible or not. In Task 3, we have to choose the appropriate LAN device by doing some research and discussing which device we want to use in our network construction. This also requires us to choose our devices accordingly considering all the factors and aspects of the hardware we want to use for each lab and room.

Task 4 requires us to make the connections between devices in our network by connecting servers, routers, PC and other devices by considering four physical areas when planning which are work area, telecommunications room (distribution facility), backbone or vertical cabling, and distribution or horizontal cabling. We need to determine the appropriate location to place the device and ensure a successful connection. In Task 5, we need to set up an IP addressing scheme by dividing subnets from the network addresses assigned to our group. This task requires us to divide the IP addresses for all the different labs and rooms in our building plan. The last task is Task 6 where we have to report on the work we have done in Tasks 1 to 5 and think about how it can be made better.

2.0 PROJECT BACKGROUND AND AN OVERVIEW OF THE CLIENT'S CURRENT STATUS AND ISSUE

The Faculty of Computing (FC) currently has 1200 students (both undergraduate and postgraduates), 97 academics and 35 support staff. To facilitate the 10% growth in both students and academic staff in the next 3 years, FC plans to build a new building 2 floors. The new building will house 4 new laboratories, 1 video conference room for virtual project meetings. It will also house a student lounge that will provide students an area to work and relax while connected to the network via WIFI. A total of 30 workstations for each laboratory and this laboratory is divided into 2 general purpose laboratories, 1 network laboratory and 1 IOT laboratory. Each laboratory and student lounge will be 14mx10m in size. The laboratory must be equipped with a high-speed internet connection in preparation for education in line with 4IR (4th Industrial Revolution). The Network Lab is equipped with network devices for teaching whereas the IOT lab is equipped with devices and hardware that can facilitate learning. FC Dean wanted the building to be 'ready for anything' and a reliable, efficient, cost effective and safe network that can be easily managed.

Another essential for the designed network system is it should be cost efficient while providing the highest performance, the equipment purchased, and the technology used must be wisely chosen to achieve the highest possible benefit with lowest cost. During the transition to the School of Computing toward the future, it is also important that the access is still provided to their user during this transition from old equipment to new equipment so the tasks on going by the user will not be interrupted. The new building is expected to have cutting-edge technology that is capable to withstand the growth of technology for the future 20 years. The designing process should also take consideration of future issues which is wireless connectivity that cover the whole building and scalable network for future growth as in future, wireless connection might play a big role in network connection. In sum, the essential element that need to be taken consideration in the designed system is easy to be managed and scaled, high performance and high security measures

3.0 COMPILED SOLUTION

3.1 TASK 1: PROJECT SETUP
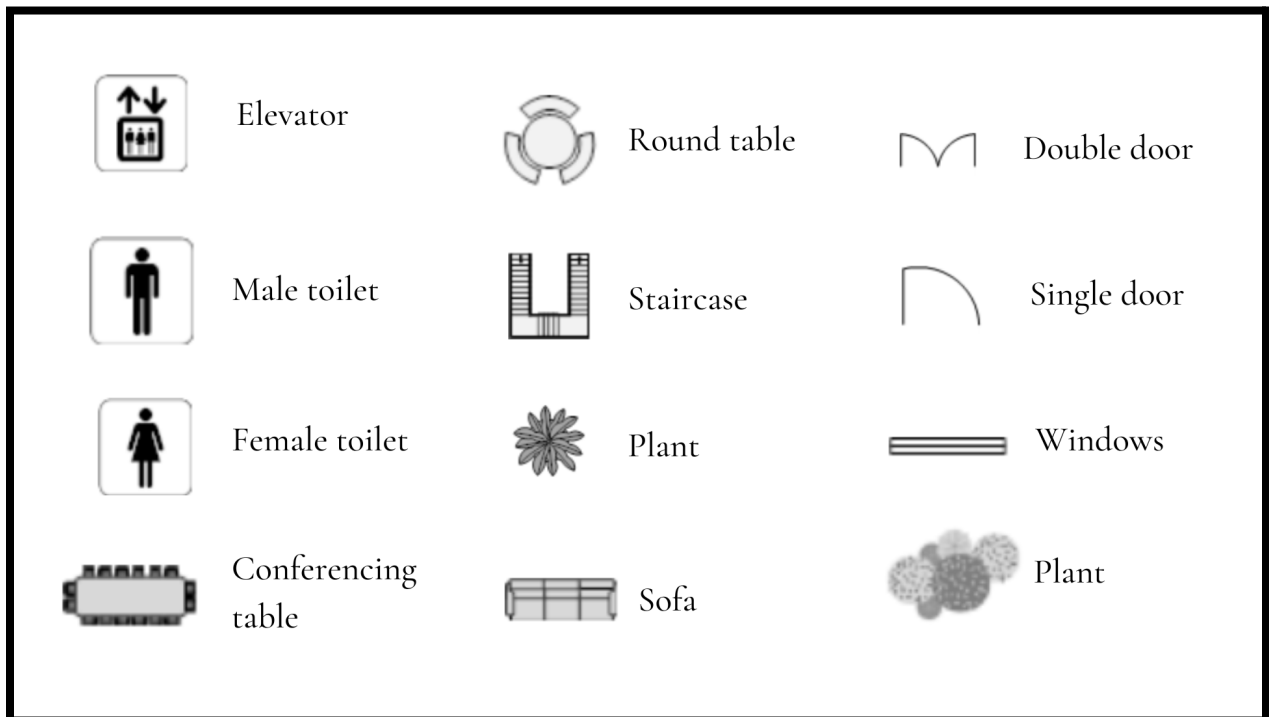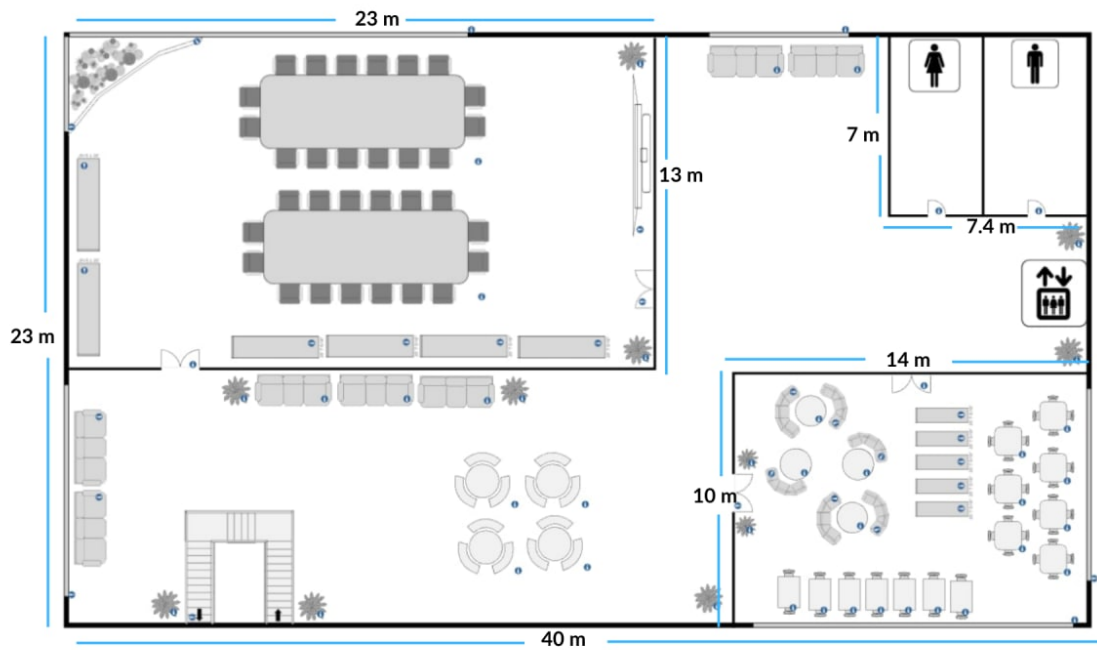
Ground Floor
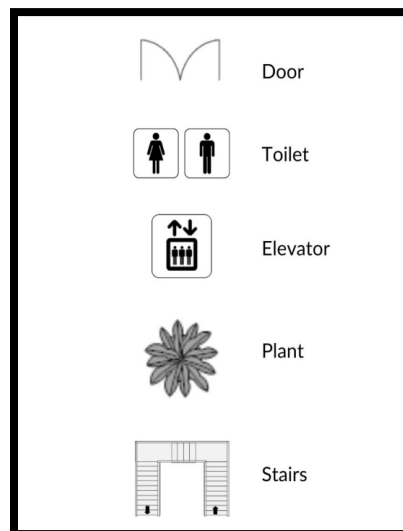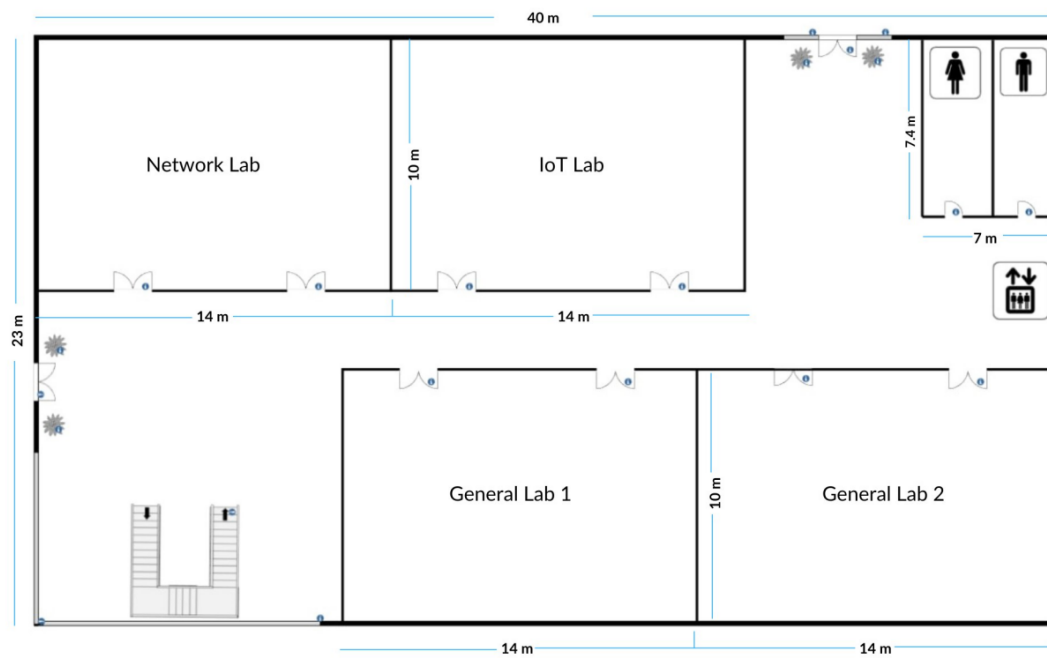
Figure 1: Floor Plan for Ground Floor

First Floor
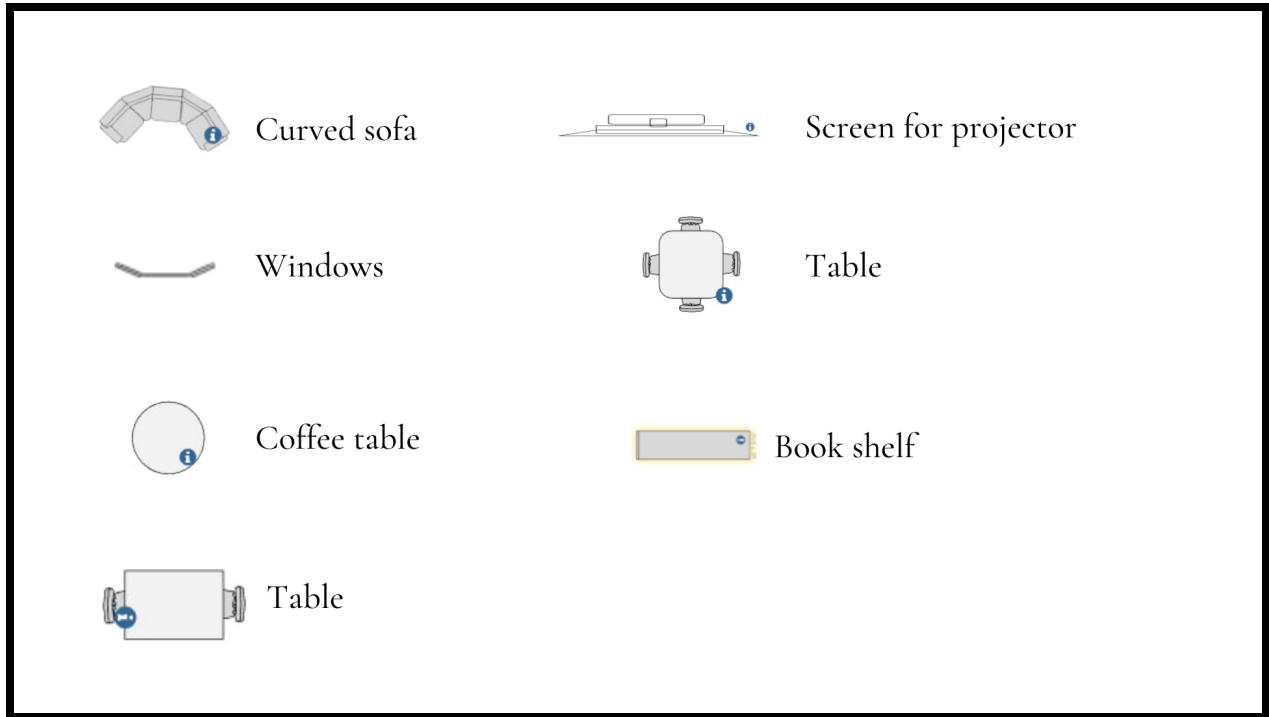
Figure 2: Floor Plan for First Floor

Lab

(2 General purpose labs, 1 Network lab and 1 IOT lab)

14 m

10 m

10m x 14m

	desk		window
	book shelf		screen
	chair		white board
	computer setup		double door
	plant		
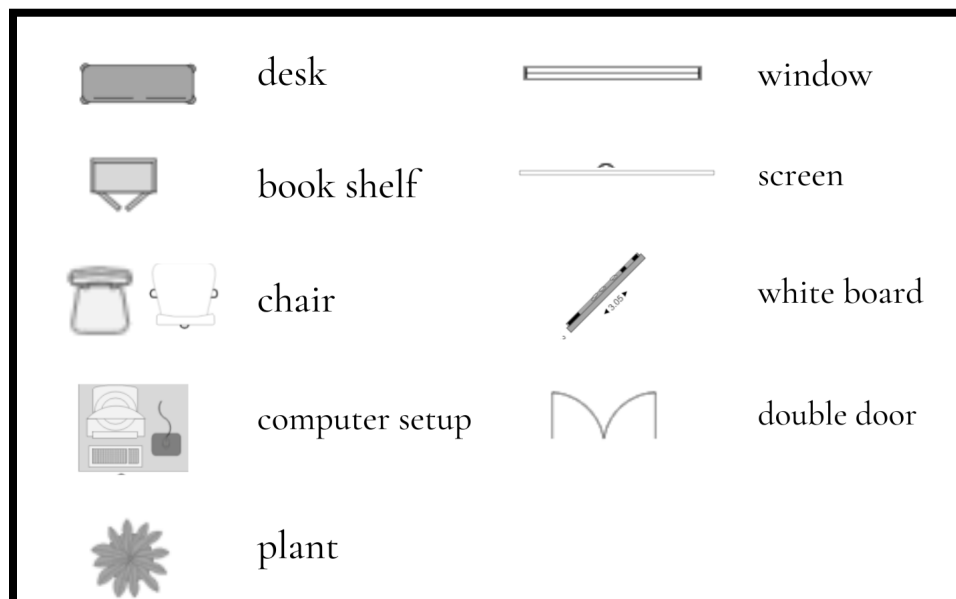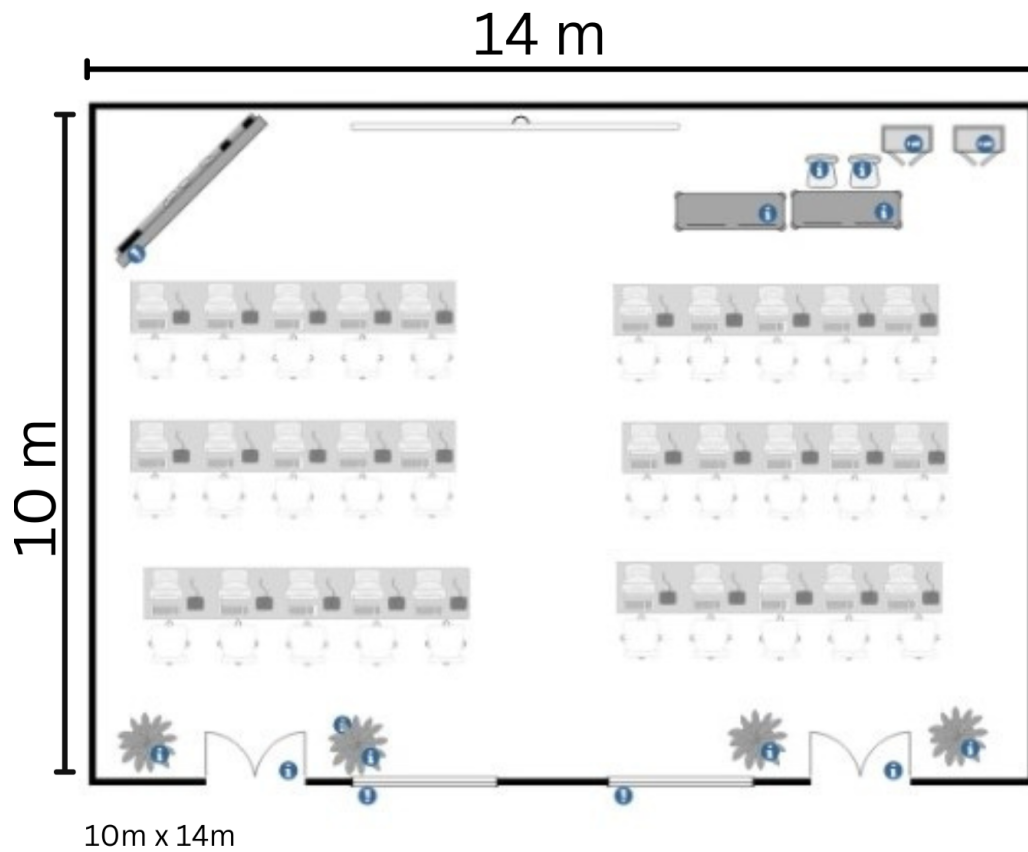
Figure 3: Floor Plan for Each Labs

Reflection for Task 1

       This task requires us to make the layout and design of our own additional building based on the requirements which are four laboratories, a video conference room and a student lounge where each laboratory and student lounge will be 14m x 10m in size. We found it difficult at first to divide the labs and rooms for each floor because we had never designed a floor plan. But with the help and cooperation of each member, we managed to complete this task within the given time and we were able to learn and experience designing our own building using the new software.

3.2 TASK 2: INITIAL DESIGN - PRELIMINARY ANALYSIS

Questions

Question 1: What is a router, modem, access point and switch?

A modem connects to the Internet. A modem is the gateway to the Internet. The modem translates the digital 1s and 0s from the computer into analog information for the cable or telephone wire to carry out to the world and translates incoming analog signals in the same way.

A router connects devices to the modem. Standalone modems aren't able to send data to multiple devices simultaneously. They usually only have one Ethernet port, and only produce one IP address, which identifies location to the Internet. A router connects to all home's devices and links them to each other through Ethernet cables or Wi-Fi and then connects to the modem. A router also gives each device its own internal IP address, which it uses to route traffic between them. The modem receives information from the Internet, sends it to the router and the router sends it to the computer that asked for it. The network created by the router is known as a local area network, or LAN and it connects to a larger wide area network, known as WAN.

An access point adds wireless connectivity. A wireless access point connects to the router, usually over Ethernet and communicates with Ethernet-less devices over wireless frequencies. Wireless access points are better for businesses because of its broad transmission range, high user access and stronger signal sending and receiving capabilities. Wireless APs also have a better safety performance, which is essential for any business.

A switch connects extra computers to the router. A switch is used in a wired network to connect to other devices using Ethernet cables. The switch allows each connected device to talk to the others. Wireless-only networks do not use switches because devices such as wireless routers and adapters communicate directly with one another. Switches allow you to connect dozens of devices and keep traffic between two devices from getting in the way of other devices on the same. Moreover, switches allow communication within a network that's even faster than the Internet.

Question 2: How to create a Local Area Network (LAN) that can connect to the Internet?

Instructions to Set Up LAN Network

Create Network

1. Identify the local services that are available on the network. Identify network-attached printers, network disk drives, any server that will share printers or disks.

2. Identify how many devices will have to connect to the network. Each device, server or workstation will require a unique address.

3. Run cables to workstations where possible. A wired LAN will always get better performance and be more secure than a wireless LAN. Wherever possible, run a cable to servers, printers, IP phones or work locations. Run a cable to any area where you are likely to work. Use standard Ethernet cables or building wiring as installed according to the TIA-568 standard.

4. Select and purchase a switch or cable router. The simple secure way to connect to the Internet is to use a cable router. Many makes and models are available. If the model we choose does not have enough ports to connect all of the computers, then we will need to purchase a switch as well.

5. Configure the WAN port of the cable router. Configuration details will vary from vendor to vendor. We need to configure the WAN port to be supplied by the Internet service provider.

6. Configure the LAN ports of the cable router. Most cable routers will act as a Dynamic Host Configuration Server, or DHCP server. This means that the router will give addresses to workstations automatically. Be certain that the address pool has enough

addresses for all of the workstations. Make certain that there are enough addresses outside of the range for any hosts that need static addresses.

7. Connect the wires for the network. Workstations and servers can be connected with standard Ethernet cables. Connect the switch to the cable router LAN ports by using the up-link or straight port on the switch. If the switch does not have an uplink port, connect any standard port of the switch to a LAN port on the cable router with an Ethernet crossover cable. Ethernet crossover cables can be purchased at any electronics store.

8. Test the services and Internet connectivity. Test each of the workstations to ensure they can connect to the Internet and test any local servers and printers. Print test pages on the shared printers. Tests read and write permissions on shared file servers by copying files to the servers and copying files from the server to a workstation.

Question 3: How to ensure that every user can access the wireless Internet connection?

    A. Installation
  a. Acquire a wireless router.
  b. Connect the router to your modem.
  c. Connect a computer via Ethernet cable.

    B. Configuration
  a. Install the router software.
  b. Open the router's configuration page.
  c. Enter your Internet connection information.
  d. Set your wireless settings.
  e. Apply your settings.
  f. Place your router.

    C. Connection
  a. Connect a device to the network.
  b. Enter the password.
  c. Test your connection.

Question 4: Which equipment requires protection and what kind of security measure should we implement in a building?

The equipment or devices that require protection include routers, switches, load-balancers, intrusion detection systems, domain name systems, and storage area networks. It is because most organizational and client traffic will pass through these devices.

A router is a device that connects two or more packet-switching networks or subnets. It performs two main functions which is managing traffic between these networks by forwarding data packets to their intended IP addresses and allowing multiple devices to use the same Internet connection. Most routers allow us to create a secure network by providing a secure network that helps us lock down the network and give it a passphrase. Using this method, only people with the passphrase can connect to our network. Then, most routers come with a firewall and it will block any information requests from the Internet directed to our computer. Next, since malicious code can be added to our computer from the websites we open, most routers have an option to define an Internet access policy that can block access to certain websites and this can also be used as a feature to block access to certain services and ports that our devices know to be infected.

Network switches connect devices such as computers, printers, wireless access points in the network to each other and allow them to communicate by exchanging data packets. Network switches are specifically designed to increase operator efficiency by eliminating the need for multiple keyboard and mouse systems, effectively eliminating the possibility of sharing data between multiple systems and networks. The simplest form of switch security is to use port-level security. When using port-level security, the MAC address and/or number of MAC addresses of connected devices are controlled.

The Domain Name System (DNS) is the Internet's phone book because humans access information online through domain names. Web browsers interact via Internet Protocol (IP) addresses and DNS translates domain names to IP addresses so that browsers can load Internet resources. The DNS system is not designed with security in mind like most Internet protocols and it may contain some design limitations. These limitations when combined with advances in

technology make DNS servers vulnerable to a wide spectrum of attacks, including spoofing, amplification, DoS (Denial of Service), or interception of private personal information. Then, since DNS is part of most Internet requests, it can be a prime target for attacks. We may use tools or software such as DNSSEC used to protect against attacks by digitally signing data to help ensure its validity. A DNS firewall can also be used because it provides some security and performance services for DNS servers.

Other tools to implement the security measures are load-balancers, Intrusion Detection System (IDS) and Storage Area Network (SAN) security. Load-balancers refers to the efficient distribution of inbound network traffic across a group of back-end servers and also known as a server farm or server pool. A load balancer is located in front of our servers and routes client requests across all servers, capable of serving them in a way that maximizes speed and capacity utilization. If one server goes down, the load balancer redirects traffic to the remaining online server and when a new server is added to the server pool, the load balancer automatically starts sending requests to it.

An intrusion detection system (IDS) is a device or software application that monitors a network for malicious activity or policy violations. Any malicious activity or breach is usually reported or collected centrally using security information and event management systems. An IDS will perform traffic analysis for pass and match traffic sent on subnets to known attack libraries when placed at a strategic point or points in the network to monitor traffic to and from all devices on the network. Once an attack is identified, or abnormal behavior is detected, an alert can be sent to the administrator.

A Storage Area Network (SAN) is a high-speed dedicated network that provides network access to storage devices. A SAN typically consists of hosts, switches, storage elements and storage devices connected using various technologies, topologies and protocols. It presents the storage device to the host so that the storage appears to be locally attached.

Question 5: How to ensure network security?

Network Security as preventive measures taken to protect the network infrastructure from unauthorized access, modification, malfunction, misuse, improper disclosure or destruction of data. It can be ensured by creating a virtual private network (VPN), using a multilayer security system and installing and encrypting the files.

Firstly, network security can be ensured by creating a virtual private network (VPN). A VPN creates a more secure connection between a remote computer and a computer server. With a VPN, only those authorized to access a system will be able to do so. A VPN can reduce the chances of hackers finding a wireless access point and break into our system.

Next, network security can be ensured by using a multilayer security system. Multi-layered security refers to a security system that uses multiple components to protect operations at multiple levels or layers. It is the act of securing a network with a combination of various security tools such as the simultaneous use of antivirus programs, firewalls, and intrusion detection systems.

Lastly, the network security can be ensured by encrypting the files. Encryption can protect sensitive data on a computer's operating system using software specifically designed to mask the IP address. By looking for "https" in the address bar along with a padlock icon, we can identify whether a website has been protected using encryption.

Question 6: What cable type is suitable to be implanted in this building?

Fiber optic networks have made great strides in the business world, as these networks allow faster data transmission than previous networks. However, schools have also realized the great benefits that can be gained from establishing fiber optic networks in their buildings, fiber optic cable networks not only provide better security and communication within the school but also provide new learning methods for students. Making information easier to access easier, allows lecturers to incorporate teaching videos and prevent outside access to the faculty network are some of the benefits that can be gained from using fiber optic.

Firstly, fiber optic makes information easier to access. This is because fiber optic cables use light to receive and transmit data, which makes them faster than traditional copper cables. If the faculty has fiber optic technology, the Internet can handle the use of hundreds of students at once since students today use smartphones, tablets, laptops and desktop computers to access information on the Internet and run programs for school projects that require fast-moving Internet.

Secondly, fiber optic allows lecturers to incorporate teaching videos. As the faster Internet becomes accessible, lecturers will also benefit from the speed of fiber optic networks. Lecturers will be able to incorporate instructional videos as part of their lesson plans, which can help illustrate concepts and make lessons more dynamic and engaging for students.

Lastly, fiber optic can prevent outside access to the faculty network. A faculty with a fiber optic network gives the faculty's internal network more protection than traditional copper cables. Hackers or potential network intruders will have a harder time obtaining sensitive information because fiber optic cables are difficult to access.

Question 7: How to set up IP addresses for an Office?

We may need multiple IP addresses as it will prevent traffic from being exchanged via the gateway, speeding things up and reducing the load. Moreover, one IP address is not sufficient as it may confuse the destination of the packet from the internet.

Although setting up Dynamic Host Configuration Protocol (DHCP) is simple, we may encounter some issues such as the difficulty of remote administration which is not ideal for an academic LAN. Thus, a static IP address is going to be set up although it is time-consuming. Below are the steps on how to set up a static IP address for each device in the LAN. (Finn McChuhil, 2018):

1. A range of valid IP addresses to be used on the network is selected.
2. A unique IP address is assigned to each computer and network ready device on the LAN. For instance, on a network with no more than 250 attached devices, a common scheme is to assign IP addresses with a range of 192.168.1.1 through 192.168.1.254 and a subnet mask of 255.255.255.0.
3. The IP address 'xxx.xxx.xxx.0' is a reserved address for a network ID and IP address 'xxx.xxx.xxx.255' is reserved for a call-back address. Neither of them should be used to assign for network-ready devices in the LAN.

Question 8: How to support high-performance on core backbone?

After considering the requirements, we decided to use fiber optics support high-performance on core backbone. The core communication cabling throughout the developed world has largely been replaced by the fiber optics cabling as it has become a preferred choice for building backbone networks. The advantages of fiber optic cabling include more secure, easier to install due to the small diameter and light weight of cabling, allows signals to be transmitted over longer distances, expands bandwidth and improves the scalability of IT networks, very low bit error rate due to considerable resistance to electromagnetic interference, and faster Internet speeds. (Anthony Novello, 2020)

Question 9: Should servers be gathered and put in one room rather than distributed in each lab?

After doing some research and having some discussions among group members, we decided to gather the servers in one room rather than distribute them in each lab. Having a server room that gathers all the servers benefits us from the aspect of management and security. Firstly, as all the servers are in the same room where we manage our network server resources, we can easily control and manage the network connectivity, power, room temperature and ventilation at the same time. We can reduce trouble by just going through one room but not many rooms which will cost a lot of time and money. If any technical problems occur, technicians can solve the problems easier and faster. At the same time, the management environment of the server room can be done more efficiently because room temperature control and ventilation can be done easily. Thus, it can be said that maintenance is easier if all the servers are gathered in one room compared to distributed servers in each lab.

Besides that, with the server implemented together, the implementation of security on both physical and software is easier to apply on the servers. We can protect the servers physically by having closed-circuit television(CCTV) and maybe have some workers guarding the room during working hours. For network security, the technician can react and solve the danger and threat immediately when it is realized by heading to the room and solving the problems.

Thus, we have decided to gather all the servers by having a server room to avoid the difficulty in maintaining the servers and security.

Question 10: What is the total bandwidth required in the building?

      The Federal Communications Commission (FCC) defines high-speed Internet as 25 Mbps, thus each workstation in Lab should have at least 25Mbps. However, considering that each person may have their own devices, we decided that each computer should meet an average bandwidth of 35Mbps. Each lab has 30 workstations in total, thus the total bandwidth for each lab is 1050Mbps. Since we have four labs, the total bandwidth for labs is 4200Mbps. The student lounge and the lobby on the first floor that can accommodate around 100 people should have 3500Mbps. As the video conferencing room should have a better Internet experience, the suggested bandwidth of Wi-Fi is around 500Mbps. Overall, the total bandwidth for the whole building is recommended to be around 10Gbps.

Project Feasibility

After identifying the requirements of the project, our project's feasibility has been determined. Our group has enough information to continue our project.

The budget given is RM3,000,000. It is enough and possible to move on with our floor plan. This is because we have tried to reduce our costs by designing a building that will reduce troubles. For example, we create a server room that can easily maintain and manage. Thus we will need lesser technicians and staff to manage the server room. We also design the first floor with floor-to-ceiling windows that can make the building brighter so that we can save more electricity. Through these we can save more budget and spend more on the network system.

Based on the floor plan that we had done, we met the requirements in the case study. At the same time, we have considered all the security measures that are needed. For instance, we have included closed-circuit television (CCTV) which can record all the activities happening in the building to avoid crimes. This CCTV can also help us to investigate certain things that happen in the building as it can provide video footage as evidence. Since we also have a server room that can make it easier to manage all the servers and network connection resources, we can save more time and money from the maintenance aspect. Network security is also important from our perspective as the students, lecturers, and staff will be using the internet to access their private information such as name, IC numbers, and other information.

We also considered the process of studying and teaching in the building. We calculate how many devices will be used by the students and lecturers so that we can consider the bandwidth for each lab and other rooms in this building. This is to make sure all of them can have the best experience of studying and using the internet in this building. Thus, all the processes of learning and teaching are able to be conducted smoothly without any internet problems.

The equipment that will be used in the building such as routers, modems and assessment points have been identified. Which cable type is suitable for our building has also been identified. All the equipment and floor plan that we plan are able to achieve and we already

considered all the things that are quite important for us such as IP address. Thus, it can be said that the floor plan is feasible.

Reflection for Task 2

For this task, we are required to generate at least 10 questions to ask users or to research because they will be useful for us when we want to develop a network plan in the next task. Therefore, we divide the questions for each member where two people make two questions and the other two come up with 3 questions. From the generated questions, we search for answers from various sources on the Internet to get the best answer for the question. From our findings, we have concluded that our group has enough information to proceed with our project because we have identified the necessary devices in our project and we have also looked at all aspects such as cost, bandwidth and network security to ensure that it is possible to implement and meet user needs.

3.3 TASK 3: CHOOSING THE APPROPRIATE LAN DEVICES

Router

One or more packet-switched networks or subnetworks can be connected using a router. By sending data packets to their intended IP addresses, it manages traffic between different networks and permits several devices to share an Internet connection.

Product	Synology RT2600ac	ASUS AX6000 (RT-AX88U)	Cisco RV345 Dual WAN Gigabit VPN Router
Specification	- With CPU Dual core 1.7 GHz 4x4 MIMO Omni-directional high-gain dipole (2.4GHz / 5GHz) 7 gigabit LAN port and 3 gigabit WAN (DUAL WAN support) 1 USB 3.0 port, 1 USB 2.0 port and 1 SD card reader (SDXC, SDHC) - IEEE 802.11a/b/g/n/ac; Simultaneous dual-band Wi-Fi; Beamforming; 2.4GHz:	4x4 dual-band that provides 160MHz bandwidth 1 RJ45 for 2.5 Gigabits BaseT for WAN/LAN, 1 RJ45 for 2.5 Gigabits BaseT for LAN, 4 RJ45 for Gigabits BaseT for LAN, 1 USB 3.2 Gen 1 and 1 USB 2.0 - Has AiProtection Pro, powered by Trend Micro with automatic	2 WAN ports (RJ-45) for load balancing and resiliency 16 LAN ports for high-performance connectivity 2 USB ports to support a 3G/4G modem or flash drive 900 Mbps TCP throughput for improved productivity - VPN functionality for secure interconnectivity, including

	800Mbps; 5GHz: 1.73Gbps ● VPN server/client (Synology SSL VPN, PPTP, OpenVPN, L2TP/IPSec); VPN pass-through (PPTP、IPSec、L2TP) ● Support layer 7 Qos		standard IPSec, Layer 2 Tunneling Protocol (L2TP) over IPSec, and Cisco IPsec ● Support for the Cisco AnyConnect Secure Mobility Client, ideal for remote access by mobile devices
Price	RM2,815.00	RM1,619.00	RM1,400.00
Reference	1. https://www.synology.com/en-global/products/RT2600ac#availability 2. https://shopee.com.my/%E3%80%90Hot-Style%E3%80%91-SYNOLOGY-Rt2600Ac-Wireless-Router-Rt-2600-Ac-Sharing-Device-Wi-Fi-i.421915523.9056648749	1. https://www.amazon.com/dp/B07HM6KJN8?tag=thebalance-onsite-prod-20&linkCode=ogi&th=1 2. https://shopee.com.my/product/58359596/2026548334	1. https://shopee.com.my/Cisco-RV345-Dual-WAN-Gigabit-VPN-Security-Router-i.226783022.6717922179

Through the comparison between these three routers, we have decided to choose the **Synology RT2600ac** as this router has the best specification. Even though the Synology RT2600ac has lesser ports compared to Cisco RV345 Dual WAN Gigabit VPN Router, Synology RT2600ac supports layer 7 Qos which enables the routers to perform with better performance. At the same time, Synology RT2600ac also up to 800 Mbps and 1733 Mbps on the 2.4 GHz and 5 GHz radios, respectively. Synology RT2600ac also provides VPN which makes the security of the network more secure.

Switch

A network switch is defined as a hardware component which is responsible for relaying data from a computer network to the destination endpoint through packet switching, MAC address identification, and a multiport bridge system. A network switch connects and transmits data packets to and from devices on a local area network (LAN).

Product	S5850-48T4Q, 48-Port Ethernet L3 Switch, 48 x 10GBASE-T, with 4 x 40Gb QSFP+, Support MLAG	S5860-20SQ, 24-Port Ethernet L3 Switch, 20 x 10Gb SFP+, with 4 x 25Gb SFP28 and 2 x 40Gb QSFP+, Support Stacking, Broadcom Chip	S3910-24TS, 24-Port Gigabit Ethernet L2+ Switch, 24 x Gigabit RJ45, with 4 x 10Gb SFP+ Uplinks, Stackable Switch, Broadcom Chip
Specification	48x 100/1000M/5G/10G Multi-gig RJ45 with 4x 40G QSFP+(split to 4x 10G) - Support MLAG (Multi-Chassis Link Aggregation) for Uninterrupted Services 1+1 AC Hot-swappable Power Supplies and 2+2 Smart Fans - Support Data Center Features (PFC, ECN etc.) to Build a Lossless and Low-latency Network - Support CLI/WEB/SNMP/SSH/OVSDB/RPC-API for Flexible Operation - Network Monitoring through Sampled Flow (sFlow) - Support SSH, ACL,	- Broadcom BCM56170 Chip, All 10G/25G/40G Ports Support Stacking 1+1 Hot-swappable Power Supplies, Smart Fans - Support QoS, DHCP, BGP, VRRP, QinQ, etc. - Support WEB/CLI/SNMP/SSH for Flexible Operation - Network Monitoring through Sampled Flow (sFlow) - Support SSH, ACL, AAA, 802.1X, RADIUS, TACACS+, etc. for Security - IPv4/IPv6 Dual-Stack for Future Network Expansion	- Broadcom BCM56150 Chip, Support Up to 4 Units Stacking 1+1 Hot-swappable Power Supplies, Smart Fan - Support SSH, DHCP, RIP, OSPF, VRRP, etc. - Support WEB/CLI/SNMP/SSH for Flexible Operation - Network Monitoring through Sampled Flow (sFlow) - Support SSH, ACL, AAA, 802.1X, RADIUS, TACACS+, etc. for Security ≥8KV Lightning Protection

	AAA, 802.1X, RADIUS, TACACS+, for Security		
Highlights	● S5850-48T4Q features an advanced hardware design combined with 48x 100/1000M/5G/10G BASE-T ports and 4x 40Gb ports. ● This 10GBASE-T switch offers backwards compatibility with installed Ethernet cabling and standard RJ-45 connectors. ● The switch comes with the complete system software with comprehensive protocols and applications to facilitate the rapid service deployment and management for traditional Layer 2 and Layer 3 networks. ● Offering high-performance, high port density, and low latency, S5850-48T4Q is well-suited to both the core and aggregation layers, enabling it to meet data centers, careers	● 24-Port Ethernet L3 Switch, 20x 10Gb SFP+, with 4x 25Gb SFP28 and 2x 40Gb QSFP+, Support Stacking, Broadcom Chip ● The S5860-20SQ 24-port 10Gb Ethernet layer 3 switch features 20x 1G/10G downlinks, 4x 10G/25G SFP28 and 2x 40G QSFP+ (can be split into 4 x 10G SFP+) uplinks that all support virtual stacking. ● This managed enterprise switch adopts cutting-edge Broadcom chips to deliver 760 Gbps switching capacity and 565 Mpps forwarding rate. ● It is packed with redundant hot-swappable power supplies, dual hot-swappable smart fans and hardware-level dual-flash chip for superior processing performance and network reliability.	● The S3910-24TS gigabit Layer 2+ stackable managed switch features 24x 10/100/1000BASE-T and 4x 10Gb SFP+ uplinks that is best for complex environment deployment, which resists corrosion, dust and moisture, supports -10°C ~ 60°C operation and 8KV lightning protection. ● The 24-port gigabit managed switch equipped with 1+1 hot-swappable dual power supplies, supports 4 units physical stacking to deliver redundancy, simple management and resilience of network capacity. ● Further, with Broadcom BCM56150 switch chip, S3910-24TS can provide 128 Gbps switching capacity and 96 Mpps forwarding rate to deliver higher network performance.

	and enterprise network requirements. ● Multi-interface speeds switch with VXLAN, MLAG for Enterprises, Data Centers and ISPs	● FS agile S5860-20 SQ managed switch is ideal for large-scale campus network aggregations, small and medium-sized network cores to meet the needs of high-speed, safe, intelligent enterprise networks. ● Most cost-effective switch with 25G/40G uplinks for SMBs and Enterprise	● Besides supporting IPv4/IPv6 and rich layer 3 routing features (static routing, OSPF, RIP, RIPng and etc.), the gigabit switch enables flexible deployment for diverse networking demands. ● High-reliability switch with OSPF, VRRP, DHCP Server features for SMBs, Enterprise Edge
Price	RM21,901.00	● RM7,405.00	RM3,561.00
References	https://www.fs.com/sg/products/69378.html?country=my&currency=MYR&languages=English&paid=google_shopping&utm_country=9066744&gclid=CjwKCAiAhqCdBhB0EiwAH8M_GlBPkiah98qsjLSB71dbrbTugRqRMPo5stfRuYsVwhtzYYzOBjCJ0xoCKe0QAvD_BwE	● https://www.fs.com/sg/products/108710.html?country=my&currency=MYR&languages=English&paid=google_shopping&utm_country=9066744&gclid=CjwKCAiAhqCdBhB0EiwAH8M_GmH8UUn1N02a8S9FPe3jMJ5oU9Md-mRCsypWieOhVBZChmRQ4twtkRoCttwQAvD_BwE	https://www.fs.com/sg/products/108712.html?country=my&currency=MYR&languages=English&paid=google_shopping&utm_country=9066744&gclid=CjwKCAiAhqCdBhB0EiwAH8M_Gjkyov4KOkGif95G-VC1vpVAJje2C62O2RuNPAp1ejD28nMQtrqCEhoCWi8QAvD_BwE

Based on these comparisons, **S3910-24TS, 24-Port Gigabit Ethernet L2+ Switch** has been chosen as the first and right choice due to its specifications and features. First of all , the price for this switch is budget friendly and affordable which is RM 3,561.00 compared to S5850-48T4Q, 48-Port Ethernet L3 Switch and S5860-20SQ, 24-Port Ethernet L3 Switch. Secondly, it has L2 features which is Layer-2 switches perform the switching function to

rearrange the data frames from the source to a destination end by learning the MAC address of the destination node from the address table of the switch. This is because we do not need any L3 capacities for a computer lab. Thirdly, 10Gbps fiber link is enough to campus core router where **S3910-24TS, 24-Port Gigabit Ethernet L2** has 4x 10Gb SFP+ uplinks that is best for complex environment deployment, which resists corrosion, dust and moisture, supports -10°C ~ 60°C operation and 8KV lightning protection. In conclusion, **S3910-24TS, 24-Port Gigabit Ethernet L2+ Switch** is the best choice in terms of high-reliability switch and most cost-effective switch.

Patch Panel

A patch panel in a local area network (LAN) is a mounted hardware assembly that contains ports used to connect and manage incoming and outgoing LAN cables. Patch panels provide a way to keep large amounts of cables organized, enabling flexible connections into network hardware located in data centers or access or wiring closets. Each of these ports contains wires that go to a different location.

Product	IWILLINK Patch Panel 48 Ports, Cat6 / Rj45 Patch Panel, 2u Network Patch Panel Utp 19-Inch, Black	Cable Matters UL Listed Rackmount or Wall Mount 48 Port Network Patch Panel (Cat6 Patch Panel / RJ45 Patch Panel)	AMPCOM Supreme Series CAT6 48 Ports Patch Panel, Rack Mount - 2U, 19 inch, RJ45 Ethernet 568A 568B, 50u Gold Plated, with Rear Cable Management Bar
Specification	- Install this Ethernet patch panel effortlessly in universal 19" racks, cabinets, or wall mount brackets with 2U (3.5") standard height - Heavy duty network patch panel 48 port supports Ethernet, made for Cat 6 cabling, compatible with Cat 5e /Cat 5 - Gold plated contacts ensure a correction	- Heavy duty 48 port patch panel supports 10G Ethernet and is backwards compatible with Gigabit Ethernet. Made for Cat 6 cabling, but backwards compatible with Cat 5e and Cat 5 cabling - Future-proof your network connection for 10-Gigabit Ethernet with this durable	- Cat6 48 port 50u patch panel for 100/1000 Mbps networking, Cat6/Cat5e/Cat5 compatible, accept 22-26 AWG solid and stranded UTP cables - T568 A&B Wiring color coding, written-on label and numbered ports on the back and front for easy Installation

	free connection. Numbered ports and color-coded T568A and T568B wiring diagrams give quick reference. White space for easy marking and identification ● This patch panel enables quick, easy cable patching. Just plug Cat6 cables into its 48 front RJ45 ports, and use a 110 or Krone punch-down tool to terminate color-coded connections in the rear ● IWILLINK is committed to providing customers with the highest quality products and services. If you have any dissatisfaction or quality problem when you receive the item, you can always contact us and we will give you a full	RJ45 patch panel ● Install this Ethernet patch panel effortlessly in universal 19" racks, cabinets, or wall mount brackets with 2U (3.5") standard height ● Gold plated contacts ensure a correction free connection. Numbered ports and color-coded T568A and T568B wiring diagrams give quick reference ● Network patch panel complies with the UL fire safety requirement (E486099). Use included D-rings and cable ties for easy cable management	and identification T568 A&B Wiring color coding, written-on label and numbered ports on the back and front for easy Installation and identification ● 110 type punch down termination, and can be mounted in standard EIA 19" Racks ● Heavy duty black powder coat steel construction, 50u gold plated contacts for long term safe use ● Package: 1 x Patch Panel, 1 x rear cable tie-down support bar, 1 x Wire Stripper, 1 x Dust Proof Cover, Screws, Cable ties

	refund or replacement ● Network patch panel complies with the CE and RoHS. Use included D-rings and cable ties for easy cable management		
Price	RM 256.37	RM 309.43	RM 265.04
Reference	https://www.amazon.com/Iwillink-Network-19-Inch-Compatible-Cabling/dp/B09VTKXMJZ/ref=sr_1_1_sspa?keywords=48%2Bport%2Bpatch%2Bpanel&qid=1672114241&sr=8-1-spons&spLa=ZW5jcnlwdGVkUXVhbGmaWVyPUEzRlUzRzI2UUIzTDRKJmVuY3J5cHRlZElkPUEwNzI0NTkxMU04UDZPMVdGTFhLSSZlbmNyeXB0ZWRBZElkPUEwOTExMjM3UUxXRk1EU0xaQiZ3aWRnZXROYW1lPXNwX2F0ZiZhY3Rpb249Y2xpY2tSZWRpcmVjdCZkb05vdExvZ0NsaWNrPXRydWU&th=1	https://www.amazon.com/Cable-Matters-Rackmount-Wallmount-48-Port/dp/B0072K1P8C/ref=sr_1_7_sspa?keywords=48+port+patch+panel&qid=1672114241&sr=8-7-spons&psc=1&spLa=ZW5jcnlwdGVkUXVhbGmaWVyPUEzRlUzRzI2UUIzTDRKJmVuY3J5cHRlZElkPUEwNzI0NTkxMU04UDZPMVdGTFhLSSZlbmNyeXB0ZWRBZElkPUEwNjgzMTIwMjhUN0lTS0hJRTlDDNyZ3aWRnZXROYW1lPXNwX210ZiZhY3Rpb249Y2xpY2tSZWRpcmVjdCZkb05vdExvZ0NsaWNrPXRydWU=	https://www.amazon.com/AMPCOM-Supreme-Rackmount-Wallmount-Management/dp/B07FRDWHL2/ref=sr_1_21?keywords=48%2Bport%2Bpatch%2Bpanel&qid=1672114241&sr=8-21&th=1

Based on these comparisons, **IWILLINK Patch Panel 48 Ports, Cat6 / Rj45 Patch Panel, 2u Network Patch Panel Utp 19-Inch, Black** is the best option to be chosen. It is because the features and specification is almost the same as other patch panels but with the cheapest price.

Wireless Access Point

According to Cisco System (2022), a wireless access point (WAP) is a networking device that allows wireless-capable devices to connect to a wired network. It is simpler and easier to install WAPs to connect all the computers or devices in the network than to use wires and cables. Access Point is a central unit in an all-wireless network where it functions as a hub that links all stations together.

Product	D-Link DAP-2680 Wireless AC1750 Wave 2 Dual-Band PoE Access Point	TP-LINK EAP653 AX3000 Ceiling Mount WiFi 6 Access Point
Specification	• Supports IEEE 802.11a/b/g/n/ac Wave 2 wireless1 interface • 3 X internal dual-band antennas • Operates at 2.4 GHz and 5 GHz frequency • Maximum bandwidth: 450 Mbps for 2.4 GHz and 1300 Mbps for 5GHz • Supports WPA-personal, WPA Enterprise, WPA2-Personal, WPA2-Enterprise and WEP 64/128-bit encryption • MAC address access control • Network Access Protection (NAP) • Internal RADIUS server Network Management: • Telnet • Secure Telnet (SSH) • Web (HTTP) • Secure Socket Layer (SSL)	• Supports IEEE 802.11ax/ac/n/g/b/a wifi standards • 4 X 4 spatial streams • Maximum bandwidth: 574 Mbps for 2.4GHz and 2402 Mbps for 5 GHz • Supports WEP, WPA Personal/Enterprise, WPA2 • Personal/Enterprise, WPA3-Personal/Enterprise • Encryption protocols • Mac address filtering with a maximum number of 4000 • Centralized management with cloud access and Omada application • Provides a 2.5 Gbps Ethernet port (supports IEEE802.3at PoE) • Easy to be installed • Wall and ceiling mountable

	• Easy to be installed • Wall and ceiling mountable	
Price	RM 772.00	RM 629.00
Reference	https://shopee.com.my/D-Link-DAP-2680-Wireless-AC1750-Wave-2-Dual%E2%80%91Band-PoE-Access-Point-i.42575106.2044587055?sp_atk=42496e91-4dbc-44bb-9486-381fa932f070&xptdk=42496e91-4dbc-44bb-9486-381fa932f070	https://shopee.com.my/TP-LINK-EAP110-EAP115-EAP225-EAP245-EAP610-EAP650-EAP653-WIRELESS-DUAL-BAND-GIG-CEILING-MOUNT-ACCESS-POINT-i.29242218.1467937887?sp_atk=118dacc9-f112-4e45-836d-52dd7ec46cd8&xptdk=118dacc9-f112-4e45-836d-52dd7ec46cd8

According to the comparison, **TP-LINK EAP653 AX3000 Ceiling Mount Wi-Fi 6 Access Point** TP-Link access point is a better option because it has a high-efficiency Wi-Fi 6 so that more connected devices can enjoy faster speeds. Besides, video streams and voice calls are unaffected as users move between locations due to the seamless roaming. Besides, there is a powerful centralized cloud management where Omada SDN integration manages the whole network locally or from the cloud via web UI or Omada app. In terms of price, it is also cheaper with high performances.

Cable

LAN cable is referred to as twisted pair cables which are able to reduce signal noise and interference. There are several categories of LAN cable which are Cat5e, Cat6, Cat6A, Cat8 cable, etc. In this context, we apply Category 6 cable to optimize performance and accommodate the size of the 23 AWG conductors. Moreover, LAN cable comes in shielded and unshielded versions. Shielded LAN cables are for EMI (Electromagnetic Interference) areas whereas unshielded LAN cables are for homes and businesses when no EMI is present. Thus, we are going to choose the unshielded LAN cable.

Product	PROLINK Cat6 UTP Full Copper Cable	CK-LINK CAT6 UTP CABLE	Ubiquiti Cat6 UTP cable
Specification	• 4-pair unshielded twisted pair • Thicker conductor diameter • Provide higher reliability and higher data rates • Support transmission bandwidth 250 Mhz • Support 10 Gbps up to 55 meters • Uses 23 AWG solid copper conductor pairs • Colour: Blue • Length: 305m	• 4-pair unshielded twisted pair • Thicker conductor diameter • Support transmission bandwidth 250 Mhz • Support speed of up to 10G Ethernet • Support 10 Gbps in less than 50 meters • Uses 24 AWG solid copper conductor pairs • Colour: Blue • Length: 305m	• 4-pair unshielded twisted pair • Support the use in the plenum area • Support transmission bandwidth 600 Mhz • Support up to 10 Gbps (UC-C6-CMR) • Supports speed of up to 10G Ethernet • Uses 23 AWG solid copper conductor pairs • Colour: White • Length: 304m

Price	RM 299.00	RM 309.00	RM 939.00
Reference	[PROLiNK CAT6 / CAT5e UTP LAN Networ (end 9/20/2024 12:00 AM) (lelong.com.my)](#)	[CK-LINK CAT6 UTP NETWORK CABLE 305M (end 9/19/2023 12:00 AM) (lelong.com.my)](#)	[Ubiquiti UC-C6-CMR UC-C6-CMP CAT6 U (end 2/10/2023 12:00 AM) (lelong.com.my)](#)

Through the comparisons, **PROLINK Cat6 UTP Full Copper Cable** is more suitable among these options. This is because it can support high transmission bandwidth and a network speed of 10 Gbps up to 55 meters which is indeed a suitable length for the distance between the devices in the building. In terms of price, it is the cheapest with a suitable performance.

Expected Cost

No	LAN Devices	Quantity	Price per Unit (RM)	Total Price (RM)
1	Synology RT2600ac	1	2,815.00	2,815.00
2	S3910-24TS, 24-Port Gigabit Ethernet L2+ Switch	4	3,561.00	14,244.00
3	IWILLINK Patch Panel 48 Ports, Cat6 / Rj45 Patch Panel, 2u Network Patch Panel Utp 19-Inch, Black	4	256.37	1,025.48
4	TP-LINK EAP653 AX3000 Ceiling Mount WiFi 6 Access Point	8	629.00	5,032.00
5	PROLINK Cat6 UTP Full Copper Cable	9	299.00	2,691.00
Total Cost				25,807.48

Reflection

1. **Are you surprised by the prices? How were you surprised?**

Yes. This is because the total cost is really low compared to our budget of RM 3,000,000. We are also surprised by the price of the patch panel as the patch panel is not as expensive as we thought. However, we feel shocked about the price of the switch. The price of one switch is the highest which is RM 3561. Since we need 4 switches, the total cost of the switch will be RM 14, 244. After doing research, we are surprised by how different brands of products with similar functions and specifications can also have different prices. Even one product can also have a huge range between the prices.

In conclusion, it is important for us to understand our project in order for us to select the right product regarding the functions and specifications. Even though some products may be cheap, they may not reach our expectations. Vice versa, even though some products are expensive, we may not need the functions and specifications of the products.

2. **Have you ever considered cost as a factor for choosing networking devices?**

Yes, it is because cost is also one of the factors in network planning that needs to be given due consideration to meet the needs of users. Without sufficient cost, we cannot start buying the components or devices needed to build the network. A device with many features and capabilities at a lower price is an example of good spending for network production. If we want to have a good network, we have to consider the cost as an element that needs to be taken into account because it will help us in adding any additional features in developing a better network.

Cost is usually one of the most important factors when choosing equipment for a network. The capacity and features will determine the cost of a switch or router. Device capacity includes the number and type of ports available and the backplane speed. Network management capabilities, embedded security technologies, and optional advanced switching technologies are other factors that impact cost. The expense of cables required to connect each device to the network must also be considered. Another important element that affects cost considerations is how much redundancy to include in the network. This includes the device, the port of each device and the copper or fiber optic cable. This shows the importance of cost in the networking planning even though it is just a small business networking as it acts an important factor to meet the user needs.

3. Differences between the same devices from different brands

At first instance, products (devices) and brands seem the same, but by searching for the differences, we get to know their actual meanings. The fact that a product is a single entity, while a brand may include millions of products, is the primary distinction between the two. Therefore, the term "brand" is broader than "product". The brand alone is what people use to identify a product.. The main key difference between product (devices) and brand is that the product performs its general functions, but a brand offers value to the customers.

We obtained some findings by comparing between ASUS and Cisco routers. Asus routers provide a pleasant and stable networking experience, breeze to set up, have lots of options, and are very reliable. Moreover, it's only required to reboot it once or twice a year. ASUS routers tend to have 2 CPUs, one for Wi-Fi and one for cabled connections, which helps speed up Wi-Fi throughput speeds, and increases stability. Cisco routers required rebooting several times each month because it would overheat, dropout, or just randomly become unstable on some connected devices while others were fine. Cisco is often the cheapest solution, but they always use plastic casings, with poor ventilation, so you end up restarting the router from time to time as it inevitably becomes unstable.

In addition, For TP-Link Wireless Access Point has faster speed (including short distance and long distance) and wide coverage. They also have more accessories, such as smart parental controls and network security features. On the other hand, D-Link Wireless Access Point has high-gain antennas for wide coverage and Ethernet ports for wired devices.

TP-Link and D-Link are both very popular and well-reviewed brands in the Wi-Fi router market. Based on the comparison, we can conclude that TP-Link provides stable and reliable fast speed and wide coverage and it's sold at an affordable price. TP-Link is very suitable for all kinds of families, because of its simple and stylish design.

Reflection for Task 3

For this task, we need to find out what devices (network and end-user devices) are needed to achieve the objective of fulfilling the requirements and needs of the organization.We figure out that there are many different types of network devices like routers, switches, patch panels, wireless devices, and cables are coming in different brands like Cisco, Huawei and Asus with their own capabilities and price ranges. It was a tough task for us. But we learned that exploration is key here to start with a basic search on Networking Devices for universities and we work from there.

Hence, a lot of consideration needed to be taken to ensure that the devices that we bought met the specific usage requirements for the building. Moreover, we also encountered that the given budget for the project was not all spent via the list of devices needed. In fact, we must consider installation payment, configuration, technical and mechanical stuff as well as wiring. Everything will cost a value from the given budget.

3.4 TASK 4: MAKING THE CONNECTIONS - LAN AND WAN
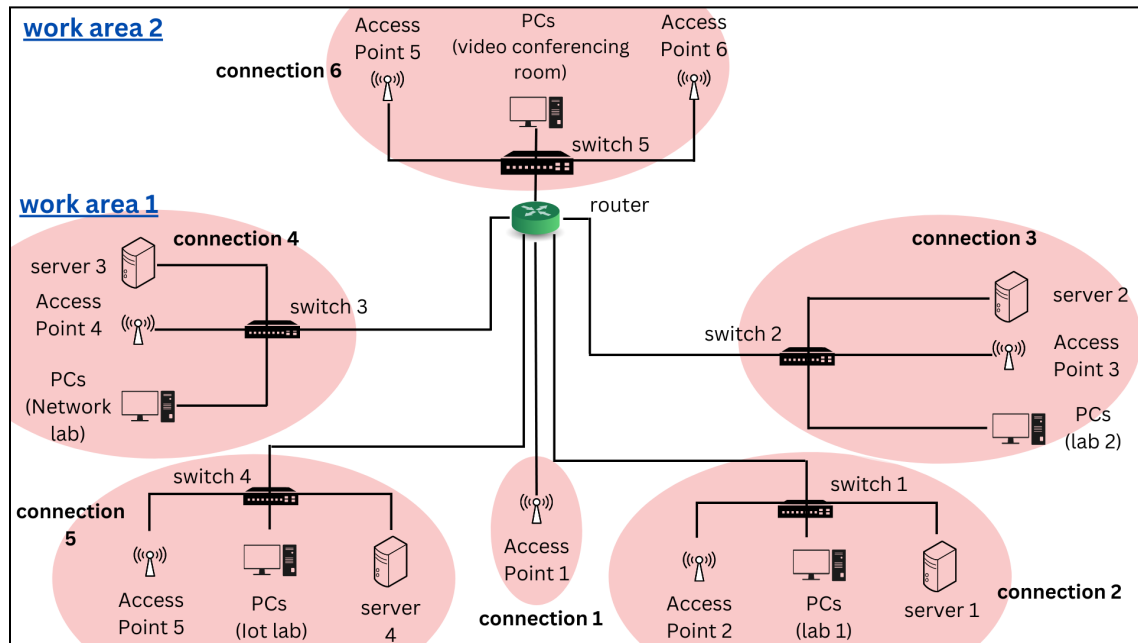
a. Identifying the work areas on the floor plan.
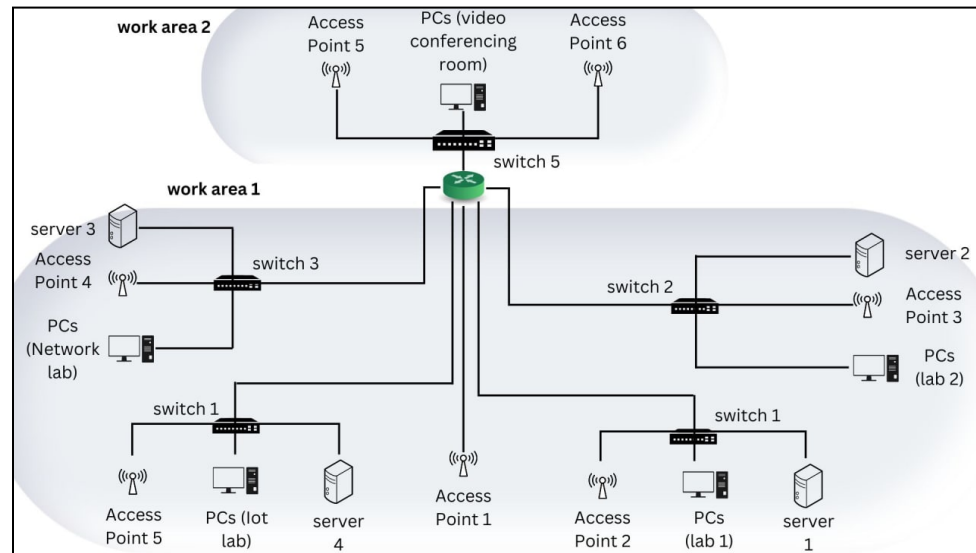
Figure 4: Work Areas on the Floor Plan

Work Area 1 - The ground floor of the building has provided a connection to four of the labs, a video conferencing room and the student lounge. The labs include two general-purpose labs, a network lab and an IoT lab. Each lab will have a 48-port switch that connects to the router and connects to 30 PCs (30 ports used), 1 access point (1 port used) and 1 server (1 port used). Thus, a total of 32 ports are used in each lab. Besides, the ground floor work area also provides a connection of access points for the end-user (PCs, tablets, laptops, smartphones) that directly connect with the router.

Work Area 2 - The first floor of the building provides a connection to a video conferencing room, and the student lounge. The first floor will be using a 48-ports switch that connects with the router. The switch will connect to 1 PC from 1 access point in each video conferencing room (1 port used in each room), 10 PCs in each video conferencing room (10 ports used in each room) and 1 access point at the student lounge (1 port used) which will use a total of 12 ports.

b. Identifying the number of connections, patch cords and switch ports.

<u>**The number of connections**</u>

Figure 5: Work Areas Connection on the Floor Plan

Based on the above diagram, we have identified six (6) connections for this project.
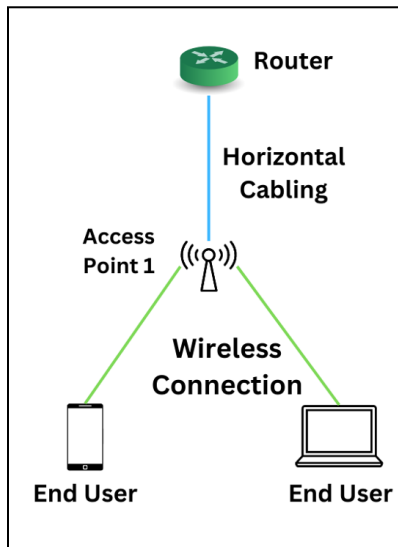
Figure 6: Connection 1
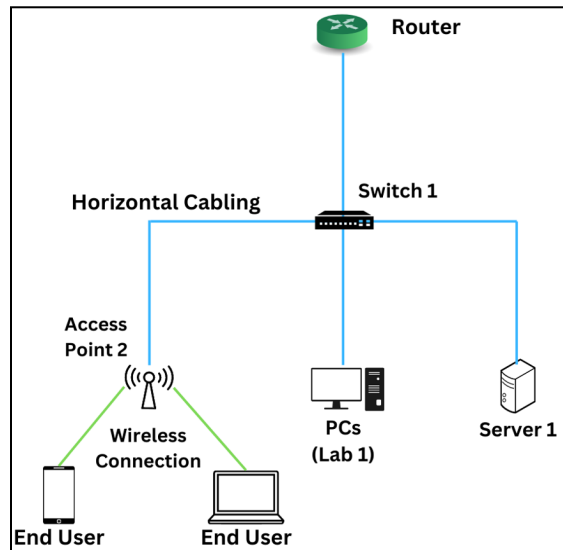
Figure 7: Connection 2
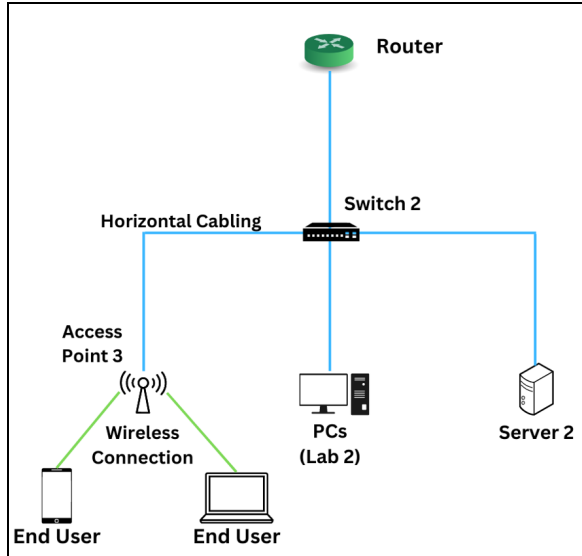
Figure 8: Connection 3
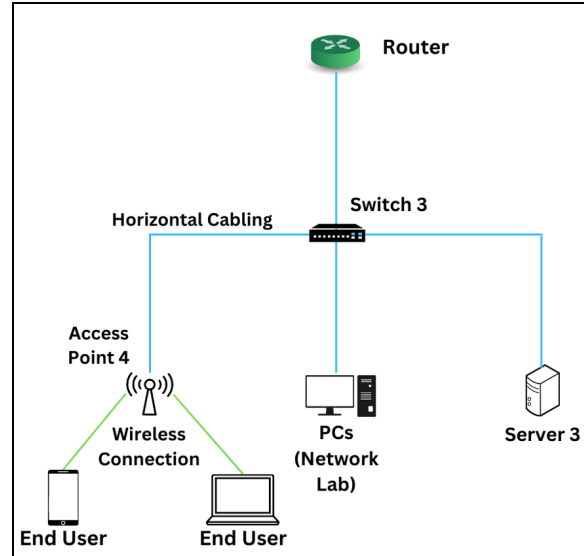
Figure 9: Connection 4
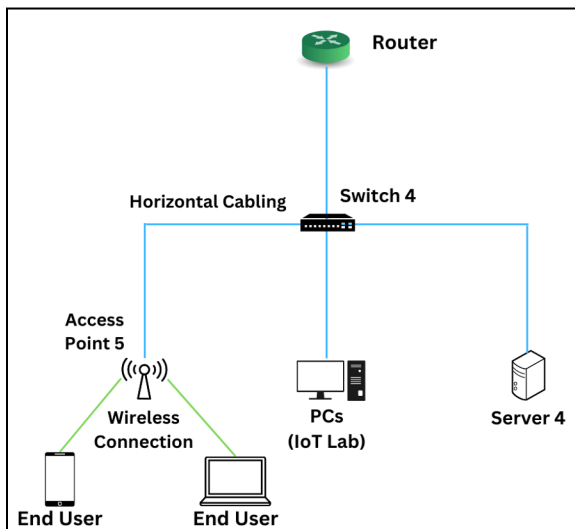
Figure 10: Connection 5
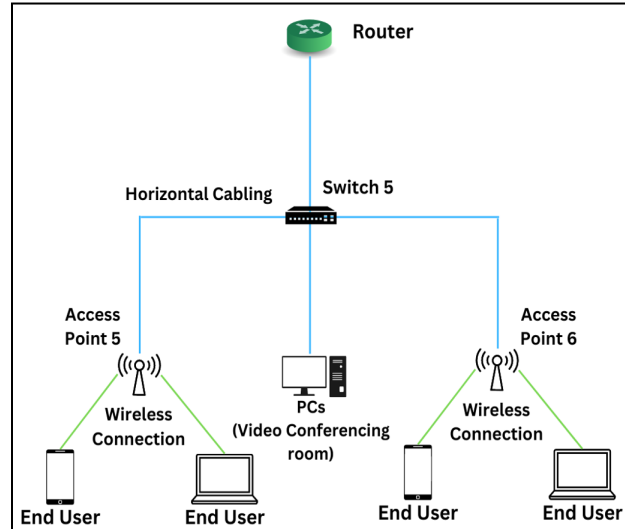
Figure 11: Connection 6

The number of patch cords

We use CAT6 cable as the patch cords. Overall, we will use approximately 146 patch cords.

In each lab, a 48-ports switch will connect with 30 PCs, 1 access point and 1 server. Thus, we will use 32 patch cords in each lab. Since there are four labs with one switch each, we need 4 patch cords to connect the switches to the router. Moreover, on the

ground floor, we have a connection between an access point to the router so we need 1 patch cord for it. The total number of patch cords used on the ground floor is 133.

On the other hand, for the first floor, we will use a 48-ports switch to connect the router with 1 patch cord. Then, we will use 10 patch cords in the connection between 10 PCs in the video conferencing rooms and the switch. Last but not least, we need 2 patch cords to connect 2 access points to the switch. The total number of patch cords used on the first floor is 13.

The number of switch port

For this project, we planned to use five 48-ports switches. Among the five switches, four will be used for the ground floor to connect each lab's PCs, server and access point to the router whereas one will be used for the first floor to connect PCs in the video conferencing room and two access points to the router. We planned to use switches that have PoE. Power over Ethernet (PoE) is a technology for wired Ethernet LANs (Local Area Networks) that allows the electrical current necessary for the operation of each device to be carried by the data cables rather than by power cords. Doing so, this can minimize the number of wires that must be strung in order to install the network. Besides, we have ensured the switches picked are able to transmit data at high speed.

c. **Identifying cable types and length.**

There are a total of 5 switches, one router and 6 access points in the building. We will use Cat6 cable in this building.

Ground floor
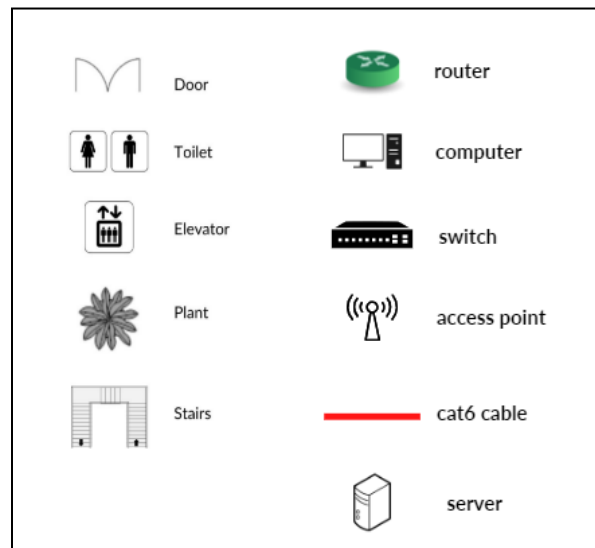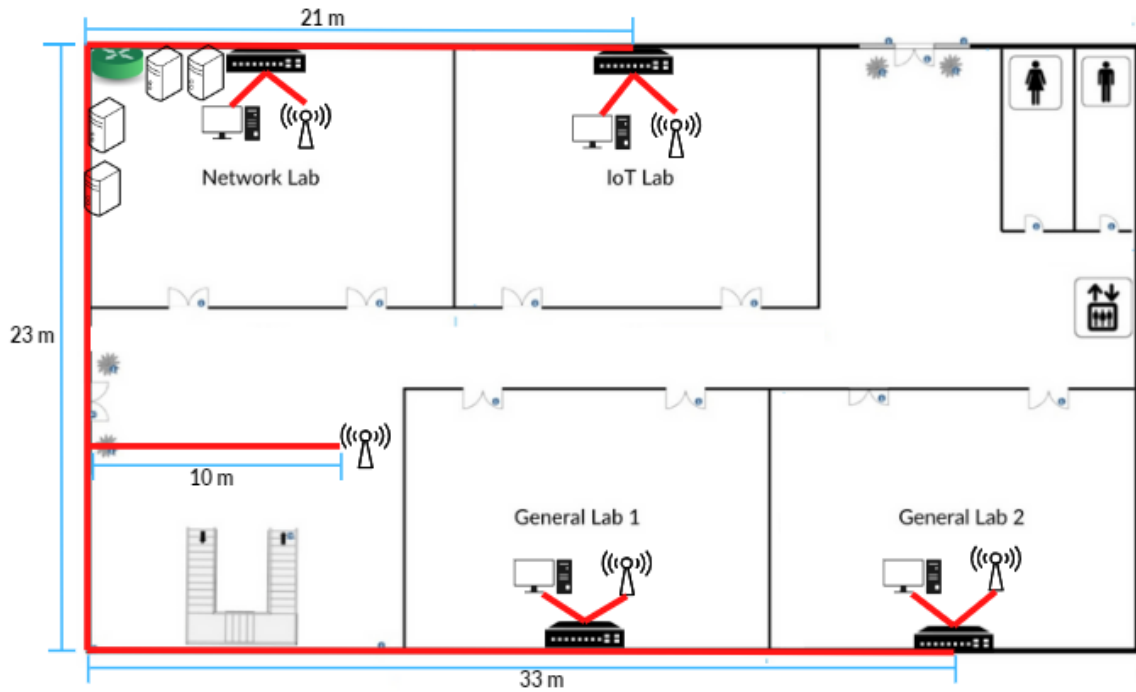
Figure 12: Ground Floor Network Connection

Estimated length of cat6 cable needed

= 4 switches to router + access point to router + 4 server to 4 switches

= (21+23+33+23+19+7)+(15)+(1+19+40+52)

=126+15+112

=253m

First floor

0.75 m

17.25 m

5 m

20 m

Legend:

Symbol	Description
Elevator	Elevator
Male toilet	Male toilet
Female toilet	Female toilet
Conferencing table	Conferencing table
Round table	Round table
Staircase	Staircase
Plant	Plant
Sofa	Sofa
Double door	Double door
Single door	Single door
Windows	Windows
Plant	Plant
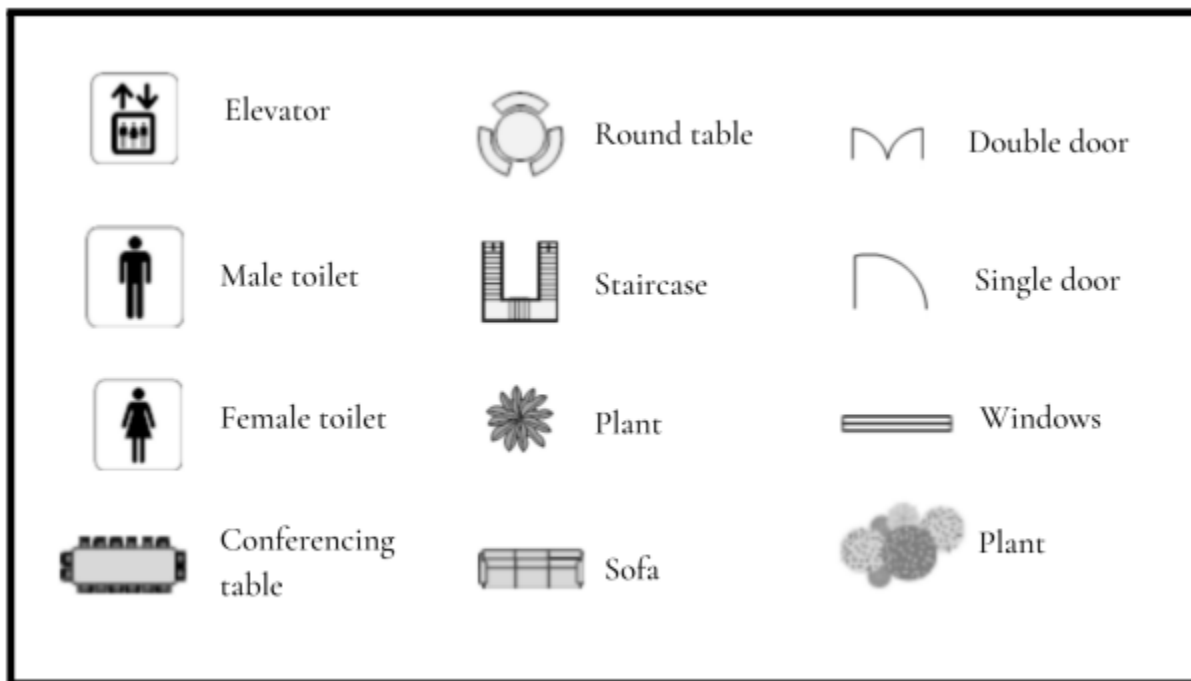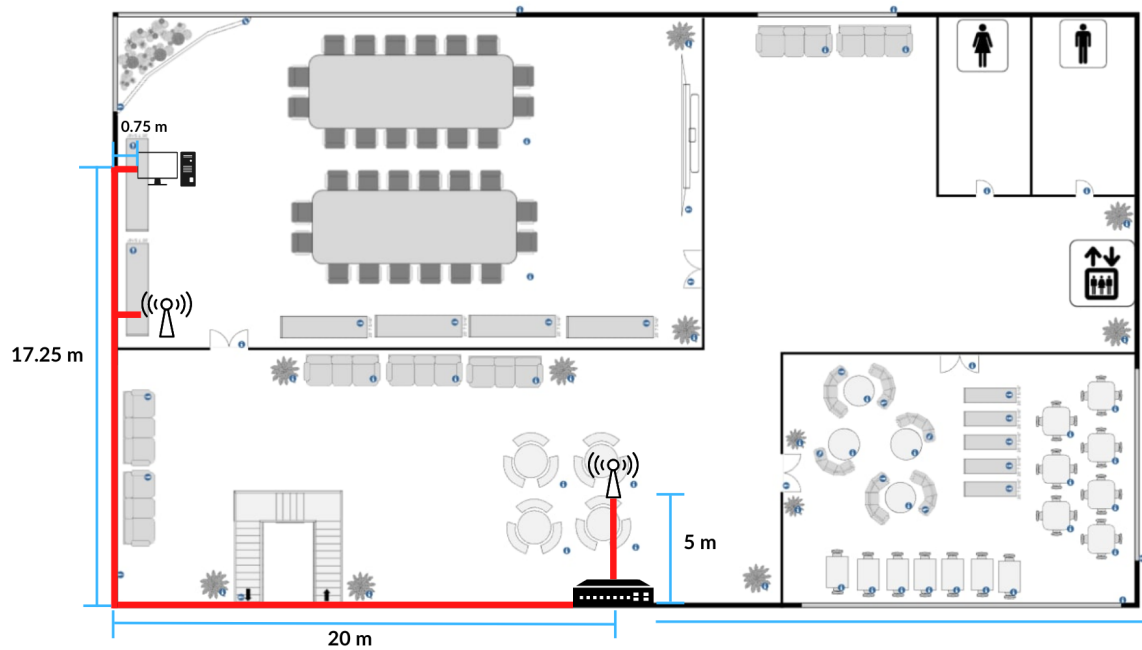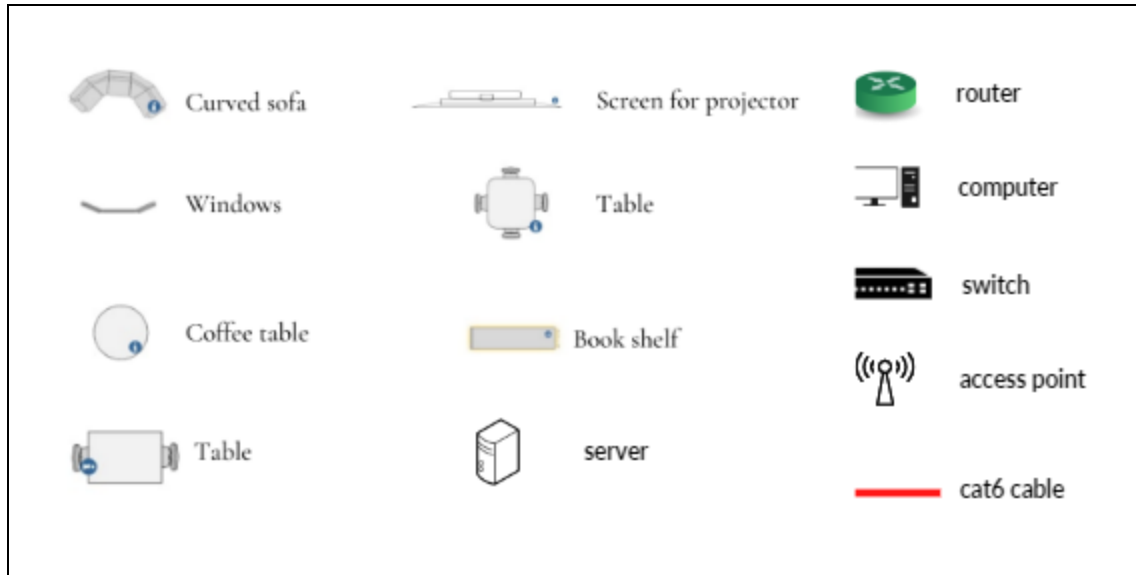
Figure 13: First Floor Network Connection

Estimated length of cat6 cable needed

= Router (Ground Floor) to Switch + Access Point to Switch + Video Conferencing
Room (Include PC and Access Point) to Switch

= 3 + 5 + (0.75+17.25+20) + (11.25 + 20)

= 77.25 m

Remark: 3m is the height from wall to ceiling.

Lab (2 General purpose labs, 1 Network lab and 1 IOT lab)
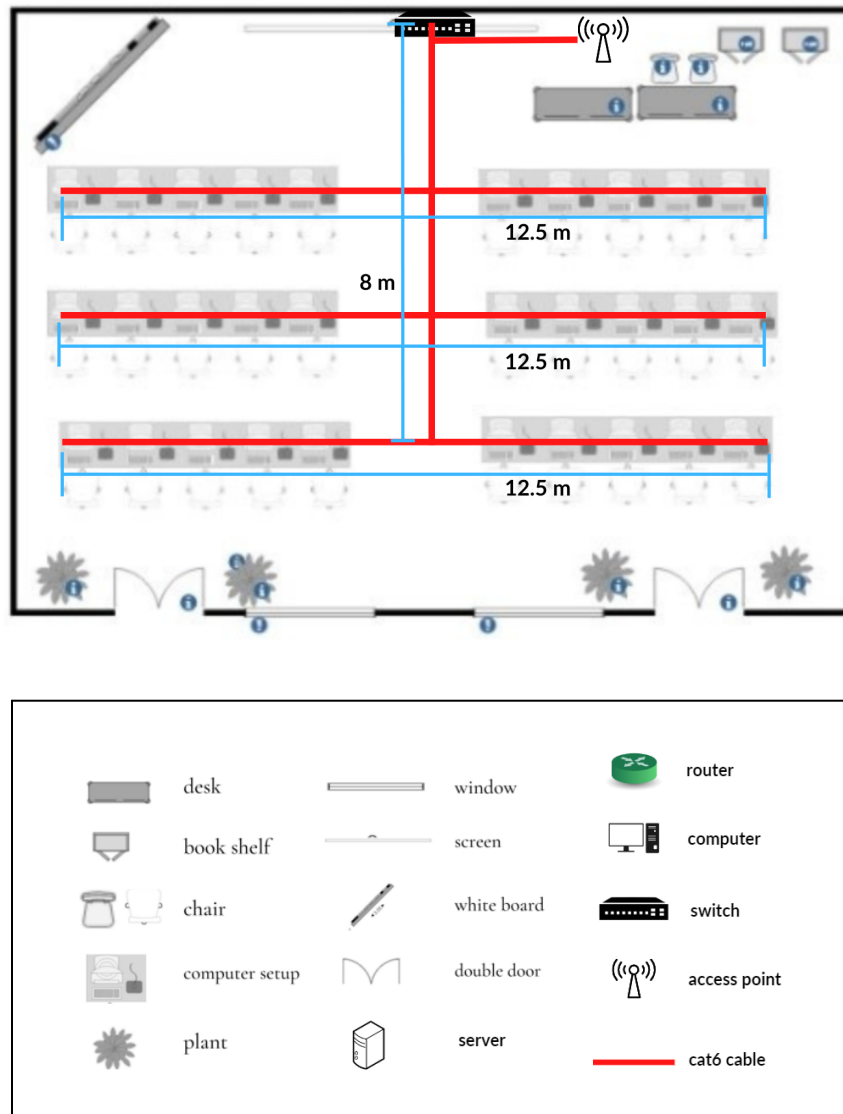
Figure 14: Network Connection for Each Lab

Estimated Length of Cat6 cable needed:

= Switch to access point + switch to each workstation PC

= 5 + [(5.25 + 6.25 + 7.25 + 8.25 + 9.25) x 2] + [(7.75 + 8.75 + 9.75 + 10.75 + 11.75)x2]

   + [(10.25 + 11.25 + 12.25 + 13.25 + 14.25) x 2]

= 5 + 72.5 + 97.5 + 122.5

= 287.5m

Video conferencing room
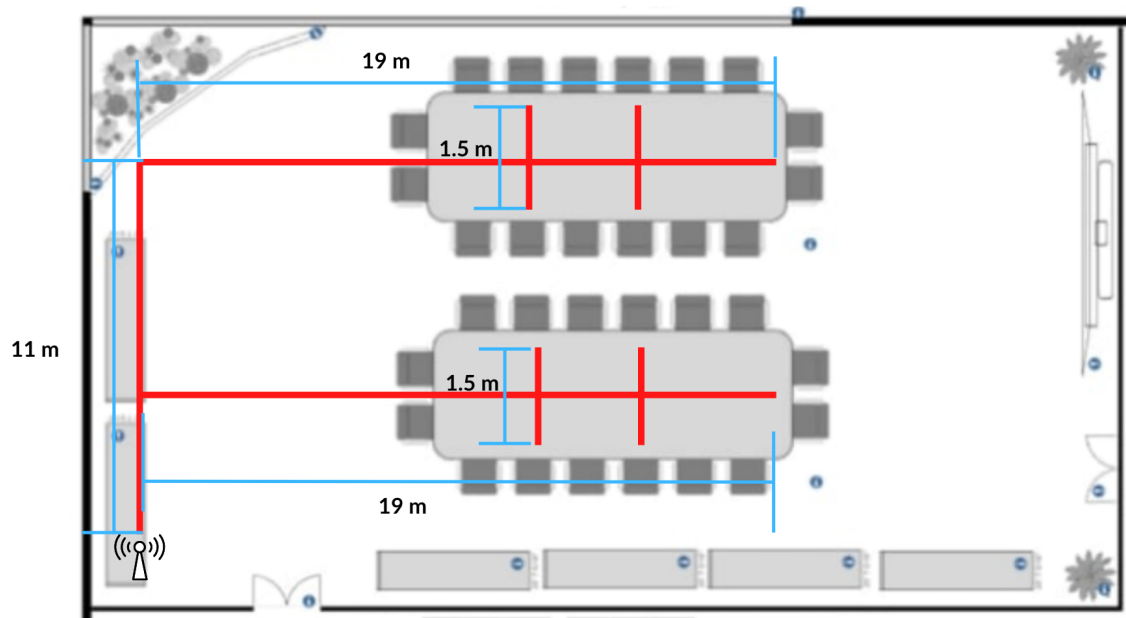
Figure 15: Video Conferencing Room Network Connection

Estimated length of Cat6 cable needed

= Access point to each workstation PC

= (11 + 19) + (4.5 + 19) + [(11 + 0.75 + 11) x 2] + [(11 + 0.75 + 14) x 2] + [(4.5 + 0.75 +

   11) x 2] + [(4.5 + 0.75 + 14) x 2]

= 30 + 23.5 + 45.5 + 51.5 + 32.5 + 38.5

= 221.5 m

Assume the ceiling height is 3m (around 10 feet)

(All estimation done based on the picture above and calculation is shown below.)

Estimated Total Length of Cat6 cable needed:

Ground Floor + First Floor

  = (General Purpose Lab1 + General Purpose Lab 2 + Network Lab + IoT Lab + Ground Floor Cable Connection) + (Video Conferencing Room + First Floor Cable Connection)

  = [(287.5 x 4) + 253] + (221.5 + 77.25)

  = 1701.5 m

  $\approx$ 1702 m

Reflection for Task 4

In this task, we are required to put all the infrastructure and devices into place. For example where the switch is placed in the lab? and how are these new rooms/networks connected to the main institution network? Once our group has chosen the internetworking devices that are needed for the network, the devices have been interconnected. We also take into consideration four physical areas when planning.. Based on our floor plan, we have measured the floor plan for the case study to see the maximum distance we have to cover. After we have finished measuring the floor plan, we have identified the work areas for both floor 1 and 2

Moreover, we measure the floor plan to see the maximum distance needed to cover from the MDF (Main Distribution Facility) to correctly suggest locations and cable structure. We also add in the cable length going up the walls and around corners. Cable lengths have been determined and matched with technology used.Estimated Total Length of Cat6 cable needed for this project was approximately 1702 m while ceiling height is 3m. For the network distribution, we have carefully considered all the factors required to make the connection of the work areas for networking to be working successfully.

3.5 TASK 5: IP ADDRESSING SCHEME

Introduction

IP addressing is important in ensuring that each host can connect to the network without address conflict. In this assignment, we need to explore the best way to subdivide the subnets from the network address assigned to our group. Below are the available networks listed according to the group and the network address assigned to our group is 192.18.0.0/8.

Group/Section	Network Address
1	192.16.0.0/8
2	192.17.0.0/8
3	192.18.0.0/8
4	192.19.0.0/8
5	192.20.0.0/8
6	192.21.0.0/8
7	192.22.0.0/8
8	192.23.0.0/8
9	192.24.0.0/8
10	192.25.0.0/8

Figure 16: Network Address Assigned for Our Group

Since the notation is /8, the subnet mask is 255.0.0.0. By doing the AND operation, on the IP address and the subnet mask, we get the network address of 192.0.0.0 and the broadcast address of 192.255.255.255. Therefore, the usable IP address that we can use to assign to the end hosts ranges from 192.0.0.1 to 192.255.255.254.

Subnet Mask	Network Address	Broadcast Address	Usable Host IP Address
255.0.0.0	192.0.0.0	192.255.255.255	192.0.0.1 - 192.255.255.254

We have 4 labs in total which includes 2 General Purpose Lab, 1 IoT Lab and 1 Network Lab, and a Video Conferencing Room. Therefore, task 5 requires us to divide the IP addresses according to the number of end users for each room.

Work Area

Ground Floor
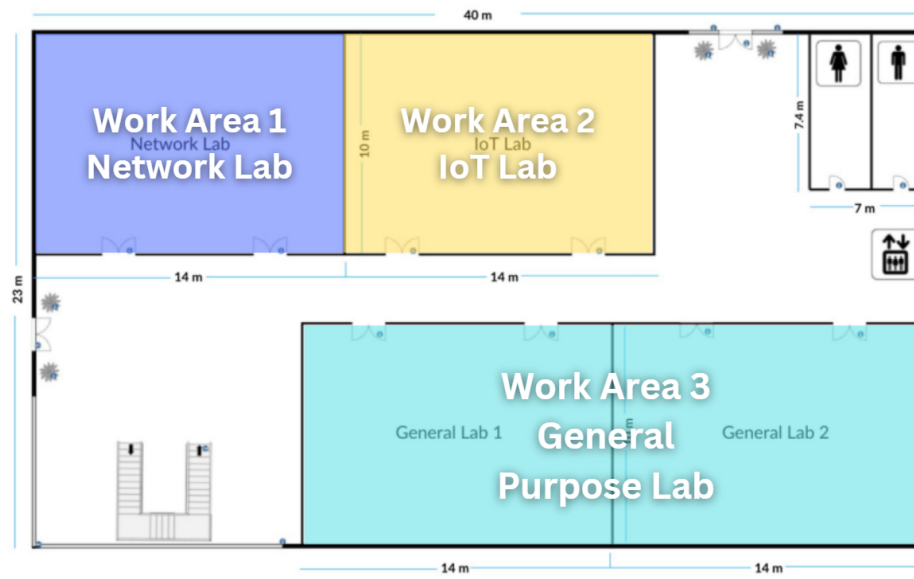
Figure 17: Work Areas on Ground Floor

First Floor
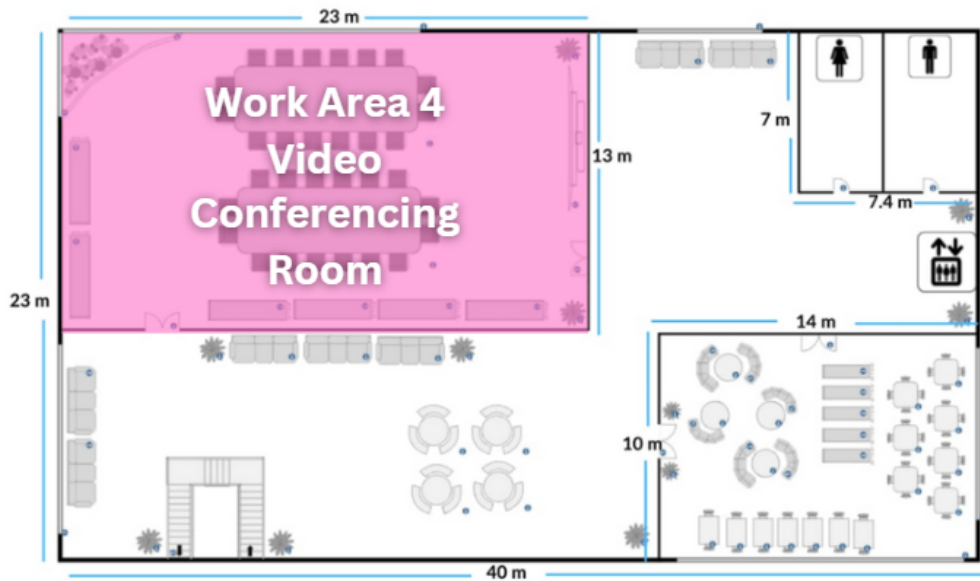
Figure 18: Work Area on First Floor

A. Subnet mask.

Subnet	Area	Subnet Mask (Binary)	Subnet Mask (Decimal)
1	Network Lab	11111111.00000000.00000000.00000000	255.0.0.0
2	IoT Lab		
3	General Purpose Lab		
4	Video Conferencing Room		

B. Range of IP address, network and broadcast address for subnet.

Subnet	Area	Range of IP Address	Network Address	Broadcast Address
1	Network Lab	192.18.1.1 - 192.18.1.33	192.18.1.0	192.18.1.34
2	IoT Lab	192.18.2.1 - 192.18.2.33	192.18.2.0	192.18.2.34
3	General Purpose Lab	192.18.3.1- 192.18.3.63	192.18.3.0	192.18.3.64
4	Video Conferencing Room	192.18.4.1 - 192.184.2	192.18.4.0	192.18.4.3

C. Range of IP addresses allocated for user types based on the area.

i. Work Area 1: Network Lab

User	IP Range
Switch	192.18.1.1
Server	192.18.1.2
Access Point	192.18.1.3
Student PC (30 PCs)	192.18.1.4 - 192.18.1.33

ii. Work Area 2: IoT Lab

User	IP Range
Switch	192.18.2.1
Server	192.18.2.2
Access Point	192.18.2.3
Student PC (30 PCs)	192.18.2.4 - 192.18.2.33

iii. Work Area 3: General Purpose Lab

User	IP Range
Switch	192.18.3.1
Server	192.18.3.2
Access Point	192.18.3.3
Student PC (60 PCs)	192.18.3.4 - 192.18.3.63

iv. Work Area 4: Video Conferencing Room

User	IP Range
Switch	192.18.4.1
PC (1 PC)	192.18.4.2

Reflection for Task 5

  For this task, we explore the best way to divide the subnetwork from the Network Address that has been assigned to our group which is 192.18.0.0/8. We learned that IP addressing is crucial in making sure that every host can connect to the network without conflict of addresses. We divide it in the best possible way for our network into all the different labs and rooms which cover the network lab, IoT lab, general purpose lab and video conferencing room.

4.0 CONCLUSION

ACHIEVEMENT:

The main goal of this project is to build an upgraded Faculty of Computing with the building to be 'ready for anything' and have a reliable, efficient and secure network that can be easily managed. It took a few weeks to complete this project. The project can be considered as success and achieving the goals we have set for each task. First of all, after identifying the requirements of the project, we have successfully completed our project within the given budget which is RM3,000,000.

Furthermore, we also have achieved our other goals which is to upgrade the network system that will allow them to utilize the elements to help their business. Those elements are.

- A system that is easy to manage and scalable
- Improve overall performance.
- Supply protection from network breaches such as Internet Worms, denial-of-service attacks and e-business application attacks.
- Capability to support high-performance to the core backbone
- Ability to support features such as Quality of Service and security in hardware via access control lists (ACLs).
- Enable secure VPN connections from remote locations

We must admit that the project is not as easy as we thought because we have faced a lot of problems and obstacles in every project task. However, we worked effectively together. We understood each of our strengths and made sure they were used throughout this project. We learned how to choose the appropriate network devices depending on the requirement and budget given by creating our own floor plan. It was a great experience for us to draw the floor plans and determine the suitable position of each device. Moreover, we also learned the ways to set the IP address scheme for every network in the whole system and identified the proper connections and cables

STRENGTH

Besides the fundamental knowledge of the network system, we also learned the importance of teamwork in a project. We are always aware that we work as a team. It does not mean that some do the work and others just coast and do nothing. Getting our hand into everything is the key , as this is how we learn. We have conducted a meeting for every task before we started to work on it. It was one of the effective ways to ensure all the team members know the workflow and progress of the project from start to end in detail. We believed the cooperation and communication between the team are the key to a successful group project. One of the great aspects that we learn in this project is time management. We always ensure that our given tasks have been done in a given time. We always keep in our mind that it is easy to put things to the last minute and pushing things to the last minute will reflect our work.

WEAKNESS

Insufficient understanding of network system planning at the first stages was very challenging for us where it was our main weakness. We have zero experiences and basic knowledge where we could make mistakes. For example, things that we find difficult are making connections. How are these new rooms/networks connected to the main institution network? and how do you connect the different floors? So,during these stages we tend to make decisions on a very simple model that we were confident and could complete within the amount of time we were given to finish the project.However, we tend to do more research to gain sufficient information that is needed to design a good network.

In conclusion, we are very grateful by giving an opportunity to do this project and apply our knowledge learned from the course. We do believe all the lessons we learnt in this project would be very beneficial to us in the future

5.0 TEAM MEMBER AND RESPONSIBILITY

Task 1

Team member	Responsibility
Lu Qi Yan	1. Brief on task 1 2. Meeting minutes
Lee Rong Xian	1. lists all the requirements for task 1 2. Divided the task into 4 parts 3. Sketch 1 video conferencing room and 1 student lounge
Harchana	1. Sketch 2 general purpose labs
Yusra	1. Sketch 1 Network lab and 1 IOT lab

Task 2

Team member	Responsibility
Lu Qi Yan	1. Brief on task 2 2. Divided the task into 4 parts 3. Answer for 2 question 4. Project feasibility
Lee Rong Xian	1. Suggested 10 question 2. Answer for 2 question 3. Meeting minutes
Harchana	1. Answer for 3 question
Yusra	1. Answer for 3 question

Task 3

Team member	Responsibility
Lu Qi Yan	1. Doing 1 parts of LAN devices (router)
Lee Rong Xian	1. Doing 1 part of LAN device (wireless access point & cable)
Harchana	1. Doing 1 part of LAN device (switch) 2. Meeting minutes
Yusra	1. Doing 1 part of LAN device (patch panel)

Task 4

Team member	Responsibility
Lu Qi Yan	1. Brief on task 4 2. Divided the task into 4 parts 3. Part A - Sketching and Part C
Lee Rong Xian	1. Part B – Sketching and identify the number of patch cords and switch ports 2. Meeting minutes
Harchana	1. Part B – Identify the number of connections
Yusra	1. Part A - Identify the work areas

Task 5

Team member	Responsibility
Lu Qi Yan	1. IP addresses for the IOT Lab
Lee Rong Xian	1. Brief on task 5 2. IP addresses for the Network Lab
Harchana	1. IP addresses for the General Purpose Lab
Yusra	1. Divided the task into 4 parts 2. IP address for the video conferencing room 3. Meeting minutes

Task 6

Team member	Responsibility
Lu Qi Yan	1. Abstract
Lee Rong Xian	1. Project background and overview of the client's current status and issue 2. Compile the report til task 4
Harchana	1. Reflection task 4,5 2. Conclusion
Yusra	1. Rearrange the report 2. Table of content 3. Table of figure 4. Introduction 5. Reflection task 1,2,3

6.0 REFERENCES

Task 2

1. Cybersecurity & Infrastructure Security Agency (CISA). (2018, June 21). *Security Network Infrastructure Devices*. Retrieved November 7, 2022, from https://www.cisa.gov/uscert/ncas/tips/ST18-001

2. Teodor Topalov. (2015). *An Overview of Essential Security Measures for Competitive Organizations*. Retrieved November 7, 2022 from http://www.inquiriesjournal.com/articles/1269/2/an-overview-of-essential-security-measures-for-competitive-organizations

3. Finn McChuhil. (2018). *How to Set Up IP address for an Office*. Retrieved November 7, 2022, from https://smallbusiness.chron.com/set-up-ip-addressesoffice-51486.html

4. Anthony Novello. (2020). *How a Fiber Optic Backbone Network Can Save You Down Time*. Retrieved November 7, 2022, from https://www.buildingsiot.com/blog/how-a-fiber-optic-backbone-network-can-save-you-down-time-bd#:~:text=Benefits%20include%3A&text=Easier%20to%20install%20due%20to,considerable%20resistance%20to%20electromagnetic%20interference

5. AH Ari Howard Sep 7, & Howard, A. (2022, October 11). *Internet speeds explained: How to pick The speed you need*. Allconnect. Retrieved November 7, 2022, from https://www.allconnect.com/blog/consumers-guide-to-internet-speed

6. Vertiv. (2021, June 30). *What is a server room?*. Retrieved November 7, 2022, from https://www.vertiv.com/en-asia/about/news-and-insights/articles/educational-articles/what-is-a-server-room/

7. Prasanna Bidkar. (2022). *How Do Routers Provide Security?*. Retrieved November 8, 2022 from https://smallbusiness.chron.com/routers-provide-security-70778.html

8. CloudFlare. (2022). *What is a Router?*. Retrieved November 8, 2022 from https://www.cloudflare.com/learning/network-layer/what-is-a-router/

9. John Burke. (2020, June). *Network Switch*. Retrieved November 8, 2022 from https://www.techtarget.com/searchnetworking/definition/switch

10. Jessica Ciesla. (2018, May 29). *Secure Switches Can Defend Against Cyber Attacks*. Retrieved November 8, 2022 from https://www.raritan.com/blog/detail/secure-switches-can-defend-against-cyber-attacks

11. Pearson. (2012, Jan 24). *Basic Switch Security Concepts and Configuration*. Retrieved November 8, 2022 from https://www.pearsonitcertification.com/articles/article.aspx?p=1829347#:~:text=The%20simplest%20form%20of%20switch,Statically

12. CloudFlare. (2022). *What is DNS? | How DNS Works*. Retrieved from https://www.cloudflare.com/learning/dns/what-is-dns/

13. SNIA. (2022). *What Is a Storage Area Network (SAN)?*. Retrieved November 8, 2022 from https://www.snia.org/education/storage_networking_primer/san/what_san

14. CloudFlare. (2022) *What Is DNS Security?*. Retrieved November 8, 2022 from https://www.cloudflare.com/learning/dns/dns-security/

15. Jenna Phipps. (2022, Oct 25). *What Is Storage Area Network Security?*. Retrieved November 8, 2022 from https://www.enterprisestorageforum.com/networking/san-security/

16. Nick Bambulas. (2022, May 10). *10 Proven Ways to Secure a Computer Network*. Retrieved November 8, 2022 from https://www.gflesch.com/elevity-it-blog/ways-to-secure-a-computer-network

17. Logsign Team. (2019, Mar 13). *How to Ensure Network Security?*. Retrieved November 8, 2022 from https://www.logsign.com/blog/how-to-ensure-network-security/

18. Amy Mersch. (2021, Oct 4). *What is Layered Security & How Does it Defend Your Network?*. Retrieved November 8, 2022 from https://blog.totalprosource.com/what-is-layered-security-how-does-it-defend-your-network

19. Fiberplus. (2020, Mar 11). *How Schools and Students Can Benefit From Fiber Optic Technology*. Retrieved November 8, 2022 from https://www.fiberplusinc.com/services-offered/schools-benefit-fiber-optic-technology/

20. Jayasekara, G. P. D. C. M. (2022). *Computer Networks For A School: Case Study Analysis.* Computer Networks For A School: Case Study Analysis (September 13, 2022).

Retrieved November 8, 2022 from

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4217756

21. Kelly, S. & Kumar, K. (2022). *LAN Networking*. In Unity Networking Fundamentals (pp. 239-247). Apress, Berkeley, CA. Retrieved November 8, 2022 from https://link.springer.com/chapter/10.1007/978-1-4842-7358-6_7

22. Raghunandan, K. (2022). *Wireless LAN (Local Area Network).* In Introduction to Wireless Communications and Networks (pp. 223-245). Springer, Cham. Retrieved November 8, 2022 from https://link.springer.com/chapter/10.1007/978-3-030-92188-0_12

23. Leliopoulos, P. & Drigas, A. (2022). *The evolution of wireless mobile networks and the future 5G mobile technology for sustainability*. Technium Sustainability, 2(4), 28-43. Retrieved November 8, 2022 from https://techniumscience.com/index.php/sustainability/article/view/7346

Task 3

1. Cisco System. (2022). What is an Access Point? Retrieved December 7, 2022 from https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-access-point.html#~types-of-access-points

2. What is a router? (n.d.). Retrieved December 24, 2022 from https://www.cloudflare.com/learning/network-layer/what-is-a-router/

3. Hyde, P. (2022, September 20). The 7 best small business routers of 2022. The Balance. Retrieved December 25, 2022 from https://www.thebalancemoney.com/best-small-business-routers-4171956

4. Sharma, A. K., Wadhawan, S., Datta, R., & Mittal, S. K. (2022). Inter-networking: An Elegant Approach for Configuring Layer-2/Layer-3 Devices for Attaining Impulsive Outcomes. In Sustainable Communication Networks and Application (pp. 1-27). Springer, Singapore. Retrieved December 26, 2022 from https://link.springer.com/chapter/10.1007/978-981-16-6605-6_1

5. Andrew F. (2021, November). Patch panel. Retrieved December 26, 2022 from https://www.techtarget.com/searchnetworking/definition/patch-panel#:~:text=A%20patch%20panel%20in%20a,incoming%20and%20outgoing%20LAN%20cables.

6. Rack Solutions. (2019, September 6). Patch Panel: What it is and Why Your Data Center Needs it. Retrieved December 26, 2022 from https://www.racksolutions.com/news/blog/patch-panel/

7. Shehzad, M. N., Kamboh, U. R., Taqdees, M. D., Waheed, Z., Usman, M., & Buttar, A. M. (2021, November). Diverse Dynamic Routing Protocols Distribution in the Large Network with Route Redistribution Techniques using GNS3. In 2021 International Conference on Innovative Computing (ICIC) (pp. 1-7). IEEE. Retrieved December 26, 2022 from https://ieeexplore.ieee.org/abstract/document/9692938/

7.0 APPENDICES

Group 3, The Phoenix
MEETING FOR TASK 1   28/10/2022

28 OCTOBER 2022 / 7:30 PM / GOOGLE MEET

ATTENDEES

Lee Rong Xian, Lu Qi Yan, Yusra Nadatul Alyeea, Harchana

AGENDA

Make sure all of us understand task 1.

1. Lu Qi Yan does a briefing on task 1 to make sure all of the team members understand the task.

2. Lee Rong Xian lists all the requirements for task 1 in our telegram group.

3. Harchana and Yusra are highly active in asking questions and answering other members' confusion.

Decide the detail of the floor plan.

1. We discuss the details in the floor plan, such as which lab should be on which floor, and how many toilets for each floor.

2. We also discuss the size and shape of the floor plan.

3. The minimum size is calculated and then decided after discussion among members.

Divide the task.

1. The task is divided into 4 parts by Lee Rong Xian.
2. One member will do the meeting minutes while three other members will do the floor plan.

Finish the task.

1. Team members will start to sketch the floor plan together by using 'SmartDraw' an online application.
2. Members are highly cooperative and work together until finish sketching the floor plan.

NOTES

- 2 general purpose labs, 1 Network lab, and 1 IOT lab will be on the ground floor while the video conferencing room and student lounge will be on the first floor.

- The size of each floor will be 800m^2 .

- Details of the division task are as follows:
  - Meeting minutes by Lu Qi Yan.
  - 2 general purpose labs will be sketched by Harchana.
  - 1 Network lab and 1 IOT lab will be sketched by Yusra.
  - 1 video conferencing room and 1 student lounge will be sketched by Rong Xian.

ACTION ITEMS

Bil	Items	Status
1.	Make sure all of us understand task 1.	Done
2.	Decide the detail of the floor plan.	Done
3.	Divide the task.	Done
4.	Finish the task.	Done

Group 3, The Phoenix

MEETING FOR TASK 2
07/11/2022

ATTENDEES

Lee Rong Xian, Lu Qi Yan, Yusra Nadatul Alyeea, Harchana

AGENDA

Confirmation for the 10 questions of problem statement.

1. Lu Qi Yan does a briefing on task 2 to make sure all of the team members understand the task.

2. Lee Rong Xian suggests 10 questions for the problem statements in our telegram group.

3. Harchana and Yusra suggest their ideas about the problem statements.

Divide the task.

1. The task is divided into 4 parts by LU QI YAN.

2. Suggested that **two** of the group members be in-charge of answering 3 questions each, **one** of the group members in-charge of answering 2 questions with the discussion of feasibility, and **one** of the group members in-charge of answering 2 questions with meeting minutes.

Finish the task.

Bil	Items	Status
1.	Make sure all of us understand task 1.	Done
2.	Decide the detail of the floor plan.	Done
3.	Divide the task.	Done
4.	Finish the task.	Done

ACTION ITEMS

Bil	Items	Status
1.	Confirmation for the 10 questions of the problem statement.	Done
2.	Divide the task.	Done
3.	Finish the task.	Done

Group 3, The Phoenix

MEETING MINUTES FOR TASK 3

19/12/2022 (MONDAY)

---

19 DEC 2022 / 13:00 PM / N28 BK1

ATTENDEES

Lee Rong Xian, Lu Qi Yan, Yusra Nadatul Alyeea, Harchana

(All the group members were present)

AGENDA

a) Research the different network devices that we need to accomplish the objective.

b) Decide which LAN devices we need to accomplish the needs as mentioned in the case

study.

c) Find information on the devices that have been chosen

1. Harchana does a briefing on task 3 to make sure all of the team members understand the task.

2. All the group members have been do research on the different network devices for further discussion.

3. All of them were suggest their ideas on choosing the appropriate the right LAN devices.

During the discussion,

   a. Lee Rong Xian suggests which LAN devices is to accomplish.

   b. Yustra do a quick survey on market prices of the LAN devices

   c. Lu Qi Yan find further information on the LAN devices

   d. Harchana do search on suitable networking devices for schools or universities and how many of them are required for further use.

Divide the task.

1. The task is divided into 4 parts by Lee Rong Xian.

2. 1 person will do meeting minutes with one part of LAN device.

3. 1 person will do 2 part of LAN devices.

4. Other 2 people will do the remaining 2 part of LAN devices.

Finish the task.

Bil	Items	Group member
1.	Doing 1 part of LAN device (switch) with meeting minutes	Harchana A/P Arulappan
2.	Doing 2 parts of LAN devices (wireless access point & cable)	Lu Qi Yan
3.	Doing 1 part of LAN device (patch panel)	Yusra Nadatul Alyeea
4.	Doing 1 part of LAN device (router)	Lee Rong Xian

ACTION ITEMS

Bil	Items	Status
1.	Research the different network devices that we need to accomplish the objective	Done
2	Decide which LAN devices we need to accomplish the needs as mentioned in the case study.	Done
3	Find information on the devices that have been chosen.	Done
4	Divide the task.	Done
5	Finish the task.	Done

Group 3, The Phoenix

MEETING FOR TASK 4
28/12/2022

ATTENDEES

Lee Rong Xian, Lu Qi Yan, Yusra Nadatul Alyeea, Harchana

AGENDA

Initiate the task.

1. Lu Qi Yan leads the discussion and analyse the task to make sure all the member understands.

2. Lee Rong Xian emphasis to the group members to do research on the project.

3. Harchana and Yusra suggest their ideas about task 4.

Divide the task.

1. The task is divided into 4 parts by LU QI YAN.

2. Suggested that **one** of the group members be in charge of **part a**, **one** of the group members in-charge of **part b**, and **two** of the group members in charge of **part c**.

Finish the task.

Bil	Items	Group member
1.	Part A - Identify the work areas	Yusra Nadatul Alyeea
2.	Part A - Sketching and Part C	Lu Qi Yan
3.	Part B – Sketching and identify the number of patch cords and switch ports	Lee Rong Xian
4.	Part B – Identify the number of connections	Harchana A/P Arulappan

ACTION ITEMS

Bil	Items	Status
1.	Connections, patch cord, and switch port identified	Done
2.	Cable length and types identified	Done
3.	A sketch of the PC and Network device arrangement (+cable) is clearly shown and labeled	Done

Group 3, The Phoenix

MEETING MINUTES FOR TASK 5

28 December 2022 (Wednesday)

ATTENDEES

Harchana, Lee Rong Xian, Lu Qi Yan, Yusra Nadatul Alyeea

AGENDA

a) **Get the Network Address from your lecturer (the project representative).**
b) **Divide it in the best possible way for your network - all the different labs and rooms.**

1. Lee Rong Xian does a briefing on task 5 to make sure all of the team members understand the task.
2. All of the group members decide who will get the network IP address from the lecturer.
3. All of us do some research about how to divide and calculate the IP address for each room.

Divide the task

1. Yusra divided the task into 4 parts.
2. 1 person will do the meeting minutes and the IP address for the video conferencing room.
3. 1 person will do the IP address for the IOT Lab.
4. 1 person will do the IP address for the Network Lab.
5. 1 person will do the IP address for the General Purpose Lab.

Finish the task

No.	Items	Members
1.	Do the meeting minutes and the IP address for the video conferencing room.	Yusra Nadatul Alyeea
2.	Do the addresses for the IOT Lab.	Lu Qi Yan
3.	Do the addresses for the Network Lab.	Lee Rong Xian
4.	Do the addresses for the General Purpose Lab.	Harchana

ACTION ITEMS

No.	Items	Status
1.	Get the network address from the lecturer.	Done
2.	Divide it in the best possible way for your network - all the different labs and rooms.	Done
3.	Divide the task.	Done
4.	Finish the task.	Done