UTM

UNIVERSITI TEKNOLOGI MALAYSIA

SECR1213-09

KOMUNIKASI RANGKAIAN

(NETWORK COMMUNICATIONS)

SEM1_2021

PROJECT

NETWORK DESIGN FOR SCHOOL OF COMPUTING N28B

GROUP MEMBER	MATRIC NO
CHIAM WOOI CHIN	A19EC0034
GOH JO EY	A19EC0047
NG JING ER	A19EC0115
ONG YIN REN	A19EC0204

ABSTRACT

A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data (Computer Hope,2020). In this project, we assumed ourselves as network consultants who were responsible for designing and setting up a small network for an organization. However, it requires a lot of research throughout the project. We have proposed a design of a two-storey building and also designed a plan of network with the most suitable components. The proposed network infrastructure is constructed based on the discussion of the research done. The network devices proposed include ASUS RT-AX88U WiFi 6 Router, 48 Port Switch and 8 port switch, generator, 48 port patch panels, Wireless Access Point, CAT 6A cable and Fibre Optic Patch Cable. A star topology has been chosen as the LAN topology to be implemented in the network as it is best suited for smaller networks and works efficiently when there is a limited number of nodes. All the network devices are chosen based on their own capabilities and price ranges which have been considered as a factor to consider the feasibility of the project. We have also proposed the network devices arrangement and cabling structure where we have considered four physical areas when planning including work area, telecommunications room, vertical cabling and horizontal cabling. The estimated total quantity of cable needed for the physical connections also was calculated to make sure the connection of networking to be successful. We also discuss IP addressing which is crucial in making sure that every host can connect to the network without conflict of addresses. For this project, we divided the subnetwork from the network address, 192.20.0.0/8 into the network portion indicated by subnet mask (/8) and the host portion is the remaining bits (32-8=24 bits) and assigned the 14 subnets according to the work area of routers and switch. All the decisions for the network design are made after discussion and a lot of research to fulfil the requirement of the feasibility of the project

TABLE OF CONTENTS

TABLE OF FIGURE

1.0 INTRODUCTION

A good network design in a university can enhance the productivity and the efficiency of the communication among the staff, lecturers, students, and also the outsiders. In this project, we are going to design a network for the upgrade needs in the school of computing at the University of Technology Malaysia. The network design can help the users in the school of computing to have full access to the learning and working information, enhance the communication among the users in the school environment, support the services related to the learning process, and also enhance administrative efficiency. A network for a double-story building, N28b is planned step by step in this project. The network design is planned for almost 1330 people with an anticipated 10% growth in the next three years.

The aims of this project are to design a network to support the current and future. The network is designed for the future with cutting-edge technology which is the technology equipped with high-level information technology developments. The network design is planned for the next 20 years and solves all the current issues in the school of computing. Since technology is changing from time to time, network structure is required to support the future needs. The security of the network is also one of the important criteria that should be considered in this project. A good network system is required to provide campus network protection from network breaches and helps in reducing data loss as well as reduce network theft and sabotage. The network project is aimed to be flexible to enable a secure VPN from a remote location. The goal of this network design of the building is a network that can be achieved in reliability, performance, security, and manageability as well as scalability. In the term of reliability, the network is designed with minimum errors, security attacks, and equipment failures. Scalable network design can support new users, connections, or systems without influencing the service that is provided to the existing users.

The objectives of this project are to design a network plan that is reliable, efficient, easy to use, and secure network to fulfill the network requirement in the campus. It should be designed with all the precautions to make sure that it is easy to manage and improve the current performance. Designing a good network for the school of computing can help the growth of the campus to support the demands in the internet speed, connections, and the increase in data transfers.

2.0 PROJECT BACKGROUND AND OVERVIEW

Network communication and network planning in building is important for the use of the network of people nowadays. Mostly for each building, there should be a network planner to plan for the network for the building. For this project, we get the knowledge from the internet and lecturer planning to build a small network for the school of computing. We do for the building School of Computing which has around 1000 students including both undergraduate and postgraduate students, 50 academic and 20 supporting staff. The floor plan that we try to do is for a 2–storey building that has 4 labs, 2 video conferencing rooms, 1 server room, 2 offices, 1 technical room and other basic facilities. For the labs, there are general purpose lab, computer security lab, network lab and IOT lab which has a total 30 workstations and one multi-terabyte storage server is planned for each lab.

There are some problems about the network of this building that we need to find a solution to. First, the analysis of requirements from the needs of the customer and user of this building is the first aspect that we need to find out. The customer and user needs are important for us to start the project so we need to do the questionnaires for this part. Then, the budget given is around RM1,800,000.00 so we have to plan to use the budget wisely in equipment and cable based on the questionnaires and research of network devices availability, usability, cost and services. Besides, we also have to plan and design a network infrastructure by identifying the work area and cable types and length for current and future needs so that the network and data of this building is able to maintain high performance in the next 20 years. Moreover, the assigning of network IP addressing is also one of the main aspects of this project because IP address subnetting ensures that traffic destined for a device within a subnet stays in that subnet, which reduces congestion. Therefore, we need to plan a small network that has high performance internet speed and devices, the reliable cost needed for future use and the effective distribution of network and IP addresses.

3.0 FLOOR PLAN

3.1 First Floor

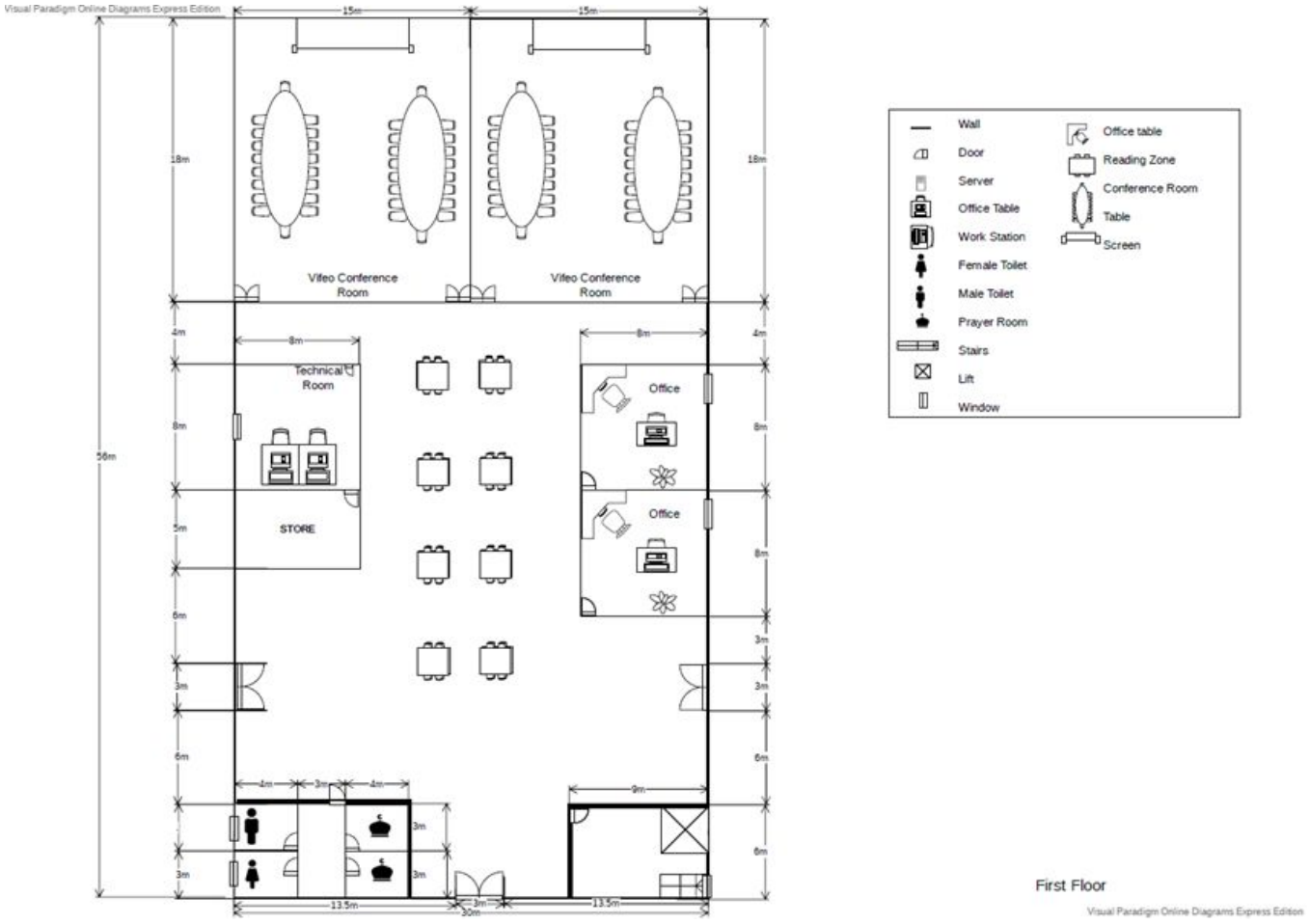

Figure 3.1 First Floor Floor Plan

3.2 Second Floor

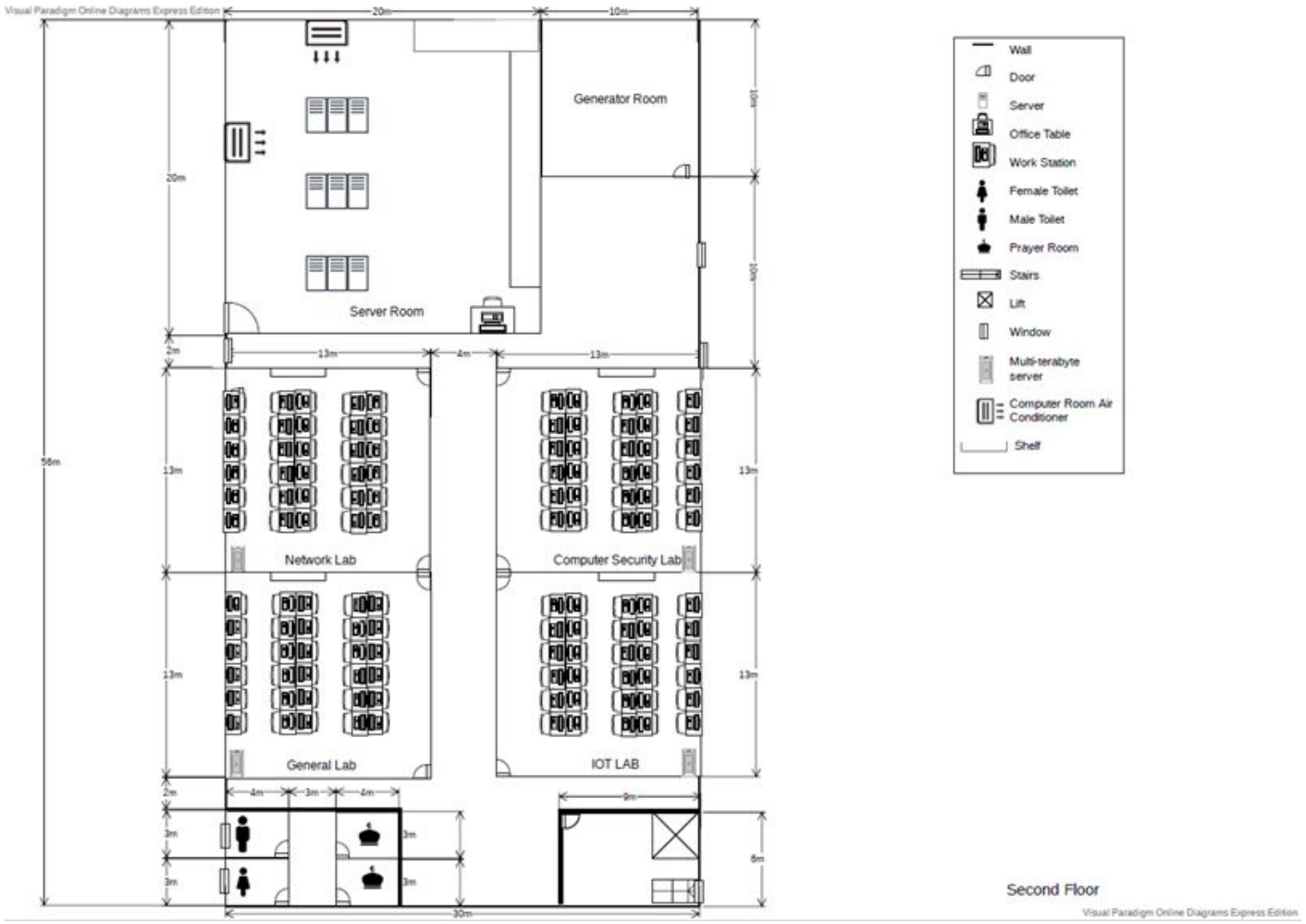

Figure 3.2: Second Floor Floor Plan

4.0 PRELIMINARY ANALYSIS

4.1 Question List

1. What is the actual goal of this network design of this building?

The network design of this building should be achieved in reliability, performance, security and manageability, as well as scalability.

- Reliability - In the term of reliability, the network is designed with minimum errors, security attack, equipment failures and so on.

- Performance - The network design is required to meet the requirement of the user with the assumption about the response time, capacity, delay, and so on. The network of this building is required to be equipped with a high-speed internet connection.

- Security and Manageability - The manageability is including fault management, security management, performance management, security management and so on. A simple and effective network that enables the network staff to manage and support the network effectiveness and efficiencies so can provide a simpler troubleshooting process.

- Scalability - Scalable network design enables to support new users, connections, or systems without influencing the service that is provided to the existing users. A scalable network is also controlled by the controlling cost. In this proposal, the network is designed to support the growth in student and academic staff as well as the new 4IR education system.

2. What are the software problems that lead to network defects?

There are several software problems that might defect the network we built, such as errors in configuration, protocol issues, security flaws, and so on.

- Error in Configuration - Initially when we set up the system, the workload of our system needs to be handled little. However, when the demand for resources increases, the system will definitely handle more and more workload. So we need to adjust the configuration according to the existing demands. Wrong configuration will make the network

connectivity unable to handle the data properly cause the data transmission will become very slow.

- Protocol Issue - TCP/IP based protocols sometimes might have bugs that will stop or slow down the delivery of the packets. Packet collisions might cause the data packets being transported via Internet Protocol not able to reach their destinations. Frequent collisions affect data transfer from one host to another.

- Security Flaws - Failure to build up the security features for the system might give a hacker the chance to invade your system. Malware is able to change the registry settings and the system will be open to attacks and hacking.

3. Which type of LAN topology do you want to implement in your network?

There are three primary LAN topologies: linear bus, ring, and star. Another network topology is hierarchical in nature, which may incorporate elements of the bus, ring, and star. The appropriate physical and logical topology for a LAN is determined by reliability and cost objectives as well as by the connectivity requirements of users.

- In bus topology there is a main cable and all the devices are connected to this main cable through drop lines. There is a device called tap that connects the drop line to the main cable. Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

- In ring topology each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it. This structure forms a ring thus it is known as ring topology. If a device wants to send data to another device then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for other devices then repeater forwards this data until the intended device receives it.

- In star topology each device in the network is connected to a central device called hub. Unlike Mesh topology, star topology doesn’t allow direct communication between devices, a device must have to communicate through a hub. If one device wants to send data

to other devices, it has to first send the data to the hub and then the hub transmits that data to the designated device. The centralized nature of a star network provides ease while also achieving isolation of each device in the network.

A star topology is best suited for smaller networks and works efficiently when there is a limited number of nodes. One of the advantages of the star network topology is that if there is a failure in cable, then it only causes one computer to get affected and not the entire network.

4. Which network device is needed to implement the network plan?

There are several network devices and each of them has different functions. Here is the introduction and function for the network devices:

- Network Hub

It used to communicate with various network hosts and also for data transferring. It works on the Layer 1 (physical) of the OSI model.The transferring of data in a computer network can be done in the form of packets. A network hub cannot filter the data and does not have intelligence to identify the data path. It leads to inefficiencies and wastage. A network hub cannot be so safe and secure to be used. In addition, copying the data packets on all the ports will make the hub slower. The network hub shares its bandwidth with every port. It leads to the utilization of the network switch. So, it is not recommended to be used.

- Switch

Switch is used to handle the data and know the specific addresses to send the message. It works on layer 2(data link) or sometimes layer 3(network) of the OSI model. It can support any type of packet protocol and can be used for filtering and forwarding the data. So this is the more clever technique to deal with the data packets. Once receiving a data packet from the interfaces in the switch, it performs error checking(check for collision and other network errors) before forwarding data and makes sure that there are no errors in the forward packet as well as forward the selective packet to the correct port. A switch to maintain a content addressable memory table of all the devices connected to it to maintain system configuration as well as memory.

- Router

Router is a network device that is used for routing traffic from one network to another. It works on layer 3(network) of the OSI model. It directs data into a network in the form of a packet. Router connects at least two networks together(two LANs or WANs or a LAN and its ISP network). It is also known as a repeater as it strengthens the signals before transmitting them. Router uses protocols to communicate with each other to calculate and configure the best route for sending data. It is a more intelligent device compared to the switch and hub as it serves as an intermediate destination to connect multiple network areas together.

- Gateway

A gateway is a passage to connect two networks together that may work upon different network models. Gateway performs at the session and transport layers in the OSI model. Gateways offer conversion between networking technologies like OSI (Open System Interconnection) & TCP/IP. Because of this, these are connected to two or many autonomous networks, where each network has its own domain name service, routing algorithm, topology, protocols, and procedures of network administration & policies.

- Modem

Modem is a network device that enables computers to send or receive data over the cable lines. It connects a computer or router to a broadband network. It modulates as well as demodulates the signal among the computer and a telephone line because the computer generates digital data whereas the telephone line generates an analog signal.

- Wireless access point (WAP)

WAP is a network device that allows other wireless capable devices to connect to a wired network through a wireless standard(Wi-Fi and Bluetooth). WAP is also known as a hotspot. It provides connectivity in campus environments and allows the users to work anywhere in the campus and remain connected to the network. It supports in larger areas compared to wireless routers. In addition, cards, adapters and servers are also recommended to use in this network plan.

5. What are the considerations for the cable installation?

In the network plan, the cabling installation must meet the needs of today's demand and prepare for the future;s problems and challenges. Cable installation is the important criteria to achieve high speed internet connection. From the research, we found out there are some points we are required to take note in the cable installation:

- Choosing a right cabling type

The types of the cables used can affect the network efficiency. Cable is the guided media in the network. The examples of the cable are twisted-pair cable, coaxial cable and fiber optics. The twisted-pair copper wire is the least expensive and most commonly used. The cable consists of the two insulated copper wires which are twisted together to reduce electrical interference from similar pairs close by. The examples of the twisted-pair copper wire are UTP and STD. UTP can be divided into Cat 1, Cat 2, Cat 3, Cat 4, Cat 5, Cat 5e and Cat 6 with different usage and data rate from 1 Mbps to 1000MBps. The lifecycle of the copper cable is 5 years. The coaxial cable is commonly used in TV systems. It consists of two concentric copper conductors to achieve high data transmission rates. The fiber optics cable consists of glass fiber that carries light pulses. It has high-speed operation and low error rate. The life cycle of the fiber optics is 30 to 50 years. It provides a better security compared to copper cable as the optical fiber does not transmit electricity and the broken optical fiber can be detected faster by using a number of monitoring techniques.

- Avoid mounting the cabling components in places that block accessibility to other equipment (such as a power strip or fans) in and out of the racks

- Avoid the following actions that can stress the cable:

– Applying extra twists.

– Pulling or stretching beyond the specified pulling load rate.

– Bending it beyond the specified bend radius, and not beyond 90º.

– Creating tension in the suspension runs.

– Stapling or applying pressure with the cable ties

By comparing different types of cable, fiber optics eliminate the traditional copper cables and achieve high speed in the network. Although fiber optics has higher cost compared to the copper cable but the price between fiber and copper has narrowed. It is better in performance and maintenance.

6. What are the functions of the server room, generator room and technical room in your building?

- Server Room

A server room is a room used to store computer servers and power them to let them operate. These servers mainly function to store all the company-related data so it is not opened for most of the employees except relevant personnel. It is devoted to storing data storage servers and computer networking devices. Depending on the size of the room and a business's needs, it may hold anywhere from ten to several hundred servers

- Generator Room

The generator room is to make sure the power supply to the server room is uninterrupted, so all the computer servers can work continuously in emergency situations. If there is a blackout, a generator room can function to provide an emergency electric supply to keep the server in the Server Room ongoing for the user to access the server as frequently as possible.

- Technical Room

The technical room is an essential part of the building, and must be dimensioned to distribute and protect the building's electrical infrastructure.

7. What is the minimum requirement of the accessibility of the internet connection?

The network design of the building is required to support the accessibility with growth in both students and academic staff in 20 years. The lab should be equipped with a high-speed internet connection for 4IR education. In order to achieve the better accessibility of the

internet connection, some network installations such as proxy servers are required to achieve high performance in the network.

8. What is the minimum requirement of the physical protection measures and the safety measures that should be implemented in this building?

Since the network is required to support thousands of users, the physical protection for the network in this building is essentially important to make sure the performance and the efficiency of the education. Physical protection is required to protect confidential information and secure the network away from unauthorized entry. There are some physical protection measures that should take note of:

- Installation of the closed-circuit television(CCTV) - The installation of the CCTV can be used to monitor the interior and the exterior of the building. It can record and monitor activities as well as keep track of what is happening in the building.

- The location of the secure room - The server room should be located in an area that is protected from fires and floods. It also should be away from the crowded area to ensure the network is protected.

- Installation of the locking system - The installation of the locking system can control access to the facility. Examples of the locking systems are password locking system, biometrics locking system(fingerprint or iris scanning), and RFID. The locking system can secure the rooms that store with high confidential and sensitive data such as the server room, storeroom, and technical room. It can keep the intruders away from the places.

9. What are the different ways of securing a computer network?

There are several ways to do this:

- Install firewalls in every computer and network. It will help to block unauthorized access to computers and networks. Firewalls are becoming more and more sophisticated with

hackers that always keep updating to the latest integrated network security methods and encryptions to prevent breaches.

- Always required employees to change their computer password every 3 months.

- Always keep the anti-virus software updated to the latest version as hackers will always have a new way to attack your computer and network.

- Train the employees. Teach the employees how to identify suspicious emails so they won't click on a malicious link that might lead to an attack on the company network.

10. How can you manage a network using a router?

Routers have a built-in console that lets you configure different settings, like security and data logging. You can assign restrictions to computers, such as what resources it is allowed access or what particular time of the day, they can browse the Internet. You can even put restrictions on what websites are not viewable across the entire network.

11. What is the requirement to design a network plan for up to 20 years?

Both software and hardware installation is needed to plan for the future. The construction of the building is needed to plan for the existing and the future problems to avoid unnecessary expenses.

The network maintenance is very important to maintain the network availability.The effective maintenance plan will provide a reliable network for the university. The network should be protected from the unexpected downtime. To maintain the network for up to 20 years, the detected issue or network problem should be solved as early as possible. Beside the installation of the firewalls and antivirus which have been discussed in the previous question, here are some of the maintenance strategies to maintain the network availability for up to 20 years :

- Software Update Capability

Every network device should always have an owner that will keep updating the device to meet the latest requirement. Even for the basic devices, there will be flaws in the software, so it is better to have someone to fix it and allow users to use it safely.

- Contact Information and Support Forum

There should be a way of contact to report any problems with the devices. The most transparent and preferable is a support forum, where users' reports of questions or problems can be reported in a publically accessible and searchable location, and responses from the manufacturer are provided. So that, the technician should be equipped with the knowledge of maintaining and supporting the software and hardware.

- Redundancy and Backing Up

Redundancy means that it should have backing up devices in the network. A suggestion from us is that it should have a minimum of 2 servers so that one will take over if the other fails or requires maintenance. A good rule of thumb is to have redundant components and services in place for any part of a network for ensuring that downtime is kept to a minimum.

Moreover, the portable devices should be maintained in good condition to avoid unnecessary expenses. The facility security is an important concern to the network. The portable devices such as the server and the workstation should be located in the locked room. This can make sure the vulnerable devices keep away from the intruders. The users should be equipped with the knowledge of the proper way to use the hardware to prevent the hardware failure.

4.2 Feasibility of the Project

The feasibility of the project has been determined and we have made the conclusion after we discuss and do the research about the requirements and other information that is necessary to develop a network plan of this building.

The network design of this building should be achieved in reliability, performance, security and manageability, as well as scalability. The LAN topology to be implemented in the network that is suitable for this building is Star Topology because Star Topology is best suited for smaller networks and works efficiently when there is a limited number of nodes. The network devices that are used in our building are router, wireless router, switch and WAP. In addition, cards, adapters and servers are also recommended to use in this network plan.

There are some physical protection measures that are required to protect confidential information and secure the network away from unauthorized entry in this building such as installation of the closed-circuit television(CCTV), installation of the locking system and the location of the secure room. The security of the computer network of this building can be maintained by installing firewalls in every computer and network and always keeping the anti-virus software updated to the latest version. It will help to block unauthorized access to computers and networks as hackers will always have a new way to attack your computer and network.

The network design of the building is required to support accessibility with growth in both students and academic staff in 20 years so the lab should be equipped with a high-speed internet connection for 4IR education.

5.0 CHOOSING THE APPROPRIATE LAN DEVICES

5.1 List of devices and the quantity needed

Product	Feature	Price	Quantity	Total
BUFFALO TeraStation 3410DN Desktop 8TB NAS (Multi-terabyte storage server)  *Figure 5.1: BUFFALO TeraStation 3410DN Desktop 8TB NAS*	• Protect Your Data • Easy to set up with SmartPhone or Tablet • Compatible with Amazon S3, Dropbox, Dropbox Business, Microsoft Azure and OneDrive • Remote Management System: save time & resources by managing multiple devices from a single console • 8 TB – 4 drives included - ships in RAID 5 = 6 TB usable capacity • Integrated Hybrid Cloud Backup / Private Cloud / iSCSI Support	2165.45	4	8661.8

WD My Cloud EX4100 24TB (server)  *Figure 5.2: WD My Cloud EX4100 24TB*	· Faster Speed, Better Streaming · Access From Anywhere · Robust Data Protection · Powered By My Cloud OS 3 · Centralize, Organize And Beautifully Stream With Plex · Compatibility may vary depending on the user's hardware configuration and operating system.	7998	9	71982
APC Smart-UPS SRT 3000VA 230V SRT3000XLI(Generator) 	● Avoids costly power problems by keeping your IT equipment and data protected and available. ● Low operating and maintenance costs with proven reliability and intelligent battery management. ● Save time with easy and convenient remote accessibility. ● Provides pure sine wave output which is recommended by server manufacturers using active power factor corrected (PFC) power supplies. ● Protects connected loads from surges, spikes, lightning, and other power disturbances.	6799	3	20397

Figure 5.3: APC Smart-UPS SRT	• Increases availability by allowing a trained user to perform upgrades and replacements of the batteries reducing Mean Time to Repair (MTTR). • Rack/tower convertible protects the initial investment in the UPS when migrating from tower to rack-mount environment.			
Cisco ASR1001-X  *Figure 5.4:Cisco ASR1001-X*	• Quad-core 2.13GHz processor with 4GB memory • 8GB flash memory • 1 SPA bay • SPA interface processor 10 (SIP10)	27953.14	2	55906.28
ASUS RT-AX88U WiFi 6 Router (Router)  *Figure 5.5: ASUS RT-AX88U WiFi 6 Router*	· 4*4 dual-band WiFi router that provides 160MHz bandwidth and 1024-QAM for dramatically faster wireless connections · Next-Gen WiFi 6 Standard - 802.11ax WiFi standard for better efficiency and throughput. · Ultrafast WiFi Speed - 6000Mbps WiFi speed to handle even the busiest network with ease.	1355	6	8130

	· Wider Usage and More Convenience - 4 antennas + 8 LAN ports to support more clients at the same time. · Commercial-grade Security - AiProtection Pro, powered by Trend Micro™, blocks internet security threats for all your connected smart devices.			
Cisco SG350X-48P Stackable Managed Switch With 48 Gigabit Ethernet (GbE) Ports (48 Port Switch)  *Figure 5.6:Cisco SG350X-48P Stackable Managed Switch*	● ETHERNET PORT CONFIGURATION: 48-port 10/100/1000, 4 x 10G uplinks (SFP+) ● POWER OVER ETHERNET: 48 PoE ports with 382W total power budget, PoE, PoE+, 60W PoE ● L2+/L3 FEATURES: Static routing, QoS, voice/guest VLAN, MSTP, IGMP snooping, time-based access control lists, 802.1x, Web-based Authentication, IPv6 First Hop-Security, IP Source Guard ● PEACE OF MIND: Limited lifetime warranty, next-business-day replacement, one year of technical support,	4961	4	19844

	and free software fixes for the term of the warranty			
NETGEAR 8-Port 10G Ethernet Smart Managed Plus Switch (XS708E) (8 Port Switch)  *Figure 5.7: NETGEAR 8-Port 10G Ethernet Smart Managed Plus Switch*	• VERSATILE MOUNTING OPTIONS • WHISPER-QUIET DESIGN PROSAFE LIFETIME PROTECTION ENERGY EFFICIENT • BUILT TO LAST: Every NETGEAR:Network switch is rigorously tested for reliability, quality, and performance	2226.66	10	22266.60
UBNT Ubiquiti Networks UAP AC EDU Ceiling Mount Access Point (WirelessAccess Point)  *Figure 5.8: UBNT Ubiquiti Networks UAP AC EDU Ceiling Mount Access Point*	• Range of 183 meter • Wireless 802.11ac • Making for campus wide deployment. • Dual-band, 3x3 MIMO technology and convenient 802.3at PoE+ compatibility. • Mobile Announcement AppBroadcast announcements with clarity from your iOS or Android-based device using our mobile app.	1980	20	39600

Monoprice Cat 6 48 Port Patch Panel (Patch Panel)  *Figure 5.9: Monoprice Cat 6 48 Port Patch Panel*	• 1U (1.75") tall • Horizontal 180° punch down • Dustproof covers • Black painted steel panel • Color coded wiring diagram on back • UL listed • 568A/B compatible • For 19" wide racks • Includes wire support bar for cable management	214.69	4	858.76
Cat6a Shielded and Foiled (SFTP) Solid PVC CMR Blue Bulk Ethernet Cable(305m)  *Figure 5.10: Cat 6A Cable*	• Support bandwidth up to 500MHz • Provide maximum network speed at 10Gbps • Double aluminum foil shielding to protect cable from external electro-magnetic interference. • Pure copper enhances durability and stability.	1000	5	5000

Cat6a RJ45 Connector (10pcs)  *Figure 5.11: Cat 6A RJ45 Connector*	• CAT6A RJ45 Plug shielded 8P8C Network Connector • High quality terminal • Not easy to oxidize with high performance • 400um phosphor bronze for stable and high transmission.	11	10	110
LC APC to LC APC Single Mode Fiber Optic Patch Cable (30m)  *Figure 5.12: Fiber Optic Cable*	• Ideal for connecting 1G/10G/40G/100G ethernet connections. • Transport data for up to 10km at 1310nm, or up to 40km at 1550nm. • E2000, LSH connector with a dust-proof cover. • Smart & Reliable - Bendable Optical Fiber	43.21	26	1128.46
TOTAL AMOUNT				253879.90

Budget Given : RM1,800,000.00

Estimated Price Needed for LAN Device in this Project : RM253,879.90

Balance = RM 1,800,000.00 - RM 253,879.90

= RM 1,546,120.10

5.2 Reflection

Are you surprised by the prices? How were you surprised?

Based on the list of prices of all the devices that we choose for our network cabling , we are quite surprised as some device prices are expensive that were not in our expectations before. Fortunately, we managed to find comfortable but high quality devices from several websites. Hence, it makes us save up more to 1M which we only used up RM253,879.90.

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

Yes, we have considered cost as a factor for choosing networking devices. It is because if we do not consider cost as a factor, we will over budget and do not have extra money in other equipment and installation. Therefore, we choose some network devices which are at a discount. We manage our budget and only choose the suitable network devices based on our research on requirement. We choose the proper hardware linking the cables, proper communication devices between the buildings, proper servers and minimizing the distance to reduce the cost. In the process of choosing networking devices, we have compared the devices that offer the same function with different brands. It will help us in choosing the right networking devices with reasonable prices. If we choose the network devices with high prices, we also need to pay a high cost in maintaining the devices in the future.

What are the major differences between the same devices from different brands? For example Cisco and Huawei Routers.

The same devices from different brands vary in their prices. The different brands offer different features in security, speed, efficiency and more. Some devices may offer better security features which results in higher prices compared to other brands that have the same function. For example, the differences between Cisco and Huawei Router is their support. Cisco ISR1100 Series supports both a built-in Wifi Access Point and Wireless LAN Controller. Besides LAN and WAN interface, it also supports WiFi IEEE802.11ac standard via a built-in,dual-radio 2x2 MIMO integrated AP. It also can act as a WLAN controller for

other external APs, handling up to 50APs. The 1111-8P ISR consistently delivered the highest average IPsec encrypted WAN throughput, at 365 Mbps. Huawei routers that can support either as a Wireless LAN Controller or a WiFi AP, but not both.Huawei routers delivered 84 to 245 Mbps. Huawei AR1220E delivered throughput varying by more than 100 percent.It can handle the APs up to 12(recommended) and 32(maximum). It can allow online users to use this series of AR routers up to 200 numbers of online users. The best devices do not depend on its brand as the same devices from different brands may offer different features that suit different users .

6.0 MAKING CONNECTIONS - LAN AND WAN

6.1 Work Areas On The Floor Plan

6.1.1 Identify Work Area

First Floor

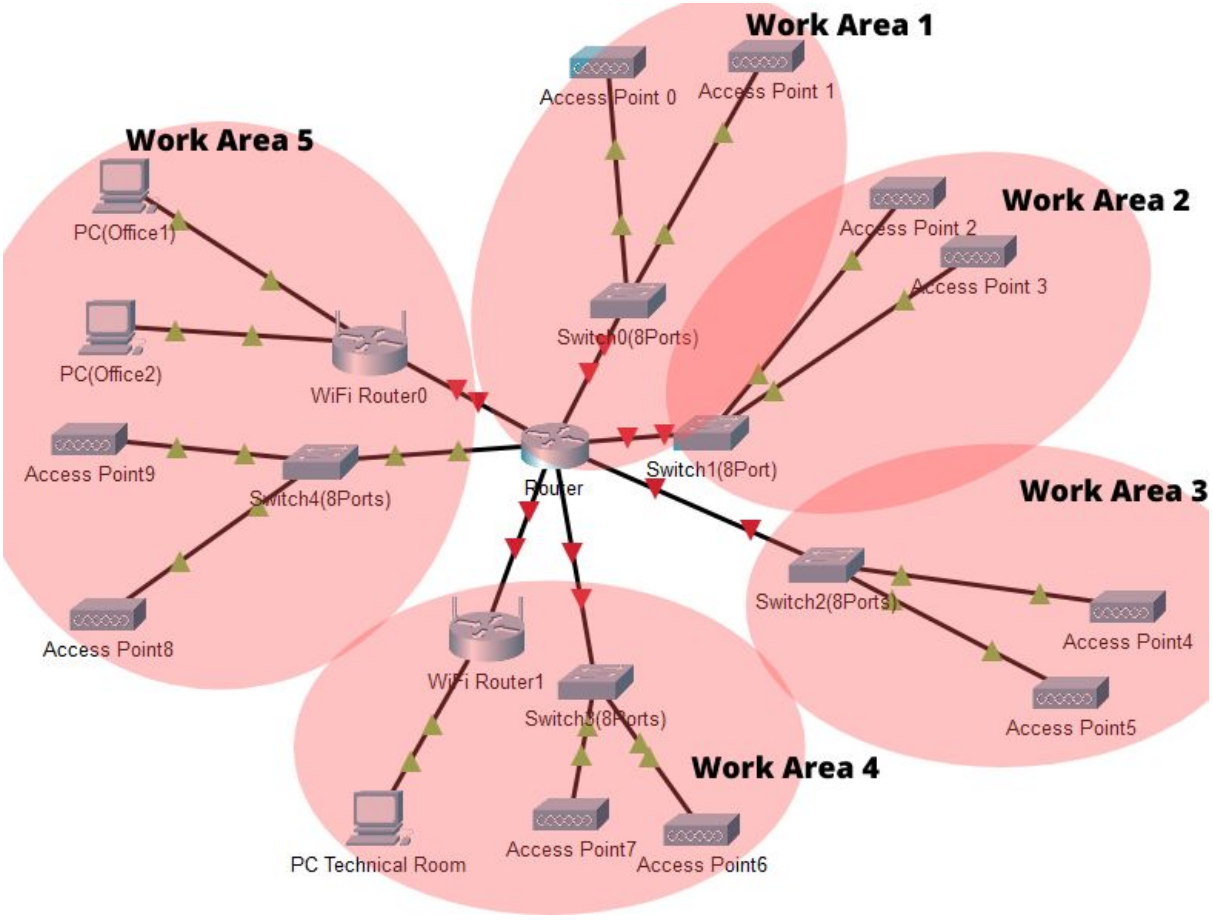

Figure 6.1: First Floor Work Area

Work Area 1: This area located at the north-west of the first floor which has the Video Conferencing Room 1 so the router connects to the switch 0 (8 port) then the switch connected to the access point 0 and access point 1 which is shared by the Video Conferencing Room 1.

Work Area 2: The north-east area of the first floor is having the Video Conferencing Room 2 and the router will connect to the switch 1 (8 port) then connected to the access point 2 and access point 3 which is shared by the Video Conferencing Room 2.

Work Area 3: This area is for the lobby area in the south area of the first floor which the router connects to the switch 2 (8 port) then connected to the access point 4 and access point 5 which is shared by the lobby area, toilet area and the area near the main entrance.

Work Area 4: The south area of the first floor is having the technical room and the router will connect to the Wifi Router 1 and the Switch 3(8 ports). The Wifi router 1 will then connect to the PC technical room while the switch 3(8 ports) will then connect to the access point 6 and access point 7 which is shared by the technical room.

Work Area 5: The west area of the first floor is having the two office rooms. The router is connected to the Wifi Router 0 and Switch 4(8 ports).The Wifi router 0 is then connected to the 2 pc computer which is in office 1 and office 2 respectively. The switch 4(8 ports) is then connected to the access point 8 and access point 9 which is shared by the two office rooms.

Second Floor

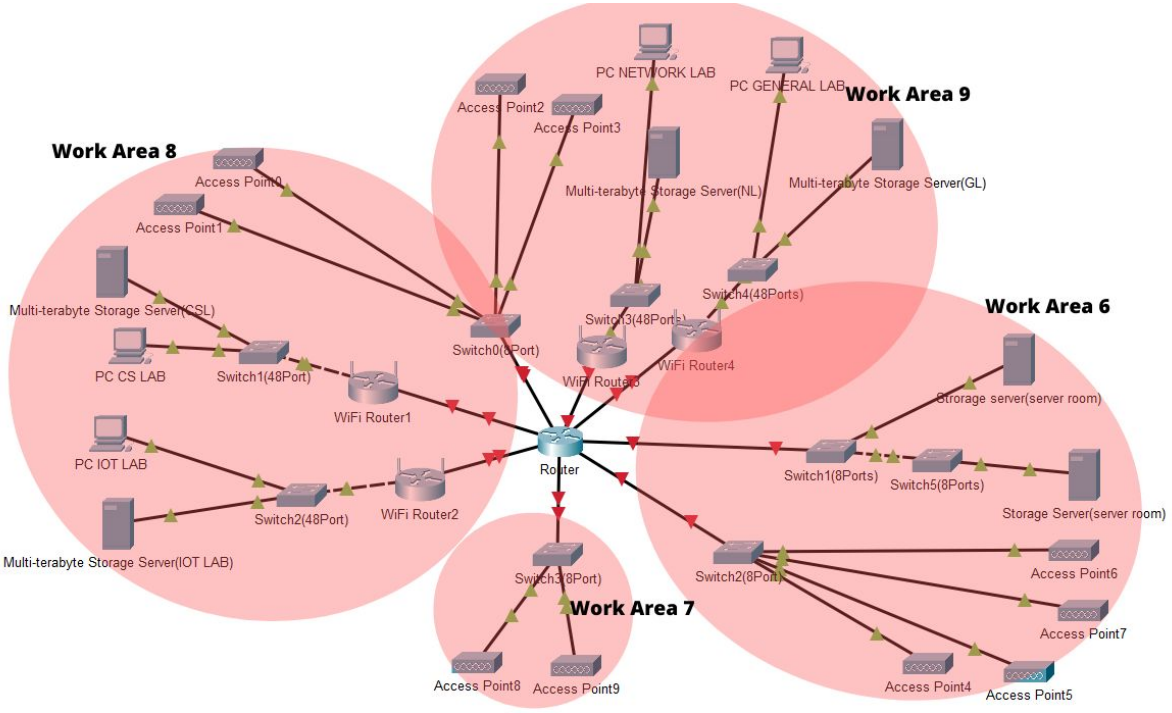

Figure 6.2: Second Floor Work Area

Work Area 6: The north area of the second floor is having the Server Room and the Generator Room. The router will connect to switch 1 (8 port) and switch 5 (8 port) which is connected to the storage servers of the Server Room. Another switch 2 (8 port) is connected to the four access points which the access point 4 and access point 5 is shared by Generator Room while access point 6 and access point 7 is shared by Server Room.

Work Area 7: The south area of the second floor has switch 3 (8 port) connected by the router and then connects to access point 8 and access point 9 which is shared by the lobby area, escalator and stairs area, and toilet area.

Work Area 8: The east area of the second floor is having the computer security lab (CS lab) and the IoT lab. The main router is connected to switch 0, two wifi routers (router 1 and router 2) in work area 8. Switch 1 (8 ports) in work area 8 is shared with work area 9 and connected to access point 0 and the access point 1 to provide wireless access in the east area of the second floor. The two wifi routers, router 1 and router 2 are connected to the 48 port

switch 1 and 48 port switch 2 in CS lab and IoT lab responding. The switch in each lab is connected to the workstation and multi-terabyte storage server.

Work Area 9: The west area of the second floor is having the network lab and the general lab. The main router is connected to switch 0, two wifi routers (router 3 and router 4) in work area 9. Switch 1 (8 ports) in work area 9 is shared with work area 8 and connected to access point 2 and access point 3 to provide wireless access in the west area of the second floor. The two wifi routers, router 3 and router 4 are connected to the 48 port switch 3 and 48 port switch 4 in the network lab and the general lab responding. The switch in each lab is connected to the workstation and multi-terabyte storage server.

6.1.2 Connection, Patch Cord and Switch

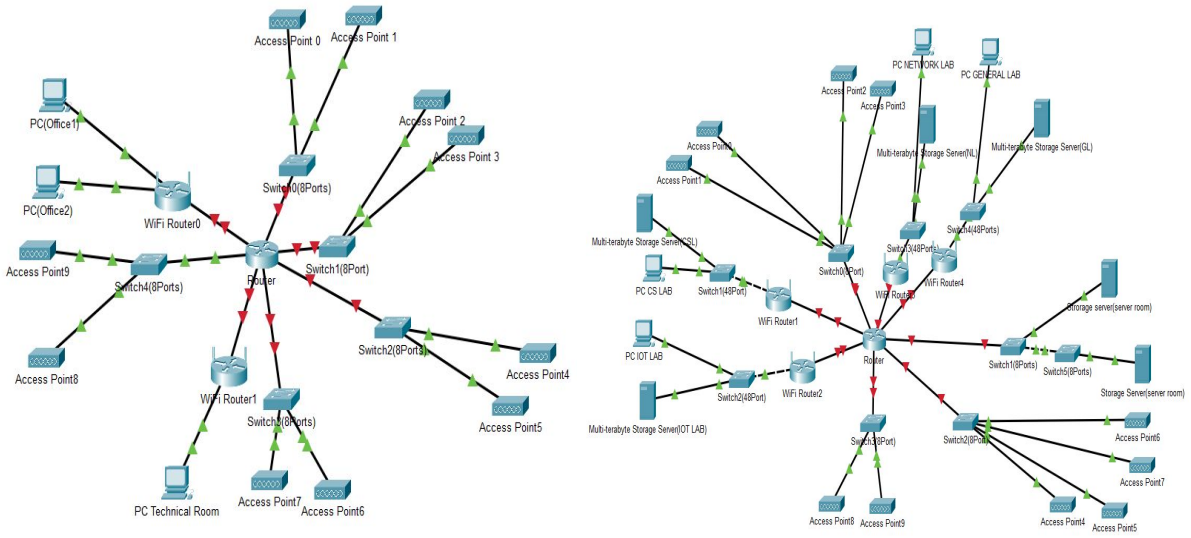

Figure 6.3: Connection of the N28B

Based on the network diagram, star topology is used in the connection. There are a total of 15 connections in this project which are 7 connections in the first floor and 8 connections in the second floor.

On the first floor, the main router is connected to 5 switches(8 ports) and 2 wifi routers. The connection between the main router and the 8 ports switches is using fiber optics cable while the connection between the wifi router is using CAT 6A cable. The 8 ports switches are connected to a wireless access point(WAP) by using fiber optics cable. The two wifi routers are placed in the technical room and the office.

On the second floor, the main router is connected to 4 switches(8 ports) and 4 wifi routers. In each lab, the wifi router is connected to the main router by using the CAT 6A cable. The wifi router is then connected to the 48-ports switch which is connected to the PCs and multi-terabyte storage server. The connection in the lab is using the CAT 6A cable. The 48-port patch panel is used in each lab for the cable arrangement. The main router is connected to an 8 port switch and the switch is then connected to another 8-port switch for the connection of the storage server in the server room by using CAT 6A cable. The main router is connected to 3 8-port switches by using fiber optics which is then connected to the

wireless access point(WAP). The connection between the switch and the WAP is also used by fiber optics cable.

6.2 PC & Network Devices Arrangement

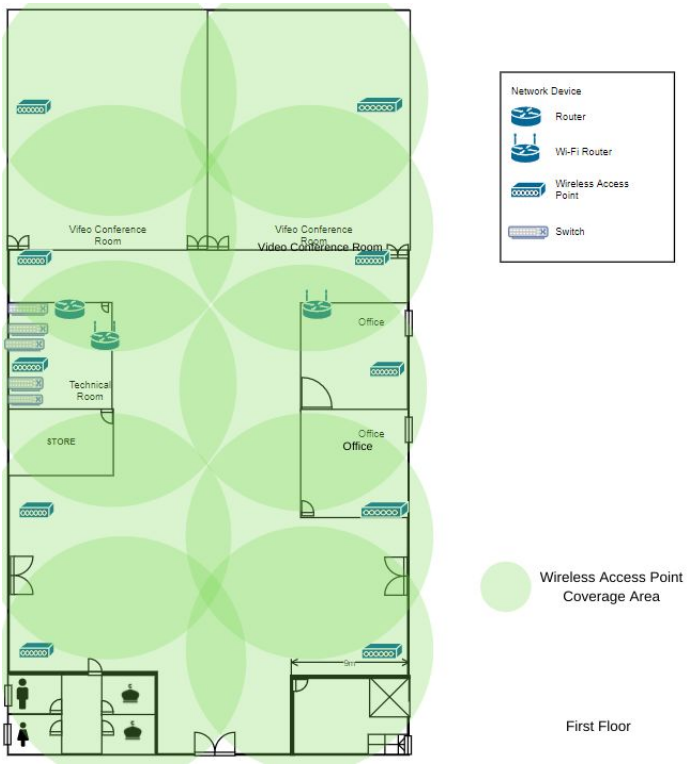

Figure 6.4: Network Devices Arrangement & WAP Coverage Area (First Floor)

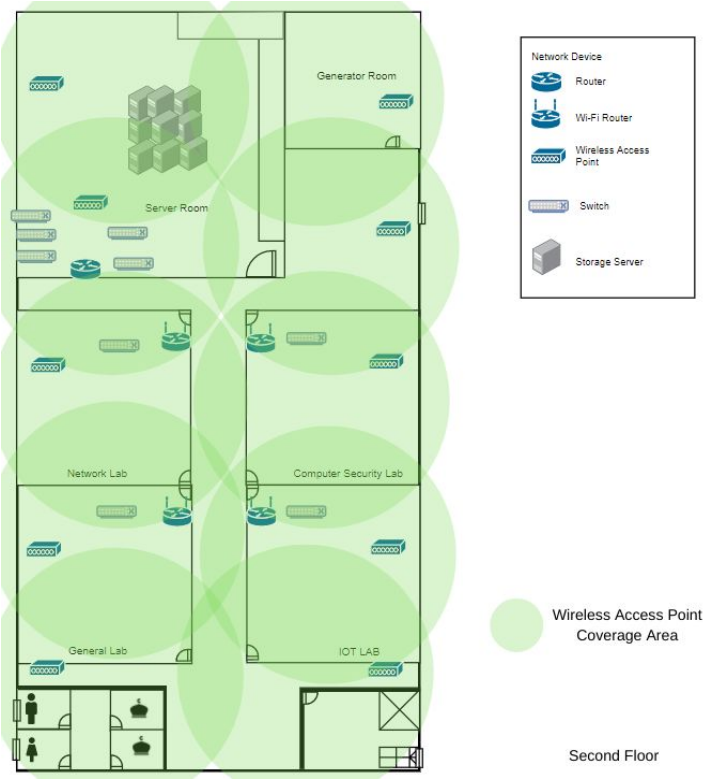

Figure 6.5: Network Devices Arrangement & WAP Coverage Area (Second Floor)

6.2.1 The Cable Types and Length

Horizontal Cabling

There are two types of cable used to connect the router and other network communication devices which are fiber optics cable and cat 6A cable. The fiber optics are used to connect between the main router, switch, and the wireless access point while the cat 6A is used to connect the main router with wifi routers in the office, lab and telecommunication room.

First Floor：

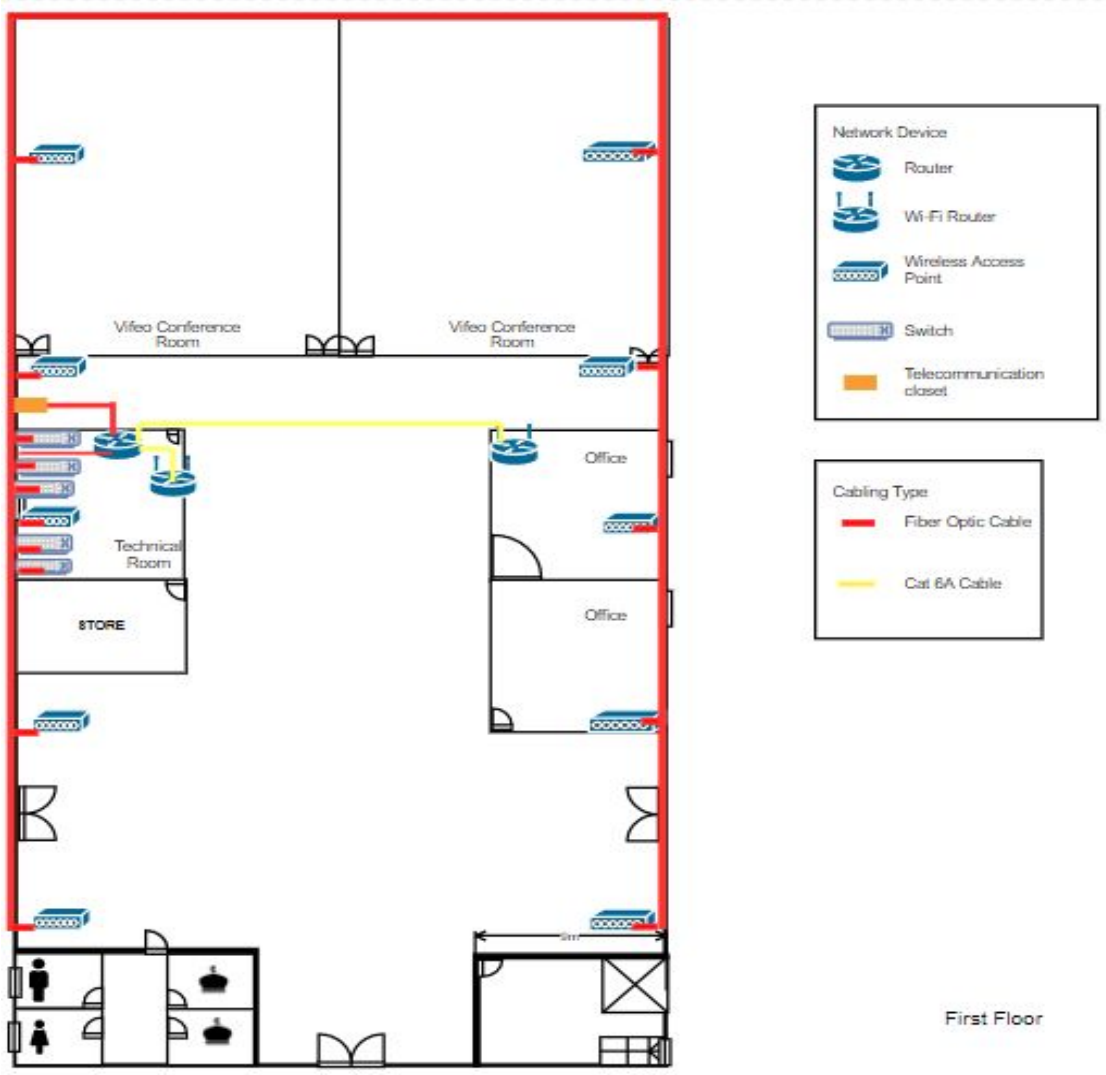

Figure 6.6: First Floor Horizontal Cabling Installation

Main Cable Length(First Floor)

Main router,Switch and Wireless Access Point(WAP), **Fiber Optics Cable**

1. Switch 0 to WAP 0 and WAP 1: Switch0 to WAP0 + Switch0 to WAP1
   = 12 + 4 = 16m
2. Switch 1 to WAP 2 and WAP 3: Switch1 to WAP2 + Switch1 to WAP4
   = 61 + 9 = 70m
3. Switch 2 to WAP 4 and WAP 5: Switch2 to WAP4 + Switch2 to WAP5
   = 17 + 61 = 78m
4. Switch 3 to WAP 6 and WAP 7: Switch3 to WAP6 + Switch3 to WAP7
   = 1 + 8 = 9m
5. Switch 4 to WAP 8 and WAP 9: Switch2 to WAP8 + Switch2 to WAP9
   = 70 + 79 = 149m

Total Fiber Optics Cable for second floor: 322m

Main router and Wi-Fi router, **CAT 6A cable**

1. Main router to Wi-Fi router 0: 2m
2. Main router to Wi-Fi router 1: 15m

Total CAT 6A cable for first floor:17m

Second Floor :

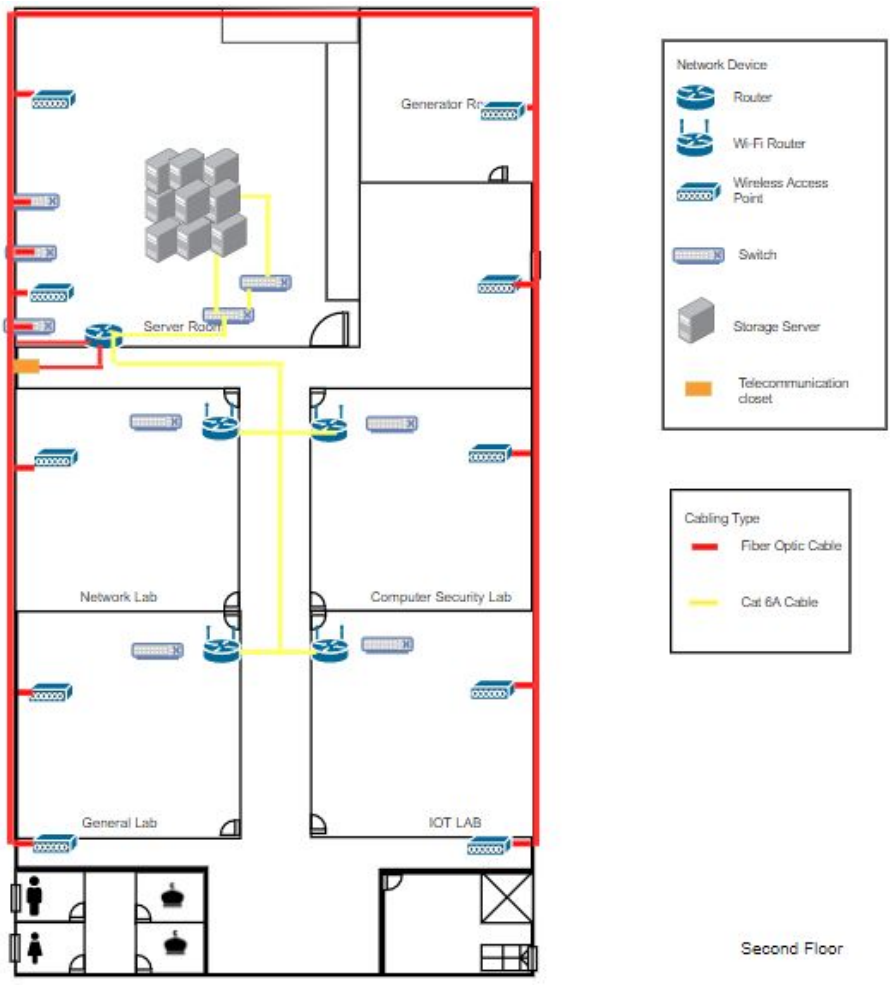

Figure 6.7: Second Floor Horizontal Cabling Installation

Main Cable Length(Second Floor)

Main router,Switch and Wireless Access Point(WAP), **Fiber Optics Cable**

1.Switch 0 to WAP0, WAP1, WAP2 and WAP3:

Switch0 to WAP0 + Switch0 to WAP1 + Switch0 to WAP2 + Switch0 to WAP3

= 1 + 9 + 56 + 65 = 131m

2. Switch 2 to WAP4, WAP5, WAP6 and WAP7:

Switch2 to WAP4 + Switch2 to WAP5 + Switch2 to WAP6 + Switch2 to WAP7

= 9 + 18 + 77 + 86 = 190m

3. Switch 3 to WAP8 and WAP9:

Switch3 to WAP8 + Switch3 to WAP9

= 27 + 95 = 122m

Total Fiber Optics Cable: 443m

Main router and Wi-Fi router, **CAT 6A cable**

1.Connection of CAT 6A cable in server room:

Main router to switch 1+Main router to switch 5+9*(Switch to server)

= 3 + 1 + (9*2) = 21m

2.Connection of Main router to 4 Labs

a. Network Lab : 18m

b. General Lab : 35m

c. CS Lab :18m

d. IoT Lab : 35m

3. Connection in the labs

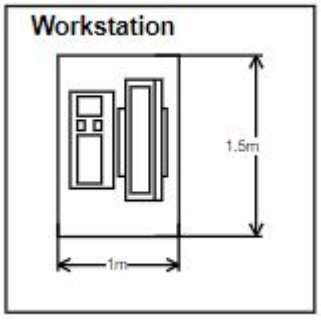

Figure 6.8: Details of the workstation in labs

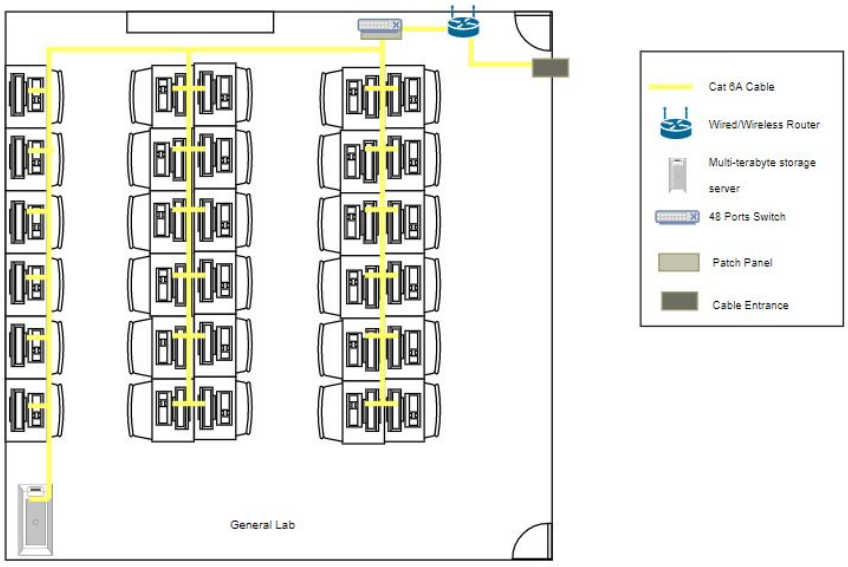

Figure 6.9: Cabling Connection in Labs

Cable Entrance to WiFi router: 4m

WiFi router to 48-port switch: 2m

Switch to workstation: 208.5m

Switch to server: 15m

Switch to floor (refer working table to floor=25inch): 0.635*31 = 19.69m

Floor to 30 workstation + 1 server (refer working table to floor=25inch): 0.635*31 =19.69m

Total Cat 6A cable for one lab : 284.57m

Total Cat 6A cable for 4 lab: 284.57*4 = 1138.26m

Total Cat 6A cable for second floor: 1265.26m

Vertical Cabling

Figure 6.10: Vertical Cabling Connection

The vertical cabling is used to connect between the first floor and the second floor of the building. The cable that is used in vertical cabling is fiber optics.

First floor to second-floor : 5m

Total Fiber Optics Cable : First floor to second-floor + First Floor + Second Floor
= 5 + 443 + 322
= 770m

Total CAT 6A Cable : First Floor + Second Floor
= 17 + 1265.26
= 1282.26m

7.0 IP ADDRESSING SCHEME

7.1 Subnetting

In this section, we are going to divide the subnetwork from the network address, 192.20.0.0/8.

Let's use IP address 192.20.0.0 with subnet mask 255.0.0.0 or /8.

IP address(Decimal) :	192.	20.	0.	0
IP address(Binary) :	**11000000**	00010100	00000000	00000000
Subnet Mask (Decimal):	255.	0.	0.	0
Subnet Mask(Binary):	11111111	00000000	00000000	00000000

1. We divided the IP address into the network portion indicated by subnet mask (/8) and the host portion is the remaining bits.

   Network portion : 8 bits
   Host portion : 32 bits - 8 bits = 24 bits

2. To calculate the Subnet IP Address , we perform a bitwise AND operation (1+1=1, 1+0 or 0+1 =0, 0+0=0) on the host IP address and subnet mask. The result is the subnet address in which the host is situated.

IP address(Decimal) :	192.	20.	0.	0
IP address(Binary) :	11000000	00010100	00000000	00000000
Subnet mask (Binary) :	11111111	00000000	00000000	00000000
Subnet address(Binary) :	11000000	00000000	00000000	00000000
Subnet address(Decimal) :	192.	0.	0.	0

   Subnet Address: 192.0.0.0/8

3. We will use a Class A address, which takes 4 bits from the Host field for subnetting and leaves 20 bits for defining hosts. As we need 14 subnets, we are having 4 bits available for defining subnets means that we can have up to 16 (2^4) different subnets but we divide the IP address into 14 subnets.

IP address	**Network portion (8 bits)**	**Subnet (4 bits)**	**Host portion (20 bits)**
Subnet Address 192.0.0.0/8	11000000	**0000**	0000 00000000 00000000
Subnet 0 192.0.0.0/12	11000000	**0000**	0000 00000000 00000000
Subnet 1 192.16.0.0/12	11000000	**0001**	0000 00000000 00000000
Subnet 2 192.32.0.0/12	11000000	**0010**	0000 00000000 00000000
Subnet 3 192.48.0.0/12	11000000	**0011**	0000 00000000 00000000
Subnet 4 192.64.0.0/12	11000000	**0100**	0000 00000000 00000000
Subnet 5 192.80.0.0/12	11000000	**0101**	0000 00000000 00000000
Subnet 6 192.96.0.0/12	11000000	**0110**	0000 00000000 00000000
Subnet 7 192.112.0.0/12	11000000	**0111**	0000 00000000 00000000
Subnet 8 192.128.0.0/12	11000000	**1000**	0000 00000000 00000000

Subnet 9 192.144.0.0/12	11000000	**1001**	0000 00000000 00000000
Subnet 10 192.160.0.0/12	11000000	**1010**	0000 00000000 00000000
Subnet 11 192.176.0.0/12	11000000	**1011**	0000 00000000 00000000
Subnet 12 192.192.0.0/12	11000000	**1100**	0000 00000000 00000000
Subnet 13 192.208.0.0/12	11000000	**1101**	0000 00000000 00000000

4. After we divide into 14 subnet IP address, we follow the 14 subnet address and:

   Set the remaining host portion (21 bits) as all zero(0) to get network address
   192.[0000 | **0000 00000000 00000000**]
   Network address of Subnet 0: 192.0.0.0

   Set the remaining host portion (21 bits) as all one(1) to get broadcast address
   192.[0000 | **1111 11111111 11111111**]
   Broadcast address of Subnet 0: 192.15.255.255

Subnet IP address	**Network portion (8 bits)**	**Subnet (4 bits)**	**Host portion (20 bits)**		**IP address**
Subnet Address 192.0.0.0/8	11000000	0000	0000 00000000 00000000		
Subnet 0 192.0.0.0/12	11000000	0000	0000 00000000 00000000	**Network address**	**192.0.0.0**
			1111 11111111 11111111	**Broadcast address**	**192.15.255.255**
Subnet 1 192.16.0.0/12	11000000	0001	0000 00000000 00000000	**Network address**	**192.16.0.0**
			1111 11111111 11111111	**Broadcast address**	**192.31.255.255**
Subnet 2 192.32.0.0/12	11000000	0010	0000 00000000 00000000	**Network address**	**192.32.0.0**
			1111 11111111 11111111	**Broadcast address**	**192.47.255.255**

Subnet 3 192.48.0.0/12	11000000	0011	0000 00000000 00000000	**Network address**	**192.48.0.0**
			1111 11111111 11111111	**Broadcast address**	**192.63.255.255**
Subnet 4 192.64.0.0/12	11000000	0100	0000 00000000 00000000	**Network address**	**192.64.0.0**
			1111 11111111 11111111	**Broadcast address**	**192.79.255.255**
Subnet 5 192.80.0.0/12	11000000	0101	0000 00000000 00000000	**Network address**	**192.80.0.0**
			1111 11111111 11111111	**Broadcast address**	**192.95.255.255**
Subnet 6 192.96.0.0/12	11000000	0110	0000 00000000 00000000	**Network address**	**192.96.0.0**
			1111 11111111 11111111	**Broadcast address**	**192.111.255.255**
Subnet 7 192.112.0.0/12	11000000	0111	0000 00000000 00000000	**Network address**	**192.112.0.0**
			1111 11111111 11111111	**Broadcast address**	**192.127.255.255**
Subnet 8 192.128.0.0/12	11000000	1000	0000 00000000 00000000	**Network address**	**192.128.0.0**
			1111 11111111 11111111	**Broadcast address**	**192.143.255.255**
Subnet 9 192.144.0.0/12	11000000	1001	0000 00000000 00000000	**Network address**	**192.144.0.0**

			1111 11111111 11111111	**Broadcast address**	**192.159.255.255**
Subnet 10 192.160.0.0/12	11000000	1010	0000 00000000 00000000	**Network address**	**192.160.0.0**
			1111 11111111 11111111	**Broadcast address**	**192.175.255.255**
Subnet 11 192.176.0.0/12	11000000	1011	0000 00000000 00000000	**Network address**	**192.176.0.0**
			1111 11111111 11111111	**Broadcast address**	**192.191.255.255**
Subnet 12 192.192.0.0/12	11000000	1100	0000 00000000 00000000	**Network address**	**192.192.0.0**
			1111 11111111 11111111	**Broadcast address**	**192.207.255.255**
Subnet 13 192.208.0.0/12	11000000	1101	0000 00000000 00000000	**Network address**	**192.208.0.0**
			1111 11111111 11111111	**Broadcast address**	**192.223.255.255**

7.2 IP Assignation

After we get the network and broadcast address, we assign the subnet address according to the 14 areas of the building. We have 2 routers and 4 switches on the first floor whereas 4 routers and 4 switches on the second floor. We assign the 14 subnets according to the work area of routers and switch.

Subnet	**Interface**	**Network Address**	**Broadcast Address**	**Range of usable address**	**Subnet mask**
0	Second Floor Switch 1(server room)	192.0.0.0	192.15.255.255	192.0.0.1 to 192.15.255.254	/12 255.240.0.0
1	Second Floor Switch 2 WAP for the north area	192.16.0.0	192.31.255.255	192.16.0.1 to 192.31.255.254	/12 255.240.0.0
2	Second Floor Switch 3 WAP for the west area	192.32.0.0	192.47.255.255	192.32.0.1 to 192.47.255.254	/12 255.240.0.0
3	Second Floor Router 1(CS Lab)	192.48.0.0	192.63.255.255	192.48.0.1 to 192.63.255.254	/12 255.240.0.0

4	Second Floor Router 2 (IoT Lab)	192.64.0.0	192.79.255.255	192.64.0.1 to 192.79.255.254	/12 255.240.0.0
5	Second Floor Router 3(Network Lab)	192.80.0.0	192.95.255.255	192.80.0.1 to 192.95.255.254	/12 255.240.0.0
6	Second Floor Router 4(General Lab)	192.96.0.0	192.111.255.255	192.96.0.1 to 192.111.255.254	/12 255.240.0.0
7	Second Floor Switch 0 WAP for east and west	192.112.0.0	192.127.255.255	192.112.0.1 to 192.127.255.254	/12 255.240.0.0
8	First Floor Router 0 (office)	192.128.0.0	192.143.255.255	192.128.0.1 to 192.143.255.254	/12 255.240.0.0
9	First Floor Router 1(technical room)	192.144.0.0	192.159.255.255	192.144.0.1 to 192.159.255.254	/12 255.240.0.0

10	First Floor Switch 0 WAP for north-west	192.160.0.0	192.175.255.255	192.160.0.1 to 192.175.255.254	/12 255.240.0.0
11	First Floor Switch 1 WAP for north-east	192.176.0.0	192.191.255.255	192.176.0.1 to 192.191.255.254	/12 255.240.0.0
12	First Floor Switch 2 WAP for the lobby	192.192.0.0	192.207.255.255	192.192.0.1 to 192.207.255.254	/12 255.240.0.0
13	First Floor Switch 3 WAP for south	192.208.0.0	192.223.255.255	192.208.0.1 to 192.223.255.254	/12 255.240.0.0

8.0 CONCLUSION

To conclude, there have been some achievements we made during this project. Each of our teammates has their own viewpoint on their successes, which is an unique experience for our team. Our biggest achievement throughout this project is we are able to identify and solve it according to the task requirements.For instance, we are required to compare the types of the devices and the price of each device but also need to determine which connections are suitable to be placed in our building. In order to conquer this situation, we discussed and divided the tasks based on the expertise of our group members.Fortunately, we are able to resolve this issue quickly and properly.

Besides achievement, our team is built up with a good team spirit.It is because our team has its own strengths and limitations too during the project.However, because of the spirit of team work within each of the group members, we drive our project in a good way. For instance, we will discuss and divide the group work equally before starting a new task of our project. All of the suggestions provided by each of the members during the discussions are useful for us to do the task efficiently. However, the weakness of our group during the project is miscommunication. It is because we are not able to meet with each other face to face for the discussions due to this pandamic which may lead to the slow and unorganised work. Fortunately, we are able to counter this issue faster.

9.0 TEAM MEMBERS AND RESPONSIBILITIES

NAME	RESPONSIBILITY
CHIAM WOOI CHIN A19EC0034	TASK 1: First Floor Floor Plan TASK 2: Provide suggestion for question list and find answers TASK 3: Research on server, generator TASK 4: Connection for work area for first floor, vertical cabling TASK 5: Subnetting
GOH JO EY A19EC0047	TASK 1: First Floor Floor Plan TASK 2:Provide suggestion for question list and find answers, determine the feasibility of the project TASK 3:Research on switch, wireless access point TASK 4: Connection for work area for first floor, horizontal cabling TASK 5: Subnetting
NG JING ER A19EC0115	TASK 1: SECOND FLOOR FLOOR PLAN TASK 2:Provide suggestion for question list and find answers TASK 3:Research on router TASK 4:Connection for work area for second floor, network devices arrangement TASK 5: IP assignation
ONG YIN REN A19EC0204	TASK 1: SECOND FLOOR FLOOR PLAN TASK 2:Provide suggestion for question list and find answers TASK 3:Research on patch panel, cable TASK 4: Connection for work area for second floor, Calculation for cable length TASK 5: IP assignation

REFERENCE

1. Singh, C. (2019, April 11). Computer Network Topology - Mesh, Star, Bus, Ring and Hybrid. Retrieved November 23, 2020, from https://beginnersbook.com/2019/03/computer-network-topology-mesh-star-bus-ringand-hybrid/
2. 2. Top 135 Networking Interview Questions & Answers. (n.d.). Retrieved November 23, 2020, from https://www.guru99.com/networking-interview-questions.html
3. Meela. (2017, August 16). Wireless Access Point vs. Wireless Router. Retrieved November 24,2020 from https://meelaz.medium.com/wireless-access-point-vswireless-router-8fc36e14b
4. Chapter 4: Cabling. (n.d.). Retrieved November 24,2020, from https://fcit.usf.edu/network/chap4/chap4.htm
5. Atalah, A., Chang-Jin, C., & Osburn, K. (2002). Comparison study of installing fiber optic cable in university campuses using trenchless techniques relative to open cut. In Pipelines 2002: Beneath Our Feet: Challenges and Solutions (pp. 1-17).
6. RT-AX88U: Networking. (n.d.). Retrieved December 13, 2020, from https://www.asus.com/my/Networking/RT-AX88U/
7. Products. (2018, September 27). Buffalo Technology. Retrieved December 13, 2020, from https://www.buffalo-technology.com/products/
8. Western Digital - US. (n.d.). Data Center Platform. Western Digital. Retrieved December 13, 2020, from https://www.westerndigital.com/products/data-center-platforms
9. Wireless Routers | Networking. (n.d.). ASUS Malaysia. Retrieved December 13, 2020, from https://www.asus.com/my/Networking/Wireless-Routers-Products/
10. N. (n.d.). Smart Managed Pro Switches | Switches | Business. NETGEAR. Retrieved December 13, 2020, from https://www.netgear.com/business/wired/switches/smart-managed-pro
11. Network Switches, LAN and Enterprise Switches. (2020, July 29). Cisco. Retrieved December 13, 2020, from https://www.cisco.com/c/en_my/products/switches/index.html

12. Athow, D. (2020, June 17). Best network switches of 2020: 1, 2, 5 and 10GbE hardware for small business and home office. TechRadar. Retrieved December 13, 2020, from https://www.techradar.com/sg/best/best-network-switches
13. Bastounis, O. (2020, December 5). Best wireless routers 2020: the best Wi-Fi for your home network. TechRadar. Retrieved December 13, 2020, from https://www.techradar.com/sg/news/networking/routers-storage/best-router-9-top-wireless-routers-on-test-1090523
14. S. (2019, December 4). 11 Best Wireless Access Points in 2020. Snap Goods. Retrieved December 13, 2020, from https://snapgoods.com/best-wireless-access-point/
15. Computer Hope, 2020. Network - Definition. Retrieve from https://www.computerhope.com/jargon/n/network.htm

APPENDICES

MEETING MINUTES

NO.	DATE	ATTENDANCE	MEETING REMARK
1.	05/11/20	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. Form group name. 2. Short brief on work distribution for Task 1(floor plan).
2.	08/11/20	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. First floor plan draft formed. 2. Discussion for floor plan changes.
3.	10/11/20	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. Second floor plan draft formed. 2. Discussion for floor plan improvement. 3. Task 1 (floor plan) completed and submitted.
4.	19/11/20	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. Discussion on preparing questions for Task 2.
5.	21/11/20	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. Discussion on the answers for questions prepared in Task 2.
6.	24/11/20	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. Task 2 completed.
7.	12/12/20	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. Discussion on Task 3 2. Research on network devices suitable for the organization
8.	13/12/20	1. GOH JO EY 2. CHIAM WOOI CHIN	1. Discussion on network devices suitable for the organization

		3. ONG YIN REN 4. NG JING ER	2. Discussion on cable suitable for the organization
9.	16/12/20	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. Task 3 completed.
10.	26/12/20	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. Discussion on network devices arrangement and the cabling structure needed for task 4. 2. Distribute work areas on floor plan for connections and calculate estimated cable length to be used.
11.	30/12/20	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. Task 4 completed.
12.	09/01/21	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. Discussion on IP addressing scheme for task 5.
13.	10/01/21	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. Divide the subnetwork from the Network Address
14.	11/01/21	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. Assigned the 14 subnets according to the different work areas of router and switch.
15.	13/01/21	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. Task 5 completed.
16.	19/01/21	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. Distribution of work based on the report

17.	28/01/21	1. GOH JO EY 2. CHIAM WOOI CHIN 3. ONG YIN REN 4. NG JING ER	1. Project documentation report completed and submit