UTM
UNIVERSITI TEKNOLOGI MALAYSIA

Network Design for Faculty Of Computing Block N28B

SECR1213 - NETWORK COMMUNICATION

Semester 3, 2024/2025

Section 01

Group : Mozilla

NAME	MATRIC NUMBER
NAZATUL NADHIRAH BINTI SABTU	A23CS0144
NURUL ATHIRAH SYAFIQAH BINTI MOHD RAZALI	A23CS0163
NUR AINA SYAFINA BINTI KAMASUAHADI	A23CS0152
WAN NUR RAUDHAH BINTI MASZMANIE	A23CS0195

LECTURER: DR.MUHAMMAD ZAFRAN BIN MUHAMMAD ZALY SHAH

DATE: 25 JANUARY 2025

ABSTRACT

This report presents the planned upgrade network of the Faculty of Computing (FC) at Universiti Teknologi Malaysia. This primary objective is to accommodate the anticipated 15% growth in student and academic staff numbers over the next four years by constructing a new 2 storey building. This new facility will include a server room, student lounge, two general lab purposes, video conferencing room, hybrid classroom, cisco lab and embedded lab. All equipment will be high speed internet to align with the 4IR (Fourth Industrial Revolution) standards. The report outlines the requirement for a scalable, manageable and secure network infrastructure, capable of high performance and protection against various cyber threats. Key goals include maintaining seamless connectivity access during the transition to new equipment, implementing cutting edge technology, cost effectively and preparing the future growth with wireless connectivity. The findings and recommendations aim to guide the development of a reliable, efficient and future ready system that supports FC mission to advance computing education and research.

TABLE OF CONTENTS

TABLE OF FIGURES

1.0 INTRODUCTION

This project, undertaken by a 4 group of students, applies theoretical networking knowledge to a real-world scenario. By addressing user needs, budget constraints, and technical feasibility, we designed a network infrastructure tailored to the case study requirements. The goal was to create a small-scale network for a two-storey Computer Science Faculty building.

The project was structured into six tasks. Task 1 involved forming a team, analyzing the case study, and creating a building layout. Task 2 focused on gathering requirements, conducting research, and evaluating feasibility. In Task 3, we selected suitable LAN devices based on functionality, cost, and reliability. Task 4 implemented these devices to create a functional network infrastructure. Task 5 ensured effective IP addressing to avoid connectivity conflicts. Finally, Task 6 documented the process and reflected on outcomes.

The ground floor of the faculty building features a Server Room for IT infrastructure, a Student Lounge for relaxation and collaboration, and two General Purpose Labs for academic activities. These spaces address foundational operational needs. The first floor includes a Video Conferencing Room for remote interaction, a Hybrid Classroom for flexible learning, a Cisco Lab for hands-on networking training, and an Embedded Lab for IoT and microcontroller projects. These advanced facilities promote innovation and practical learning.

This project enhanced our problem-solving, technical, and teamwork skills. Designing the network required creativity, adaptability, and careful planning. The resulting network infrastructure is efficient, functional, and cost-effective, meeting current and future needs.

In conclusion, this project demonstrates the value of applying theoretical knowledge to practical challenges. The network solution supports the operational and educational goals of the Computer Science Faculty, ensuring robust and future-ready infrastructure.

2.0 PROBLEM BACKGROUND AND OVERVIEW

In this project, we designed and implemented a network for a new two-storey building, applying network communication concepts to a real-world scenario. To ensure success, we combined theoretical knowledge with practical research and stakeholder engagement. By gathering input through questionnaires, we aligned the network specifications with the stakeholders' needs.

With a budget of RM3,000,000.00 and a preference for top-quality brands, careful budgeting was essential. Our research focused on identifying high-performance devices that balanced quality and cost. We planned the placement and connections of LAN devices to maximize functionality and efficiency. This involved considering device positioning, cable lengths, and high-quality cables, as most devices were not wireless.

We also calculated distances between workstations, wireless access points (WAPs), routers, and the network backbone to optimize the layout and minimize costs. During implementation, we evaluated the adequacy of selected devices and adjusted as needed. A well-structured addressing scheme, supported by subnetting, was implemented to localize traffic and reduce congestion.

Our goal was to create a network with high speed, reliable performance, and scalability for future needs. By selecting quality devices and ensuring efficient IP distribution, we achieved a design that balances functionality and long-term reliability. Careful planning resulted in a robust infrastructure tailored to stakeholder requirements.

This project highlights the value of meticulous planning, stakeholder engagement, and informed decision-making. By combining high-performance devices with cost-effective solutions, we developed a network infrastructure that meets the operational and educational goals of the new building, ensuring readiness for future advancements.

3.0 SUGGESTED FLOOR PLAN

The Faculty of Computing (FC) is planning to build a new 2-storey building to accommodate its future growth, as student enrollment and staff numbers are expected to increase by 10% in the next three years. The new building will feature several essential facilities to meet the needs of the growing community. These include two general-purpose labs, a Cisco Network Lab, and an IoT Lab, collectively equipped with a total of 30 workstations to support various academic and research activities. Additionally, the building will house a video conferencing room for virtual collaboration, a student lounge to provide a comfortable space for relaxation and socializing, and other basic facilities to enhance the overall learning environment. The floor plan for this new development incorporates a strategic allocation of resources across the two levels to optimize space usage and ensure a seamless integration of these modern amenities. Furthermore, the design includes elements such as server racks, embedded lab tables, smart boards, and projectors to create an advanced, tech-enabled infrastructure suitable for both teaching and professional development. This initiative reflects FC's commitment to fostering innovation and meeting the demands of a dynamic academic landscape.

3.1 FIRST FLOOR

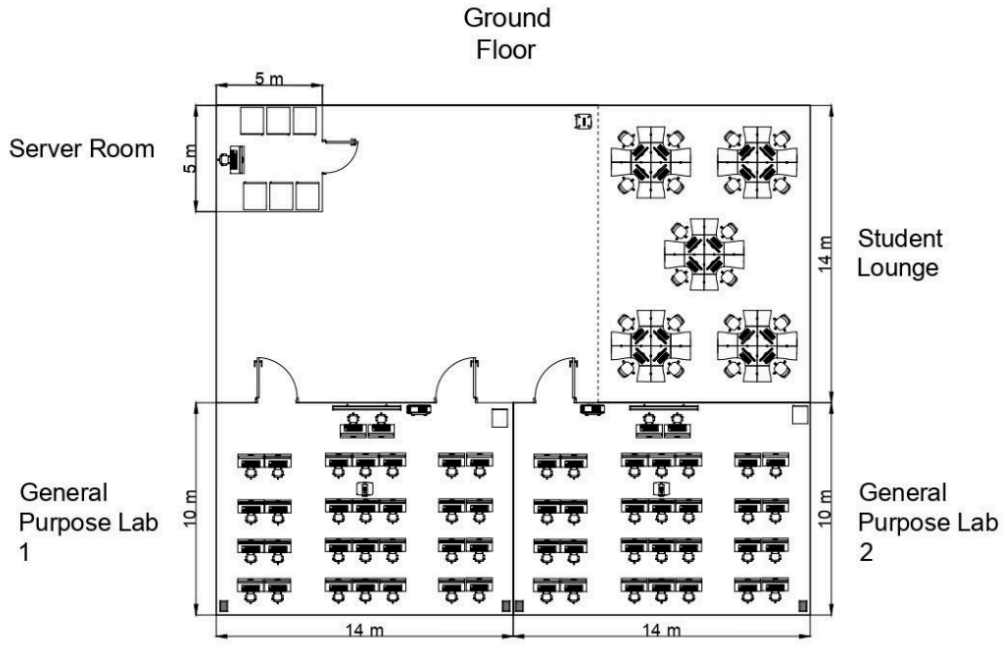


Figure 1.1 Ground Floor Plan

On the ground floor of the Faculty of Computing (FC) building, visitors are greeted by a spacious and welcoming lobby area, which serves as a central hub of activity. The design emphasizes openness and accessibility, creating a vibrant atmosphere for students, staff, and visitors alike. Adjacent to this central area, the ground floor is thoughtfully arranged to include essential spaces that cater to the academic and social needs of the Faculty of Computing community.

On one side of the floor plan is the server room, strategically positioned to house critical technological infrastructure. This room, measuring 5m x 5m, is equipped with six server racks and a workstation, ensuring seamless operation of the building's computing and networking requirements. Its placement on the ground floor allows for easy access by technical staff for maintenance and upgrades, while remaining discreetly positioned to avoid disruptions to other activities.

Located next to the server room is the student lounge, a versatile and inviting space measuring 14m x 10m. The lounge is designed to serve as a quiet study area with 20 workstations, offering an ideal environment for both group discussions and individual study sessions. Equipped with Wi-Fi connectivity, the lounge caters to students' academic needs while also serving as a space for informal gatherings.

Comfortable seating arrangements and a well-organized layout encourage productivity and foster a sense of community among students.

At the lower section of the floor plan, two General Purpose Labs are positioned side by side. Each lab measures 14m x 10m and is equipped with 30 modern workstations, two speakers, and a projector to support teaching and learning activities. These labs are designed to accommodate a wide range of academic and research tasks, from individual assignments to collaborative projects. The integration of advanced equipment promotes an interactive and dynamic learning experience. Their adjacent placement ensures convenience for students and staff, allowing for smooth transitions between spaces.

This ground floor layout has been carefully planned to prioritize functionality, accessibility, and community engagement. The combination of academic facilities, communal spaces, and critical infrastructure creates a dynamic and supportive environment that caters to the diverse needs of the Faculty of Computing. This thoughtful design ensures that the ground floor not only meets the current demands of the faculty but also accommodates its anticipated growth in the coming years.

3.2 SECOND FLOOR

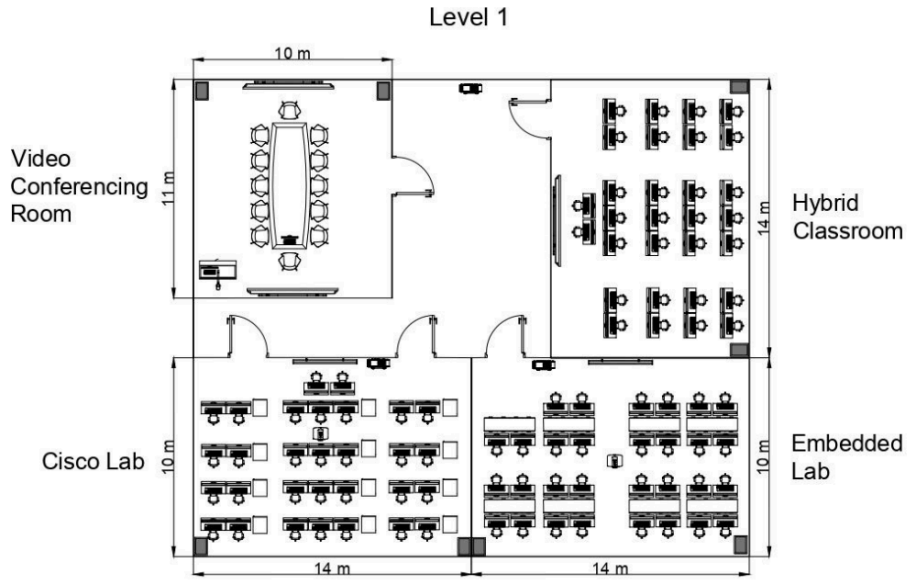


Figure 1.2 : First Floor Plan

As shown in the floor plan for Level 1, the layout has been carefully designed to optimize functionality and meet the academic and professional needs of the Faculty of Computing. The video conferencing room, located prominently on this level, is a versatile space tailored for virtual collaboration and meetings. It is equipped with a large conference table, a podium, a smart board, and two high-quality speakers. These features ensure that the room provides a seamless and professional experience, whether for internal meetings, virtual presentations, or collaborative sessions with external partners. This space is integral to fostering communication and teamwork in a modern academic environment.

Adjacent to the video conferencing room is the hybrid classroom, a state-of-the-art space designed to support blended learning approaches. This room is equipped with 30 advanced workstations, a smart board, and two strategically positioned speakers, creating an immersive learning experience. The hybrid classroom is specifically tailored for both in-person and remote education, ensuring flexibility in teaching methodologies. The workstations provide students with the resources they need to engage in interactive lessons, group projects, and individual assignments, making it a hub of active learning on this level.

On the opposite side of the floor plan is the embedded lab, a specialized space designed for hands-on learning in embedded systems and related technologies. This lab is furnished with 30

workstations, each equipped with the necessary tools and software to support students and researchers in their practical activities. A projector is installed to facilitate instructional sessions, presentations, and collaborative discussions. The layout of the embedded lab promotes a focused yet collaborative atmosphere, enabling students to work on complex projects effectively.

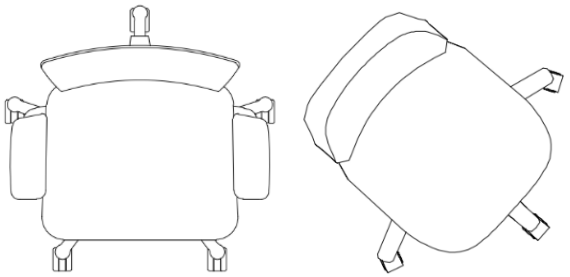
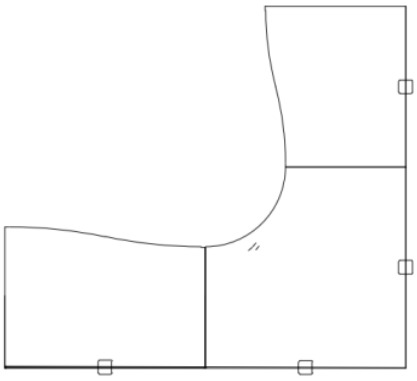
Next to the embedded lab is the Cisco lab, a critical component of the building's technical infrastructure and academic offerings. This lab is equipped with 30 workstations and 12 server racks, providing students with the opportunity to gain hands-on experience with real-world networking equipment. The inclusion of a projector allows instructors to deliver clear and engaging presentations, supporting theoretical concepts with practical demonstrations. The Cisco lab is designed to accommodate courses and activities in networking, telecommunications, and cybersecurity, making it an essential resource for both teaching and research.

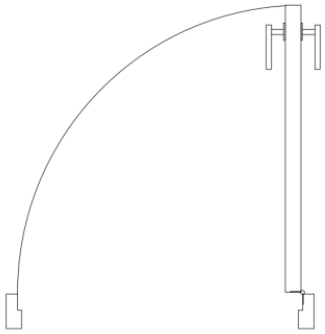
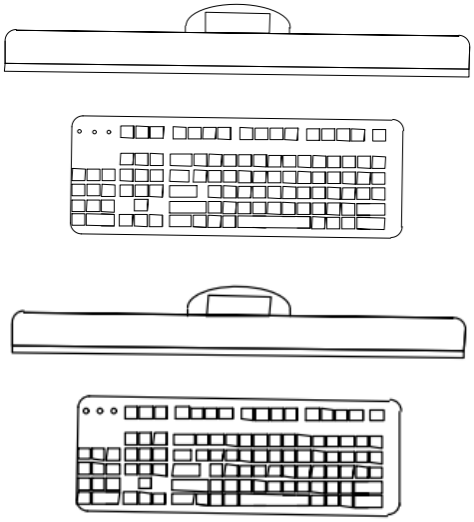
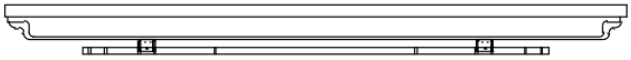
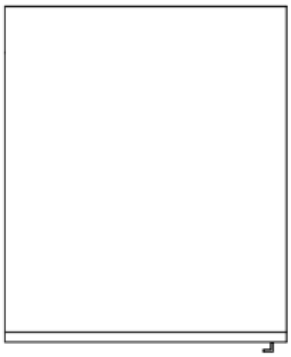
The floor plan for Level 1 reflects a commitment to fostering innovation, collaboration, and practical learning. Each space has been thoughtfully positioned to enhance functionality and accessibility, ensuring that students and staff can move seamlessly between the various facilities. The integration of advanced technologies, such as smart boards, projectors, and server racks, ensures that the infrastructure is well-suited for a dynamic and rapidly evolving academic environment.

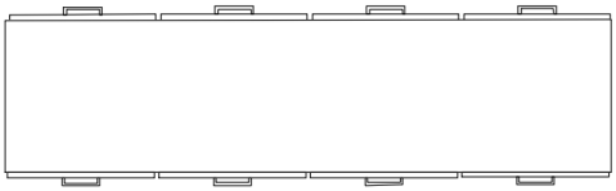
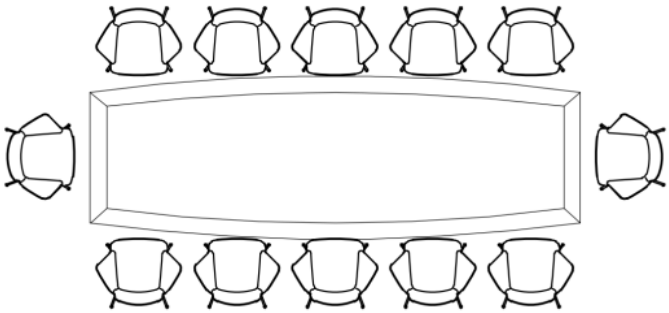
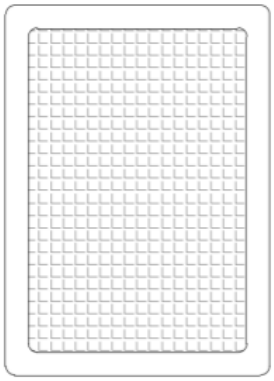
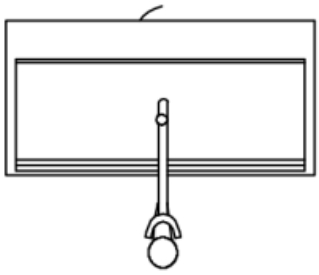
This design also includes considerations for robust networking infrastructure. With 30 workstations in each lab and classroom, the demand for reliable connectivity is high. Ethernet and Wi-Fi systems have been strategically implemented across both levels to ensure consistent network coverage, supporting a smooth and efficient workflow for everyone in the building.

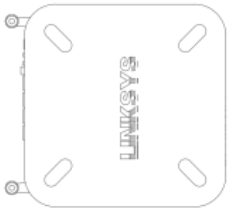
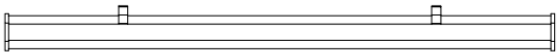
By combining modern technology with thoughtful spatial planning, this level of the building is positioned to become a cornerstone of the Faculty of Computing’s future growth, meeting the demands of an expanding community while fostering innovation and academic excellence.

LEGEND :

Icon	Name
	Chair
 	Desk
	Corner Desk

	Door
	PC
	Smart Board
	Server Rack

	Embedded Lab Table
	Conference Table
	Speaker
	Podium

	WiFi
	Projector Screen
	Projector

REFLECTION TASK 1

From task 1, we learned that understanding the project requirement and creating a detailed building layout was challenging as we need to apply theoretical knowledge in practical scenarios, enhancing our teamwork and project management skills. This includes creating the floor plan consisting of a two storey building. On the first floor, there is a server room, student lounge, general lab purpose 1 and general purpose lab 2. On the second floor, there is a video conferencing room, hybrid classroom, cisco lab and embedded lab. The emphasis on logical and mature planning , thinking like network consultants and trying for professional-grade deliverables provided valuable insights into a real world project execution. This experience made us realize the importance of clear communication through preparation to achieve high quality results.

4.0 PRELIMINARY ANALYSIS

4.1 QUESTION LIST

1. **What factors should we consider when anticipating an increase in users for each lab and classroom?**

When anticipating an increase in users for labs and classrooms, careful planning is essential to ensure the quality of the educational experience. First and foremost, providing sufficient equipment and materials is critical to prevent shortages and ensure all students have the resources they need for hands-on learning. This includes not only workstations and devices but also consumables and specialized tools for experiments and projects. Additionally, the infrastructure and layout of the spaces must be optimized to accommodate larger groups. This involves ensuring adequate workspace, ergonomic design, proper ventilation, and lighting to maintain comfort and productivity while adhering to safety regulations.

Another key consideration is resource management. Scientific equipment and software should be readily available to support data analysis, experiment design, and troubleshooting. Regular maintenance schedules and access to technical support become even more important as user numbers grow. To support effective learning, the instructor-to-student ratio should be carefully managed, possibly by increasing the number of teaching assistants or incorporating blended learning options like virtual labs and simulations. The curriculum should also be scalable to accommodate larger groups without compromising the quality of instruction.

Safety and compliance are paramount when accommodating more users. Emergency procedures, such as evacuation routes and fire safety measures, should be updated, and capacity limits must be respected to ensure a safe learning environment. Collaborative spaces and group projects play a vital role in fostering teamwork, enabling students to share resources and responsibilities effectively. Furthermore, the building's networking infrastructure should be robust enough to handle increased demand, with reliable Wi-Fi and Ethernet solutions to avoid slowdowns during peak usage.

Lastly, regular feedback from students and staff can provide valuable insights into areas for improvement. Pilot programs can be used to test changes on a smaller scale, ensuring that adjustments are effective and scalable. By addressing these factors comprehensively, labs and classrooms can accommodate growth while maintaining a high standard of safety, accessibility, and educational excellence.

2. **What types of devices (computers, printers, IoT devices, etc.) will be connected to the network in each area?**

The proposed network will incorporate a variety of devices to ensure seamless communication, efficient resource sharing, and enhanced functionality across all areas of the building. Computers will be the primary devices connected to the network, serving various tasks such as learning, teaching, research, and administrative work. Each lab, classroom, and office will be equipped with a sufficient number of computers to meet user needs. Shared printers will also be integrated into the network to provide convenient access for printing needs, allowing multiple users to share resources efficiently.

Additionally, Internet of Things (IoT) devices, such as cameras, sensors, and smart boards, will be connected to enhance the building's functionality and interactivity. Cameras may support security and monitoring, while sensors can be used for environmental controls like temperature and lighting adjustments. Smart boards, particularly in classrooms and labs, will facilitate interactive learning and presentations. These IoT devices will contribute to creating a smart and adaptable environment that meets modern educational and operational requirements.

To support the network infrastructure, switches will be deployed to connect multiple devices within the Local Area Network (LAN), ensuring efficient data transfer and communication. Managed switches will provide advanced configuration options and monitoring capabilities, allowing administrators to optimize network performance and reliability. Routers will enable connectivity between internal networks and external sources, ensuring seamless access to the internet and other networks. Firewalls will be implemented to provide essential security by filtering and monitoring traffic between trusted internal networks and untrusted external connections. These measures will protect sensitive data and ensure the integrity of the network.

Together, these devices will create a robust and secure network environment designed to support the diverse needs of the new building. The infrastructure will enable effective collaboration, communication, and resource sharing, promoting a highly productive and innovative atmosphere for users.

3. **Are there any special security requirements for different rooms, like the Cisco Lab or Server Room?**

The network design incorporates tailored security measures to protect specific rooms, such as the Cisco Lab and Server Room, where critical infrastructure and sensitive data are housed. These spaces require enhanced securities controls to safeguard against both external and internal threats. For the Cisco Lab, which involves advanced networking equipment and simulations, robust access control mechanisms, such as keycard access or biometric authentication, are crucial to ensure that only authorized personnel can enter. Additionally, the lab's network connections are segregated using VLANs to isolate traffic and minimize vulnerabilities, and firewalls are configured to monitor and restrict data flows to prevent unauthorized access to sensitive systems.

In the Server Room, which houses critical infrastructure like server racks, storage systems, and networking equipment, security requirements are even more stringent. Physical security measures include reinforced doors, surveillance cameras, and restricted access protocols, such as multi-factor authentication or biometric systems. From a network perspective, a dedicated firewall, such as the Cisco ASA 5500-X Series, is deployed to establish a robust security perimeter. This firewall not only provides multi-gigabit protection but also includes intrusion prevention and detection capabilities to proactively identify and block malicious traffic.

To further enhance security, an Intrusion Detection System (IDS) is implemented to monitor network traffic directed at the server room's VLANs. When threats are detected, alerts are immediately generated to prompt action by the IT team. The flexibility of tools like Cisco IPS, which can operate in both IDS and Intrusion Prevention System (IPS) modes, allows security measures to adapt to evolving threats. Firewalls in active-standby configurations provide redundancy, ensuring continuous protection even in the event of hardware failure.

Additionally, the server room follows strict regulatory compliance standards to protect sensitive data, such as user records and financial information. Environmental monitoring systems for temperature, humidity, and power supply are integrated to prevent disruptions that could compromise server integrity. These comprehensive security strategies ensure that the Cisco Lab and Server Room are well-protected against unauthorized access, data breaches, and operational risks, aligning with the overall objective of creating a secure and efficient network environment.

4. **How do we protect and keep important systems running?**

To ensure the continuous operation and protection of important systems, a multifaceted approach is essential. Regularly updating operating systems with critical security patches is a fundamental step, as outdated systems are particularly susceptible to vulnerabilities and exploits. Alongside this, implementing reliable antivirus software such as Windows Defender, Norton, or Kaspersky and keeping it updated helps defend against malware and other security threats.

It is equally important to update all utilities and applications to enhance system performance, address security issues, and access new features. Clearing unnecessary files and uninstalling unused programs using tools like CCleaner or similar utilities helps reduce system clutter and prevent slowdowns, ensuring optimal system efficiency. During software installations, it is critical to carefully review permissions and avoid installing bundled or potentially harmful programs that can compromise security or performance.

For hardware optimization, specific measures depend on the storage type. Systems utilizing traditional hard disk drives benefit from regular defragmentation to maintain performance. However, for solid-state drives, defragmentation should be avoided as it can reduce their lifespan. Instead, these drives should be monitored for firmware updates and performance issues.

Additional measures include implementing regular system backups to safeguard data and ensure recovery options in case of system failures. Utilizing uninterruptible power supplies protects against power surges or outages, reducing the risk of hardware damage or data loss. Finally, deploying robust network security measures such as firewalls, intrusion detection systems, and multi-factor authentication helps safeguard connected systems and maintain uninterrupted operations.

By combining these strategies, critical systems can remain secure, efficient, and resilient against potential threats and operational disruptions.

5. What equipment is needed to keep things powered and cool?

To ensure systems are powered effectively and maintained at optimal temperatures, specific equipment is essential. Deep-cycle batteries play a key role in standalone systems by storing electricity for periods when the primary energy source is inactive. These batteries work efficiently when paired with charge controllers, which regulate the flow of electricity, prevent overcharging, and extend battery life. In addition, power conditioning equipment such as inverters is vital for converting direct current (DC) to alternating current (AC), making the power compatible with standard appliances. For grid-connected systems, additional meters and instrumentation are necessary to monitor power usage and ensure compliance with utility provider standards.

Proper cooling and ventilation are critical for maintaining the safety and longevity of equipment. Temperature-controlled environments prevent overheating, which can degrade sensitive components such as batteries and electronics. Installing surge protectors, grounding systems, and safety disconnects provides additional safeguards against power surges, lightning strikes, and electrical faults, ensuring system reliability and protection against damage.

Together, these power and cooling measures form an essential foundation for sustaining reliable operations and preventing equipment failures. By addressing both power needs and environmental conditions, the longevity and efficiency of systems can be effectively preserved.

6. How fast should the internet be?

To ensure a fast and reliable internet experience suitable for various activities, the recommended download speed should be at least 100 Mbps, with an upload speed of at least 10 Mbps. These speeds can comfortably support activities such as streaming high-definition movies, attending video conferences, and gaming online, even when multiple devices are connected simultaneously. For users who frequently utilize streaming platforms or video conferencing tools like Zoom, a minimum download speed of 25 Mbps is considered essential to maintain smooth and uninterrupted performance.

For environments with many users or connected devices, faster internet plans, such as those offering gigabit speeds, may be necessary to prevent slowdowns, buffering, or connection issues. To optimize network performance further, it's important to keep the router updated with the latest firmware and consider using a mesh router system to ensure strong and consistent coverage across larger spaces. By adopting these measures and selecting internet speeds that align with usage requirements, a seamless and efficient online experience can be achieved.

7. What are the maintenance and support expectations for the network?

The maintenance and support expectations for a network involve a combination of proactive and strategic activities to ensure the continuous and smooth operation of both physical and non-physical assets within the IT ecosystem. Key components of these expectations include robust cybersecurity measures to protect against emerging threats, ongoing performance analysis to address potential issues like bandwidth bottlenecks, connection lags, and latency. Scalability is also a critical consideration, as the network needs to accommodate organizational growth and an increasing number of users and devices over time.

Regular hardware and software updates are necessary to enhance both performance and security, ensuring that the network stays aligned with the latest technological advancements and cybersecurity standards. Furthermore, compliance with relevant internal and external regulations, such as data protection laws or industry-specific standards, is crucial. A comprehensive approach to network maintenance also includes preemptive repairs based on data analytics that identify potential issues before they escalate, thus preventing system outages or disruptions.

Network maintenance can be carried out by in-house IT staff, original equipment manufacturers (OEMs), or third-party maintenance (TPM) providers, each offering different benefits based on expertise, cost, and service level agreements. Regardless of the provider, a well-defined network maintenance plan should cover services such as troubleshooting, product installation, configuration, performance monitoring, growth planning, compliance assurance, and the establishment of strong network security protocols.

By addressing these various factors and implementing a strategic maintenance and support framework, organizations can ensure their networks operate efficiently, securely, and effectively, thus supporting business continuity and minimizing the risk of disruptions.

8. What type of router is needed for the labs?

For the labs, selecting the appropriate routers and switches is crucial to meet the needs of students and instructors, particularly for CCNA (Cisco Certified Network Associate) practice. The Cisco 2900 series routers are highly recommended due to their affordability, reliability, and comprehensive support for all necessary commands required for both CCNA and CCNP (Cisco Certified Network Professional) courses. These routers provide the capability to practice a wide range of networking configurations and protocols.

While the Cisco 1800 and 2800 series are older models and may lack some of the advanced features needed for CCNA exams, they can still serve as useful options if they are available at a low cost or for free, especially for basic practice scenarios.

When selecting a router, it is essential to ensure it has sufficient flash memory and RAM to support the operating system and processes, especially if multiple configurations or simulations will be running simultaneously. This ensures smooth operation and the ability to handle various networking tasks.

For switches, the Cisco Catalyst 3650 is a reliable and modern choice that supports both CCNA and CCNP requirements. This switch provides essential features for practicing network management and configuration tasks, making it a solid investment for the lab environment.

Overall, the routers and switches chosen should support the necessary protocols and configuration practices for students to gain hands-on experience with the core skills covered in CCNA exams. This setup will allow for effective and comprehensive networking practice while ensuring compatibility with the CCNA curriculum.

9. What kind of network setup works best for the building?

For the building, the best network setup should focus on optimizing both wired and wireless connections to ensure reliable and high-performance coverage across all areas. First, placing the main router in a central location is essential to maximize coverage. This allows the router to distribute the network signal effectively to all parts of the building.

To extend the network range, Ethernet cabling is the preferred method due to its reliability and high-speed performance. Ethernet connections provide a stable backbone for the network and can be used to connect switches in remote areas, enabling multiple devices to be connected to the network without compromising performance. For areas that are farther from the main router, additional wireless access points (APs) should be deployed to ensure seamless Wi-Fi coverage throughout the building. These APs can be strategically placed to fill in coverage gaps.

While powerline adapters or mesh systems like AmpliFi, Eero, or Linksys Velop can also extend the network, they are generally less reliable than Ethernet cabling. Powerline adapters utilize the building's existing electrical wiring, while mesh systems create a network of interconnected nodes. Although these solutions can be easier to set up and require fewer physical modifications, they may not offer the same consistent performance and reliability as direct Ethernet connections, especially for high-bandwidth applications.

In terms of wireless extenders, it’s best to avoid them because they tend to only amplify weak signals without improving overall performance. They might create the illusion of a better connection, but they do not enhance the network's capacity or stability.

In conclusion, a hybrid network setup using a combination of Ethernet cabling for the main network backbone and wireless APs for extending coverage is ideal. This setup will ensure optimal performance, security, and scalability to support the growing needs of the building’s users.

10. Why should we set up smaller networks (subnetting) in the building?

Setting up smaller networks through subnetting is essential for optimizing the overall network performance and enhancing security within the building. Subnetting divides the larger network into smaller, more manageable segments, known as subnets, which helps to control and isolate network traffic. This segmentation allows the network to function more efficiently, reducing congestion and improving speed by limiting the broadcast domains to smaller groups of devices.

By implementing subnetting, the network becomes more scalable, as new devices or departments can be added to specific subnets without affecting the entire network. It also improves resource management by ensuring that devices within a subnet can communicate directly without unnecessary traffic being routed through the whole network.

Another key benefit of subnetting is enhanced security. Each subnet can have its own security policies, such as firewalls and access control lists (ACLs), which restrict communication between different subnets. This helps to protect sensitive data and prevent unauthorized access to certain network resources. For example, critical infrastructure devices, such as servers and IoT devices, can be placed on separate subnets with stricter security measures, ensuring they are not easily accessed from less secure parts of the network.

Subnetting also simplifies network management by making it easier to troubleshoot and identify issues within specific subnets, rather than dealing with the entire network. This targeted approach to monitoring and maintenance reduces downtime and increases overall network reliability.

Overall, subnetting in the building's network will ensure efficient communication, improved security, better performance, and scalability, all of which are critical as the number of users and devices grows over time.

11. **What are the primary activities or applications to be supported by the network in each room?**

The network in each room of the building will support a variety of key applications designed to enhance the overall functionality and support the specific needs of the space. In the classrooms and labs, primary activities will include access to Learning Management Systems (LMS) like Moodle, Canvas, or Blackboard. These platforms enable students to access educational resources, participate in online courses, and complete assessments. In addition, networked applications such as Microsoft Office 365 and Google Workspace will allow students and faculty to collaborate on projects, create documents, and communicate effectively through tools like email, video conferencing, and shared calendars.

For collaboration, rooms such as the video conferencing room will rely on platforms like Zoom or Microsoft Teams for meetings, discussions, and remote presentations. These applications will be supported by high-quality video and audio devices, ensuring smooth communication and interaction across distances. File sharing services like Google Drive, OneDrive, or Dropbox will allow users to upload, store, and share documents seamlessly within and across rooms.

In specialized areas like the Cisco Lab and Embedded Lab, the network will support more technical applications. Cisco Labs will run network management software, such as Cisco Prime or SolarWinds, enabling administrators to configure, monitor, and manage network performance. These tools are crucial for ensuring optimal network functionality and troubleshooting any issues that arise. Similarly, software and tools for hands-on learning and configuration of IT infrastructure will be essential in these labs.

IoT management platforms will be important in rooms with IoT devices, such as sensors or security cameras, helping to manage and monitor these devices, collect data, and automate functions. For example, these platforms could be used to control lighting, temperature, or security measures, contributing to a smarter and more efficient building environment.

Additionally, data analysis applications like Tableau, Microsoft Power BI, and Google Analytics will be used in research labs to process and visualize data, supporting the academic and research goals of the Faculty of Computing. Helpdesk and IT support systems, such as Zendesk or ServiceNow, will assist in managing any technical issues related to the network, ensuring that users can quickly address problems and keep the network running smoothly.

To ensure reliable internet access, solutions such as Distributed Antenna Systems (DAS) will be deployed to amplify signals throughout the building, overcoming structural obstacles that might interfere with wireless connectivity. Wireless repeaters and strategic placement of wireless access points (APs) will also be important in maintaining consistent coverage in all areas. Keeping equipment up to date and addressing common issues like interference or distance from APs will further improve network performance and enhance the user experience.

In summary, the network in each room will be designed to support a wide range of applications, from collaboration and communication tools to specialized software for network management and data analysis, ensuring that users in all areas of the building can work efficiently and effectively.

12. How can we ensure the internet works well for everyone in the building?

To ensure the internet works well for everyone in the building, several strategies must be implemented to address common issues that may affect wireless connectivity. A key factor to consider is the distance between wireless access points (APs) and devices, as greater distances can lead to weaker signals. Proper placement of APs in central locations can help distribute the signal more evenly across the building. Additionally, it is essential to minimize interference from other electronic devices, structural elements like walls, or metal surfaces that can block signals.

An effective solution is the implementation of Distributed Antenna Systems (DAS), which can amplify signals inside the building, overcoming obstacles and ensuring consistent coverage even in hard-to-reach areas like basements or areas with dense construction materials. Wireless repeaters or extenders can also be deployed in areas with weak signal coverage, extending the range and ensuring stable connections for devices far from the primary APs.

Regularly updating equipment, including routers, switches, and APs, is another vital step to improve internet performance. Outdated equipment may not be able to handle the latest technology standards or provide the necessary speed and capacity for growing demands, so keeping hardware up-to-date is crucial.

By combining these measures an optimal placement of APs, use of DAS, strategic installation of repeaters, and equipment upgrades so you can ensure strong, reliable internet connectivity for all users throughout the building, enhancing both performance and user experience.

4.2 FEASIBILITY OF THE PROJECT

The feasibility of this project involves an in-depth evaluation of its viability in terms of technical, economic, and operational aspects. In this report, we assess whether the proposed network infrastructure and its related systems can be implemented successfully within the available time frame, budget, and resources. This analysis also takes into consideration the potential risks and challenges associated with the project to ensure that it can be completed effectively and efficiently, ultimately supporting the goals of the building's stakeholders.

From a technical standpoint, the project is entirely feasible with the appropriate tools and resources in place. High-performance routers will be placed in high-traffic areas, such as the labs, while cost-effective routers will be utilized in less busy spaces to optimize resource allocation. To ensure reliable Wi-Fi coverage across the entire building, mesh systems will be implemented, with additional access points and wireless extenders deployed to mitigate any potential dead zones. The network will be designed with scalability in mind, featuring technologies like VLANs and SDN to enable centralized management and future expansion without needing additional hardware. Reliable cabling, such as CAT6a and fiber optics, will ensure high-speed connectivity, while dual routers will provide redundancy to avoid downtime. Security will be a priority, with firewalls and VPNs in place to protect sensitive data and maintain privacy, which is essential in an academic setting.

The economic feasibility of this project is supported by a generous RM3 million budget, which is more than adequate to cover all necessary expenses. This funding ensures that there will be no financial constraints that could impede the project's progress. The budget will be allocated for the acquisition of networking hardware, software licenses, as well as the hiring of qualified personnel to manage and implement the network. It also covers the recurring costs for server maintenance, web hosting, and system updates, which will help maintain the network's performance over time. Additionally, the project will allow for the promotion of the network to schools, educators, and other relevant stakeholders, ensuring that the system reaches its target audience. This solid financial foundation ensures that the project will meet all deadlines while maintaining high-quality standards throughout its execution.

Operationally, the project is well within the capabilities of the available resources and is designed to support the daily activities of students, faculty, and staff. The network will provide seamless connectivity across the building’s various spaces, such as classrooms, labs, and lounges. The use of VLANs will facilitate scalability, making it easy to add more users and devices as needed. Backup paths will be implemented to ensure that the network remains operational, even if a primary connection fails.

Firewalls will be carefully managed to maintain security without affecting performance, while VPNs will enable safe remote access for hybrid learning and working environments. The network will be designed to handle peak usage smoothly, ensuring that all users can access the resources they need without delays or interruptions.

In conclusion, the proposed network infrastructure project is feasible from both a technical and financial perspective. With careful planning and execution, the project will result in a reliable and scalable network that meets the needs of the building's occupants. The RM3 million budget provides ample resources to cover all necessary aspects of the project, ensuring that it is completed on time and within budget. The network will not only support the daily needs of students, staff, and faculty but also be scalable to accommodate future growth. Ultimately, this project represents a worthwhile investment that will enhance the efficiency and effectiveness of the building's operations while promoting a secure and accessible environment for all users.

REFLECTION TASK 2

For task 2, it requires us to think critically and strategically about the project requirement and feasibility. The process of generating the questions, conducting interviews and researching information enhanced our understanding and communication skills. We obtained answers by interviewing the faculty representative (our lecturer) and conducting extensive research. This approach ensures our information is both accurate and up to date. After gathering all necessary information, we analyzed the feasibility of the project. Our analysis indicated that the project is feasible, provided that recommendations for network design and infrastructure are followed. By working collaboratively, we were able to synthesize diverse perspectives and arrive at well informed conclusions. This task emphasized the importance of preparation, meticulous research and clear documentation in project planning and execution. Overall the experience was invaluable in developing our ability to conduct preliminary analysis and make informed decisions.

5.0 CHOOSING THE APPROPRIATE LAN DEVICES

5.1 LIST OF DEVICES

1. **Server**

A server is a specialized computer or software system designed to manage, store, and provide resources or services to other computers, known as clients, within a network. Servers play a central role in networking by handling tasks such as data storage, file management, hosting applications, and facilitating communication between clients. Unlike regular personal computers, servers are optimized for reliability, scalability, and performance, often running continuously to ensure uninterrupted service. Depending on their role, servers can provide various services, including web hosting, email management, database storage, or file sharing, making them essential for modern IT infrastructures.

Model	 **Dell EMC PowerEdge T640 Tower Server**	 **Huawei RH2288H V3 Server**
Performance	• 2 x Intel Xeon Platinum 8168 (24 cores each, 48 threads) • Up to 2.7GHz	• 1 x Intel Xeon E5-2620 V4 (8 cores, 16 threads) • 2.1GHz
Scalability	Highly scalable for future growth	Moderate scalability
Memory	768GB DDR4 (expandable up to 3TB)	16GB DDR4 (expandable)
Storage	6 x 1.92TB SSD (total: 11.52TB)	2 x 600GB 10K SAS (total:

		1.2TB)
Integration	Compatible with modern IT tools, software-defined technologies	Basic enterprise compatibility
Expandability	Multiple PCIe slots, additional drive bays for storage upgrades	Multiple PCIe slots, limited expandability
Price	RM 28,821.00	RM 14,092.98
References	https://www.server2u.com/shop/t640-xp8168-refurbished-dell-emc-poweredge-t640-tower-server-2xxp8160m-768gb-6x1-92tb-57402?gad_source=1&gclid=CjwKCAiA9bq6BhAKEiwAH6bqoEoGrl8Io-32YG1FfgFlaAesb2XIk0phgROAWT2ZYLx1fNneiungMRoCZEAQAvD_BwE#attr=	https://www.router-switch.com/huawei-rh2288h-v3-e5-2620-v4-16gb-ddr4-600gb-sas-sr130-460w.html

We have chosen the Dell EMC PowerEdge T640 for its exceptional performance, scalability, and ability to meet both current and future business needs. The Dell EMC PowerEdge T640 is a high-performance tower server designed for scalability and versatility, making it an ideal choice for small to medium-sized businesses with demanding workloads. Powered by dual Intel Xeon Platinum 8168 processors with 24 cores, 48 threads, and speeds of up to 2.7 GHz, the T640 significantly outperforms servers equipped with a single Intel Xeon E5-2620 V4 processor, which offers only 8 cores, 16 threads, and a maximum speed of 2.1 GHz. This enhanced processing capability makes the T640 well-suited for resource-intensive tasks.

In addition to superior processing power, the T640 features exceptional memory capacity, offering 768 GB of RAM that can be expanded up to 3 TB. This far surpasses the 16 GB RAM found in other servers, enabling the T640 to handle larger workloads and accommodate future growth in memory requirements. Furthermore, its advanced storage configuration includes six 1.92 TB SSDs, providing significantly more space and faster data access compared to other servers. With multiple PCIe slots and additional drive bays, the T640 offers extensive scalability for future upgrades.

Given its superior performance, robust scalability, and enhanced storage capabilities, the Dell EMC PowerEdge T640 stands out as a reliable and future-proof investment. It delivers the power and flexibility necessary to meet current demands while being ready for future growth, making it an excellent long-term solution for businesses.

2. Router

A router is a networking device that forwards data packets between computer networks, typically connecting different networks, such as a local area network (LAN) and the internet. Routers determine the best path for data to travel across networks by using routing tables and protocols. They are responsible for directing traffic efficiently, ensuring that data reaches its correct destination while avoiding congestion or delays. Routers also perform additional functions, such as network address translation (NAT), which allows multiple devices within a network to share a single public IP address, and providing security features like firewalls to protect the network from unauthorized access. By managing both data traffic and security, routers are fundamental components of modern networking infrastructure.

Model	 **C8500-12X**	 **S5860-24XB-U is FS**
Performance	12 x 10G SFP+ ports, typically used in enterprise routing.	High-speed with 24 x 10GBASE-T/Multi-Gigabit ports + 4 x 25Gb SFP28 uplinks.
Expendability	No direct stacking support, relies on additional modules for expansion.	Supports stacking for easy expandability.
Processor	Advanced Cisco processors, focused on routing and higher network intelligence.	Broadcom chip, designed for high throughput and Layer 3 routing.
Ports	12 x 10G SFP+ ports.	24 x 10GBASE-T, 4 x 10Gb SFP+, 4 x 25Gb SFP28 uplinks.
Scalability	Scalability via modular add-ons but lacks stacking support.	Good scalability through stacking and high-capacity uplinks.

Price	RM 309,163.23	RM17,594.00
References	https://www.cdw.com/product/cisco-catalyst-8500-12x-edge-platform-switch-12-ports-rack-mountable/6318206?msockid=1aacc11c3625648a13d5d5c73752655c	https://www.fs.com/sg/products/108716.html?country=my&currency=MYR&languages=English&paid=google_shopping&gad_source=1&gclid=Cj0KCQiAsaS7BhDPARIsAAX5cSBqMBul1WOBvwivPXsf6YwmUTkHPV_GcUH_8kHuVIfVmvvseJCj0tcaAiLPEALw_wcB

The most suitable router for our needs is the FS S5860-24XB-U, selected for its exceptional performance, advanced processing capabilities, scalability, and versatile port options. It delivers high-speed networking with 24 x 10GBASE-T/Multi-Gigabit ports and 4 x 25 Gb SFP28 uplinks, making it optimized for data-intensive tasks that require a combination of switching and routing. Powered by a Broadcom chip designed for high throughput and Layer 3 routing, this router ensures efficient handling of network traffic.

In terms of scalability, the FS S5860-24XB-U supports stacking, allowing seamless and straightforward expandability, an ideal feature for growing network environments with increasing uplink demands. Furthermore, its greater port density, offering 24 x 10GBASE-T ports and high-speed uplink options, provides flexibility for various networking requirements in high-throughput environments. These features make the FS S5860-24XB-U a reliable and future-ready choice for our network infrastructure.

3. Firewall

A firewall is a network security device designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet, to prevent unauthorized access and potential threats. Firewalls can be hardware-based, software-based, or a combination of both, and they inspect data packets to determine whether they should be allowed or blocked. Firewalls can be configured to filter traffic by specific IP addresses, ports, or protocols, and may also provide additional features such as intrusion detection and prevention, Virtual Private Network (VPN) support, and content filtering. By establishing a controlled environment, firewalls help protect sensitive data and prevent cyberattacks, making them a crucial element in maintaining network security.

Model	 **FPR2140-NGFW-K9 - Cisco Firepower 2100 Series Appliances**	 **Fortinet FortiGate 500E**
Storage	1x 200 GB with an additional spare slot for a managed service provider (MSP) storage expansion	1x 128 GB SSD
Security Capabilities	Advanced firewall, application visibility, malware protection, IPS	AI-based malware prevention, IPS, DLP, URL filtering, botnet protection
Performance	Optimized for enterprise-level threat defense and deep packet inspection	High threat protection performance with purpose-built SPU technology

Integration	Integrates with Cisco SecureX ecosystem	Fortinet Security Fabric and Fabric-Ready partner solutions
Price	RM 116,195.92	RM 25,364.53
References	https://www.router-switch.com/fpr2140-ngfw-k9.html	https://www.avfirewalls.com/FortiGate-500E.asp#pricing

We have chosen the FPR2140-NGFW-K9 - Cisco Firepower 2100 Series Appliances for its advanced security features, high performance, scalability, and seamless integration with other Cisco products, making it a reliable and future-proof solution for protecting our network. The FPR2140-NGFW-K9 - Cisco Firepower 2100 Series Appliances is an excellent choice for organizations seeking advanced security, high performance, and scalability for their enterprise networks. This next-generation firewall delivers top-notch protection against cyber threats, leveraging AI-based malware prevention, intrusion prevention (IPS), data loss prevention (DLP), URL filtering, and botnet protection, ensuring comprehensive and reliable threat defense.

Designed for scalability, it features a spare slot for adding additional storage, making it a future-proof solution for businesses with growing security requirements. Its robust security capabilities include application visibility and control, intrusion prevention, and malware protection, offering multiple layers of protection to safeguard the network. Optimized for enterprise use, the Cisco Firepower 2100 series efficiently manages high network traffic and performs thorough packet analysis without compromising performance, making it ideal for large-scale networks.

With its advanced security features, scalability, and seamless integration with other Cisco products, the Cisco Firepower 2100 series is a dependable and forward-looking solution for organizations aiming to protect their networks while preparing for future growth.

4. Wireless Access Point

A wireless access point (WAP) is a device that allows wireless devices, such as laptops, smartphones, and tablets, to connect to a wired network using Wi-Fi. It serves as a bridge between the wired network infrastructure (like a router or switch) and wireless devices, providing the wireless network connection. WAPs transmit and receive radio signals to enable wireless communication over a specific range, typically covering a defined area or room. They can support multiple devices simultaneously, allowing for better mobility within the network. Some WAPs also offer advanced features, such as Power over Ethernet (PoE), security protocols (like WPA2 or WPA3), and the ability to manage multiple SSIDs (Service Set Identifiers) for different network segments. By extending the network's reach, WAPs enable users to access network resources without the need for physical cables, making them essential components in modern networking environments, especially in large buildings or campuses.

Model	 **NETGEAR WEB 758-111 NAS WiFi 7**	 **Aruba AP-505 US**
Transmission speed	Up to 46 Gbps	Up to 9.6 Gbps.
Frequency Bands	2.4 GHz, 5 GHz, 6 GHz	2.4 GHz, 5 GHz.
Security	WPA3 encryption, enhanced efficiency with OFDMA and MU-MIMO.	WPA3, advanced security features like AirMatch and ClientMatch.
Advantages/ Disadvantages	Faster speeds, supports 6 GHz band.	Reliable for medium-density, advanced management features.
	Higher cost, limited device compatibility	Lower speeds, no support for 6 GHz band.

Price	RM 7,422.00	RM 2,691.97
References	https://www.networkhardwares.com/en-my/products/netgear-wbe758-111nas-netgear-1pt-insight-managed-wifi-7-wbe758-111nas?variant=47635341410509&gad_source=1&gclid=CjwKCAiAmMC6BhA6EiwAdN5iLd0jMgXUM2FjAv6FK2HfXXUXO_RrSxnYk4YtL4jRpn5D7A2y-jjlhxoC4ecQAvD_BwE	https://www.securewirelessworks.com/Aruba-AP-505.asp?srsltid=AfmBOopYwrG8Jrf0U1szYHMCyxjQfx6hVWVqCW4DvKAyGXcx1dG18Oee

The most suitable choice for our needs is the NETGEAR WEB 758-111 NAS WiFi 7, selected for its exceptional transmission speed, advanced frequency band support, and robust security features. It delivers speeds of up to 46 Gbps, which is five times faster than the Aruba AP-505 US, making it ideal for high-performance applications requiring ultra-fast connectivity.

The router operates on 2.4 GHz, 5 GHz, and 6 GHz frequency bands, with the 6 GHz band providing higher performance, reduced network congestion, and compatibility with emerging devices. Additionally, it offers WPA3 encryption and enhanced efficiency through features like OFDMA and MU-MIMO, ensuring superior security and optimized traffic management. These capabilities make the NETGEAR WEB 758-111 NAS WiFi 7 a reliable and future-ready solution for demanding networking environments.

5. Switch

A network switch is a device used to connect multiple devices within a Local Area Network (LAN) and enable them to communicate with each other. It operates at the data link layer (Layer 2) of the OSI model, forwarding data frames between devices based on their MAC addresses. Unlike hubs, which broadcast data to all devices, switches direct data to the specific device that needs it, improving network efficiency and reducing collisions. Switches can support both wired and wireless connections, and they come in various forms, including unmanaged, managed, and PoE (Power over Ethernet) switches, depending on the level of control and functionality needed. Managed switches offer advanced features such as VLAN support, network monitoring, and quality of service (QoS) to prioritize traffic. Switches play a crucial role in scaling networks, as they allow for more devices to be added without sacrificing performance. By creating a centralized communication point, switches improve data flow and reduce congestion within a network.

Model	 **WS-C3850-48XS-S Catalyst 3850 Switch SFP+**	 R0X27A - Aruba 6410 Switch
Port	48 x 10G SFP+ fiber ports.	Up to 48 x 10G SFP+ fiber ports
Switching Capacity	176 Gbps switching capacity	2.4 Tbps.
Advantages	• High switching capacity (176 Gbps) for large networks. • 48 x 10G SFP+ ports for high-speed fiber connections. • Cisco's IP Base features	• High switching capacity (2.4 Tbps) for large and scalable networks. • Modular design allows future expansion and flexibility. • AOS-CX operating

	for enhanced management and security. ● Excellent for data centers or high-demand environments.	system with advanced automation and analytics. ● Energy-efficient design.
Disadvantages	● Higher cost compared to more basic models. ● Not suitable for environments with extreme conditions (not hardened). ● More complex management due to advanced features.	● Higher initial cost due to modular architecture. ● Requires skilled personnel for managing advanced features. ● Larger physical footprint compared to fixed-configuration switches.
Price	RM 75,615.59	RM 57,314.29
References	https://www.router-switch.com/ws-c3850-48xs-s.html	https://www.router-switch.com/r0x27a.html

The most suitable switch for our needs is the Cisco Catalyst 3850 (WS-C3850-48XS-S), chosen for its high-speed connectivity, robust switching capacity, and seamless integration within the Cisco ecosystem. It features 48 x 10G SFP+ fiber ports, providing reliable high-speed fiber connections in a fixed configuration that is well-suited for medium-sized networks. With a switching capacity of 176 Gbps, it is optimized for high-demand environments, making it ideal for medium to large networks with typical throughput requirements.

The Catalyst 3850 supports stacking of up to nine switches, allowing for straightforward expansion as network demands grow. Its integration with the Cisco ecosystem ensures reliable and consistent performance, while the IP Base features offer enhanced management and security controls. However, it is important to note its limitations: the switching capacity may not suffice for very large-scale networks, its non-modular design limits expansion options, and its advanced features require skilled

personnel for effective management. Despite these drawbacks, the Cisco Catalyst 3850 is a dependable and efficient choice for medium-scale network environments.

6. Patch Panel-48

A 48-port patch panel is a networking device used to organize and manage cables. It acts as a central point where cables from devices like computers and servers are terminated and connected to other parts of the network. With 48 ports, it allows for easy connection, disconnection, and troubleshooting of network devices. Patch panels help streamline cable management, making it simpler to upgrade or maintain the network without accessing individual devices.

Model	 **NKPP48FMY**	 **PR175SC48-SM**
Port	48	48
Features	• **Type:** Cat5e/Cat6 patch panel.. • **Mounting**: 2U rackmount design for standard 19-inch racks. • **Use**: Suitable for Ethernet networking.	• **Type:** SC fiber patch panel for multi-mode fiber. • **Mounting:** 1U rackmount design for 19-inch racks. • **Use**: Designed for fiber optic networking with SC connections
Durability	• Built for standard Ethernet connections. • Constructed with metal housing for strength and longevity. • Less susceptible to environmental factors, as it's designed for	• Designed for fiber optic applications, so it’s built to withstand more delicate fiber optic cables. • Metal housing ensures stability, but it's more sensitive to handling

	typical office or data center environments.	than Ethernet panels due to the nature of fiber. ● Suitable for indoor use in controlled environments, typically used in data centers or telecommunications.
Price	RM 525.67	RM683.950
References	https://my.element14.com/panduit/nkpp48fmy/patch-panel-cat5e-cat6-48port/dp/2706537	https://my.element14.com/l-com/pr175sc48-sm/patch-panel-sc-sm-48port-1u/dp/2947276

The most suitable patch panel for our networking needs is the NKPP48FMY, chosen for its extensive port capacity, durable construction, and versatile features. This patch panel offers 48 ports, making it ideal for managing Ethernet networking connections using Cat5e or Cat6 cables. It provides a high-density solution for medium to large network environments, where efficient organization and reliable connections are essential.

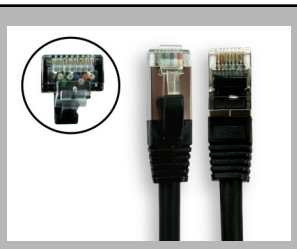
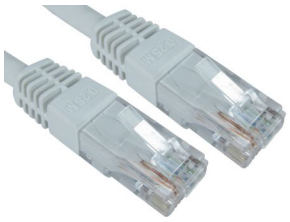
The NKPP48FMY is designed with a 2U rackmount configuration, making it compatible with standard 19-inch racks, which are commonly used in server rooms, data centers, and network closets. This design ensures that the patch panel fits seamlessly into the existing infrastructure, facilitating a neat and organized setup for Ethernet cabling.

In terms of durability, the NKPP48FMY is built specifically for Ethernet connections, making it suitable for both office and data center environments. Its metal housing provides enhanced strength and longevity, offering protection against wear and tear, and ensuring reliability even in high-traffic areas. The robust construction also makes it less sensitive to handling, reducing the risk of damage during installation and maintenance.

Overall, the NKPP48FMY patch panel offers a reliable, space-efficient solution for organizing Ethernet networks, ensuring long-term performance and ease of use in both small and large-scale network environments.

7. Ethernet Cable

An Ethernet cable is a type of network cable used to connect devices like computers, routers, switches, and modems in a wired local area network (LAN). It transmits data through copper wires and comes in various categories (e.g., Cat5e, Cat6, Cat8), with each offering different speeds and bandwidth capacities. Ethernet cables provide a stable, high-speed connection and are commonly used for reliable internet access and file sharing in home and office networks.

Model	 **RS PRO, 10m Cat8, Black RJ45 to Male RJ45 Male, S/FTP, Terminated LSZH Sheath**	 **RS PRO, 7m Cat6, White RJ45 to Male RJ45 Male, UTP, Terminated PVC Sheath**	 **RS PRO, 1.5m Cat6a, Blue RJ45 to Male RJ45 Male, S/FTPShielded**
Bandwidth	2000Mhz	600Mhz	500 Mhz
Transmission Speed	25/40Gbps	10Gbps	10Gbps
Transmission Distance	30m	100m	100m
Shielding Type	Shield	Shield	Shield/Unshield
Price	RM 162.13(10m)	RM57.08(7m)	RM28.73(1.5m)
References	https://my.rs-online.com/web/p/ethernet-cable/2761131?gb=s	https://my.rs-online.com/web/p/ethernet-cable/2646549	https://my.rs-online.com/web/p/ethernet-cable/2515168

We have chosen the RS PRO 10m Cat8 Ethernet cable for its exceptional performance and advanced features, making it the ideal choice for our network infrastructure. With a bandwidth of 2000 MHz and a transmission speed of 25/40 Gbps, this cable is designed to support ultra-fast data transfer and

high-performance networking, ensuring future-proofing for emerging technologies. Its S/FTP (Shielded/Foiled Twisted Pair) design provides robust protection against electromagnetic interference (EMI), ensuring stable and reliable connections, which is critical in a high-density environment like ours. The cable is terminated with an LSZH (Low Smoke Zero Halogen) sheath, enhancing safety by minimizing toxic smoke and emissions in the event of a fire, making it compliant with stringent safety standards. While it is priced at RM162.13, its durability, superior shielding, and advanced capabilities justify the investment, particularly for high-traffic or critical network areas where performance and reliability are paramount. This choice aligns with our commitment to building a robust and future-ready network infrastructure.

8. Ethernet Connector

An Ethernet connector, often referred to as an RJ45 connector, is a small device used to join Ethernet cables to network devices such as computers, routers, switches, and modems. It features eight metal pins that align with the individual wires inside the Ethernet cable, allowing for data transmission between devices in a network. Ethernet connectors are typically used with twisted-pair cables (like Cat5e or Cat6) and are essential for establishing a wired network connection, ensuring stable and fast data transfer.

Model	 **Cat8 Ethernet Cable Connector RJ45**	 **J00-0045NL PulseJack Right Angle 1x1 Modular Connectors - 100Base RJ45 Magnetics**
Bandwidth	Supports up to 2 GHz	Typically supports up to 100 MHz
Shielding	shielded	unshielded
Material	high-quality metal (gold-plated pins)	Plastic housing with magnetic components (for signal processing) and metal contacts for the connection
Durability	Built for high-performance networking, these connectors are designed for long-lasting use in environments where high-speed transmission is required.	These connectors are designed for lower-speed networks and are less robust compared to Cat8 connectors.

Price	RM 8.58	RM 11.23
References	https://www.globalsources.com/Modular-jack/Cable-Connector-1200681989p.htm	https://www.rj45-modularjack.com/sale-7295873-j00-0045nl-pulsejack-right-angle-1x1-modular-connectors-100base-rj45-magnetics.html

The most suitable Ethernet connector for our needs is the Cat8 Ethernet Cable Connector RJ45, chosen for its excellent bandwidth, superior shielding, durable materials, and overall reliability. With the best bandwidth for high-speed networking, it supports the highest data rates and frequencies, ensuring maximum performance for demanding applications.

The connector provides effective shielding, offering enhanced protection against electromagnetic interference (EMI), which is crucial in maintaining stable performance in high-noise environments. Its durable and reliable materials help preserve signal integrity, reduce loss, and ensure a strong, uninterrupted connection. Additionally, the connector is designed for long-lasting use, making it ideal for environments that require high-speed transmission and consistent performance over time. These features make the Cat8 Ethernet Cable Connector RJ45 the ideal choice for high-performance networking setups.

9. Faceplate

A faceplate is a device used to mount and secure network or electrical outlets on a wall or surface. In networking, it typically holds Ethernet jacks or other connectors, providing a clean and organized way to manage cables and maintain a professional appearance in a network setup. Faceplates can be single or multi-port, depending on the number of connections needed, and are often made of plastic or metal for durability. They help protect the connectors and ensure a secure and tidy installation, especially in office or data center environments.

Model	 **NK1FWHY**	 **NK2FNIW**	 **RJ45 Face Plate Premium Socket**
Port Capacity	single	dual	single or multiple
Type	standard RJ45 faceplate or socket	dual RJ45 faceplate or socket	Premium RJ45 socke
Material	plastic	plastic	High-quality plastic, with metal contacts
Application	home or office environments for basic networking setups.	dual-port Ethernet connections in networking setups requiring multiple outlets in one plate.	high-performance environments such as data centers or commercial installations
Price	RM 18.26	RM 18.33	RM39.38

References	https://my.element14.com/panduit/nk1fwhy/vertical-faceplate-1-module-white/dp/1316470	https://my.element14.com/panduit/nk2fniw/vertical-faceplate-2-module-white/dp/2707041	https://www.ebay.com.my/itm/224584723572

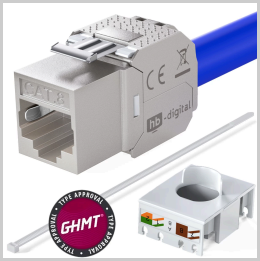
The most suitable faceplate for our needs is the RJ45 Face Plate Premium Socket, selected for its dual-port capacity, high-quality materials, and versatile application. It provides dual Ethernet connections in a single plate, making it ideal for more advanced setups that require multiple connections in a single location, allowing for enhanced network flexibility.

The dual-port design not only adds extra functionality but also maintains a premium quality, ensuring that multiple devices can be connected without compromising performance. This configuration is perfect for spaces where more than one Ethernet connection is needed but a sleek, high-end design is still desired.

Made from premium plastic, the faceplate offers enhanced durability and a polished finish, while the metal contacts ensure stable, high-quality connections. The RJ45 Face Plate Premium Socket is well-suited for businesses and larger networking environments, where a high-end, efficient, and aesthetically pleasing solution is required to manage multiple connections from a single faceplate.

10. Keystone Jack Panel

A keystone jack panel is a type of patch panel designed to hold keystone jacks, which are modular connectors used to terminate Ethernet cables and other network wiring. These panels allow for easy organization and management of network connections in a structured cabling system. Keystone jacks can be inserted into the panel, providing a neat and flexible solution for managing multiple network ports. The keystone jack panel is typically mounted in a server rack or wall-mounted enclosure and is used to connect various devices like computers, switches, and routers, offering a convenient point for cable management and quick connection changes.

Model	 **RJ45 Cat 8.1 Tool-less Keystone Jack**	 **SKMCBKPM**
Bandwidth	up to 25/40 Gbps	up to 1 Gbps
Installation	Tool-less, making it easy for fast installation	Requires a 110 or Krone termination tool for installation
Shielding	shielded	Unshielded
Material	premium plastic materials	UL94V-0 rated ABS plastic housing
Price	RM 37.14	RM29.05
References	https://www.hb-digital.de/100-Pcs-Keystone-module-RJ45-CAT-81-GHMT-certified-LSA-tool-less-rj45-keystone-jack	https://my.element14.com/tuk/skmcbkpm/keystone-rcpt-rj45-cat6-8p8c-black/dp/2534594?&CMP=KNC-GMY-GEN-SHOPPING-

		PERF-MAX-V1&mckv=_dc|pcrid||pkw||pmt||slid||product|2534594|pgrid||ptaid||&gad_source=1&gclid=CjwKCAiAjp-7BhBZEiwAmh9rBZkSLZGX-p8ez0uuMFeQXccLV2i1ColS1Jbmv9nQsiO4Y8eOdYSe8RoCch8QAvD_BwE

The most suitable keystone jack panel for our needs is the RJ45 Cat 8.1 Tool-less Keystone Jack, chosen for its superior bandwidth, easy installation, and enhanced shielding. The Cat 8.1 keystone jack offers high bandwidth capabilities, supporting speeds up to 25 Gbps, making it perfect for high-speed, high-demand networking environments, unlike lower bandwidth options that only support 1 Gbps for basic applications.

Its tool-less installation design simplifies setup, eliminating the need for specialized termination tools, which can be time-consuming and complicated, as required by other jacks. The keystone jack is built with effective shielding, ensuring superior protection against electromagnetic interference (EMI), which helps maintain signal integrity and performance in noisy environments.

Additionally, the RJ45 Cat 8.1 Tool-less Keystone Jack is made from durable, high-quality materials, offering better durability, fire resistance, and overall longevity compared to basic plastic options. This combination of features makes it a reliable and future-proof solution for advanced networking setups.

11. Network Management Devices

Network management devices are tools and equipment used to monitor, manage, and optimize network performance, ensuring smooth and efficient operation. These devices help network administrators identify and resolve issues, track network traffic, and configure settings across various network components.

Model	 **APC SRT8KXLI 230V Input Rack Mount UPS - 8000VA (8kW)**	 **SMART1500LCDT**
Power Capacity	8000VA (8kW)	1500VA
Input Voltage	230V	120V
Processor	Advanced, enterprise-level	Basic, suited for home/office use
Memory	Larger memory for monitoring	Smaller memory for basic use
Application	Large systems, data centers	Home/small office networking
Features	Smart monitoring, rack-mountable	LCD display, AVR, compact
Shielding	High-performance, shielded	Basic power protection
Price	RM50,253.54	RM1,436.68
References	https://my.rs-online.com/web/p/uninterruptible-power-supplies/2877928?cm_mmc=MY-PLA-DS	https://www.digikey.my/en/products/detail/tripp-lite/SMART1500LCDT/4439114?srsltid=AfmB

	3A-_-google-_-PLA_MY_EN_PMAX_High+Impression_20240118-_--_-&matchtype=&&ads_rl=8558441598&&&&gad_source=1&gclid=CjwKCAiA9bq6BhAKEiwAH6bqoKH7CgswDQlmeP27P_5ijFnFXzFHktzrR9Ba6J2nTYvtGEpTwZcRThoC6EYQAvD_BwE&gclsrc=aw.ds	Oopbnp4wkqfErGsZC2KEig83f2dhZbB3KDWs5jppfb8_nMuXTRD5

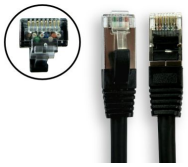
The most suitable network management device for our needs is the APC SRT8KXLI 230V Input Rack Mount UPS - 8000VA (8kW), selected for its high power capacity, advanced monitoring features, and space-efficient design. With a high power capacity of 8000VA, it is ideal for large systems, data centers, and enterprise-level applications, providing reliable support for high-power demanding equipment such as servers and network hardware.

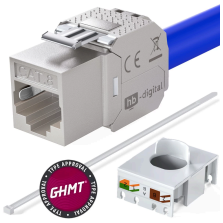
The 230V input is well-suited for international applications, particularly in regions where 230V power systems are standard, ensuring compatibility across different locations. The UPS is powered by a high-end processor designed for smart monitoring and efficient power distribution management, essential for large-scale environments. It also features advanced memory and monitoring capabilities, enabling real-time tracking of power usage, battery health, and UPS status, which is critical for enterprise environments.

The rack-mountable design enhances space efficiency in server racks, making it ideal for data centers and server rooms. It offers smart monitoring tools that track UPS health, power metrics, and provide detailed insights into performance. Additionally, the high-performance shielding ensures better protection for sensitive equipment, safeguarding it from electrical surges, interference, and power disruptions. These features make the APC SRT8KXLI UPS a reliable and efficient solution for managing power in enterprise-level network environments.

5.2 EXPECTED COST

Component	Model	Price per unit(RM)	Quantity	Total Price(RM)
 Server	**Dell EMC PowerEdge T640 Tower Server**	28,821.00	50	1,441,050.00
 Router	**S5860-24XB-U is FS**	17,594.00	2	35,188.00
 Firewall	**FPR2140-NGFW K9 - Cisco Firepower 2100 Series Appliances**	116,195.92	1	116,195.92
 Wireless Access Point (WAP)	**NETGEAR WEB 758-111 NAS WiFi 7**	7,422.00	2	14,844.00

 Switch	**WS-C3850-48XS -S Catalyst 3850 Switch SFP+**	75,615.59	15	1,134,233.85
 Patch Panel	**NKPP48FMY**	525.67	15	7,885.05
 Ethernet Cable	**RS PRO, 10m Cat8, Black RJ45 to Male RJ45 Male, S/FTP, Terminated LSZH Sheath**	162.13	52	8,430.76
 Ethernet Connector	**Cat8 Ethernet Cable Connector RJ45**	8.58	500	4,290.00
 Faceplate	**RJ45 Face Plate Premium Socket**	39.38	70	2,756.60

 Keystone Jack Panel	**RJ45 Cat 8.1 Tool-less Keystone Jack**	37.14	96	3,565.44
 Network Management Devices	**APC SRT8KXLI 230V Input Rack Mount UPS - 8000VA (8kW)**	50,253.54	2	100,507.08
 Cap Rubber Boot	**MTP-88-C8-SR-A 3**	0.45	500	225
			Total	2,869,171.70

Budget Calculation

Budget = RM 3,000,000.00

Total spend = RM 2,869,171.70

Balance = RM 3,000,000.00 - RM 2,869,171.70

= RM 130,828.30

5.3 REFLECTION

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

Yes, we were quite surprised by the prices of network devices such as servers, routers, switches, and firewalls. The costs were significantly higher than what we initially anticipated, particularly for devices equipped with advanced features like extended range options, enhanced security measures, and robust integration capabilities. The steep price tags reflect the sophistication and reliability of these devices, but they were beyond our initial budget expectations.

What stood out the most was the investment required for features that ensure long-term network efficiency, such as high-speed performance, scalability, and robust security mechanisms. While the initial costs may appear overwhelming, these devices often justify their price through long-term savings. For instance, their durability, dependable performance, and ability to minimize network downtime contribute to operational efficiency and reduce maintenance expenses over time.

In conclusion, although the prices were surprising, understanding the added value and potential cost savings these devices offer helps us appreciate why they are priced at a premium. Their features and benefits ultimately make them worthwhile investments for creating a high-quality and reliable network infrastructure.

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

Yes, of course. Cost is always a critical factor especially when the budgets are limited and tight. However, the decision will include maintenance, scalability, energy efficiency and expected lifespan. A device with higher initial costs but lower maintenance requirements may be more cost effective in the long run term.

5.3.3 What are the major differences between the same devices from different brands?

When comparing switches from Cisco and Huawei, several distinctions arise in terms of performance, scalability, and cost. Cisco switches are known for their robust features, including advanced VLAN management, superior Quality of Service (QoS), and enhanced network security. These features cater to large enterprises that demand high reliability and scalability. Cisco's switches also utilize the Cisco IOS operating system, which is praised for its consistency and extensive support. In contrast, Huawei switches offer a more cost-effective alternative while still delivering competitive features such as high port density and energy efficiency. Huawei's VRP (Versatile Routing Platform) is user-friendly but might lack the advanced options available in Cisco IOS. Moreover, Huawei switches are popular in budget-conscious markets due to their lower price point and comparable performance for medium-scale implementations (Networkise, n.d.; Lia, 2020).

Servers

(Dell PowerEdge Rack Servers and Huawei FusionServer RH Series Rack Servers)

When comparing Dell PowerEdge Rack Servers and Huawei FusionServer RH Series Rack Servers, the first major factor to consider is performance and scalability. Both brands offer Intel Xeon Scalable processors, ensuring strong performance for a variety of workloads. Dell PowerEdge is well-known for its robust performance and enterprise reliability, making it an excellent choice for businesses with established IT infrastructures. Dell's OpenManage management tools further enhance its ability to integrate with other Dell products, making it easier for IT teams to manage complex systems. On the other hand, Huawei FusionServer RH Series excels in providing flexible scalability, making it a great choice for businesses requiring scalable solutions in cloud computing, big data, and AI applications.

In terms of cost-effectiveness, Huawei FusionServer RH Series offers a budget-friendly solution, particularly appealing to companies with limited resources or those looking to scale their infrastructure at a lower cost. Huawei's focus on cost-effective performance allows businesses to grow without overspending on enterprise-level hardware. This makes the FusionServer RH Series especially suitable for small and medium-sized enterprises (SMEs) or those operating in data-intensive environments such as cloud computing and AI workloads. Conversely, Dell PowerEdge, while higher in price, justifies the cost with superior reliability, enterprise-class integration, and extensive support services. For companies heavily invested in the Dell ecosystem, the added cost is often seen as an investment in long-term performance and support

Finally, expandability and integration are essential for businesses looking to grow their IT infrastructure. Huawei FusionServer RH Series provides highly scalable solutions, designed to handle dense data center computing and software-defined storage, ensuring that businesses can expand without replacing their hardware as their needs grow. Huawei's servers also provide a good balance of performance and flexibility at a competitive cost, making them ideal for businesses focused on maximizing value. Dell PowerEdge, however, is known for its seamless integration with other Dell products, which is particularly beneficial for larger enterprises or those already using Dell's networking and storage systems. Dell's comprehensive support, along with its high reliability in mission-critical environments, makes it the go-to choice for businesses that require consistent uptime and enterprise-level security.

Routers

(Cisco C8500-12X and the S5860-24XB-U is FS)

From our perspective, Cisco C8500-12X and FS S5860-24XB-U are ideal networking devices which are designed for specific purposes. Cisco C8500-12X is excellent for large business applicability with the complex network. It provides 12x1G Ethernet ports with advanced routing and strong security that makes it perfect for companies that need reliable WAN connections and secure VPNs package with smooth application performance. Cisco's reputation for reliability and network security further strengthens its appeal. However, its solutions often come with a higher price tag and additional licensing requirements, which can increase overall costs over time.

On the other hand, the FS S5860-24XB-U is a versatile Layer 3 managed switch that offers exceptional performance and flexibility, especially for data centers and modern enterprise networks. With 24x10G SFP+ ports and 4x100G uplinks, it delivers superior switching power, making it ideal for high-speed data transmission and scalable networking. FS devices are known for their open compatibility with third-party hardware, which allows for greater interoperability compared to Cisco's proprietary ecosystem. Additionally, FS solutions are more cost-effective, with many advanced features included without extra licensing fees, making them a budget-friendly choice for organizations.

Choosing the FS S5860-24XB-U is a smart decision for organizations seeking an affordable yet powerful networking solution. Its combination of high-speed ports, scalability, and cost-effectiveness makes it well-suited for data centers and modern enterprise LAN setups. While the Cisco C8500-12X remains a reliable router for specific high-security applications, the FS S5860-24XB-U stands out as the more practical choice for those focused on performance and value in switching infrastructure.

Firewalls

(Cisco Firepower 2140 and the Fortinet FortiGate 500E)

The Cisco Firepower 2140 and the Fortinet FortiGate 500E are both advanced next-generation firewalls (NGFWs) designed to offer robust security for enterprise environments, but they cater to different needs. The Cisco Firepower 2140 is equipped with Cisco's Firepower Threat Defense (FTD) software, providing integrated firewalling, intrusion prevention systems (IPS), URL filtering, and application control in a unified platform. It offers deep visibility into network traffic, advanced threat protection, and secure network segmentation, making it ideal for businesses already within the Cisco ecosystem. Its advanced security capabilities, such as deep packet inspection, automated response mechanisms, and VPN support, make it suitable for critical infrastructure protection (Cisco Systems, n.d., retrieved December 4, 2024).

On the other hand, the FortiGate 500E is powered by Fortinet's FortiOS and focuses on high-performance security with a strong emphasis on throughput and scalability. It combines several security features such as intrusion prevention, web filtering, and advanced threat protection, making it a powerful choice for organizations with high-speed, low-latency requirements. Additionally, the FortiGate 500E supports SD-WAN, VPN, and network analytics, offering flexibility for distributed network environments (Fortinet, n.d., retrieved December 4, 2024).

While both firewalls provide comprehensive security features, the Cisco Firepower 2140 stands out in terms of quality due to its deep integration with Cisco's broader security ecosystem, making it the ideal choice for enterprises seeking a unified security approach. Its advanced threat detection capabilities, seamless integration with other Cisco security tools, and centralized management features offer unparalleled network visibility and control. In comparison, the Fortinet FortiGate 500E, while excelling in performance and scalability, lacks the same level of integration with other enterprise security solutions. Therefore, based on quality, the Cisco Firepower 2140 is the superior choice for organizations focused on comprehensive threat management and long-term network security.

Wireless Access Points

(The Netgear WBE758-111NA vs Aruba AP-505 US)

The Netgear WBE758-111NAS and the Aruba AP-505 US are both high-quality Wi-Fi access points designed to provide seamless wireless connectivity for enterprise environments. The Netgear WBE758-111NAS is an Insight Managed Wi-Fi 7 access point, supporting advanced features such as high-speed wireless performance, secure guest networks, and easy integration with Netgear's Insight platform. This device is designed for environments that demand strong coverage, high throughput, and simplified management, which makes it an ideal choice for businesses seeking a reliable and scalable solution. The Netgear WBE758 supports Wi-Fi 7 technology, ensuring it delivers the latest performance standards, including enhanced data speeds, lower latency, and better efficiency compared to previous generations (NetworkHardwares, n.d., retrieved December 4, 2024).

In comparison, the Aruba AP-505 US from Aruba Networks is a Unified Access Point designed to support high-performance, secure, and reliable connectivity for a range of applications. It features Aruba's advanced wireless technologies and management tools, ensuring enterprise-grade performance in a variety of environments. The Aruba AP-505 focuses on offering high-speed Wi-Fi 6 (802.11ax) performance, along with enhanced security features like integrated WPA3 and robust encryption options. It is particularly beneficial for businesses needing high-density environments and scalability with easy cloud-based management through Aruba Central (NetworkHardwares, n.d., retrieved December 4, 2024).

While both devices offer strong wireless performance and security, the Netgear WBE758-111NAS stands out due to its support for Wi-Fi 7, which promises superior speeds, lower latency, and improved efficiency. This makes the Netgear WBE758-111NAS the better choice for businesses looking for cutting-edge technology, future-proofing their wireless network with the latest standard for maximum performance and scalability. On the other hand, the Aruba AP-505 offers a solid solution with excellent security and performance for businesses already invested in the Aruba ecosystem but lacks the advanced capabilities of Wi-Fi 7. Therefore, based on quality, the Netgear WBE758-111NAS is the better option due to its superior technology and future-readiness.

Switch

(WS-C3850-48XS-S Catalyst 3850 Switch SFP+ and R0X27A - Aruba 6410)

When evaluating networking equipment from various manufacturers, several important factors should be taken into account like performance, price, user-friendliness, and scalability. To evaluate performance, consider elements such as the kinds of ports, switching capacity, and the device's ability to accommodate future expansion. Certain brands, such as Cisco, work seamlessly with their own products, which is beneficial if you are already utilizing Cisco devices. FS, conversely, emphasizes compatibility with different brands, providing greater flexibility.

Cost is another big factor. Cisco products are usually more expensive and may require extra licenses for advanced features. FS tends to offer more features at a lower price, with fewer extra costs. In terms of ease of use, Cisco’s devices have powerful features but may need skilled IT staff to manage. FS devices often have simpler interfaces that are easier for everyday users. Scalability is also important for some brands, able to expand easily, while others might have fixed setups that limit growth. Support and warranty options can differ too, with Cisco offering more comprehensive services, but at a higher price.

In conclusion, the right device depends on what you need most. If you want high performance and integration with Cisco products, Cisco might be the better choice. But if you’re looking for a more affordable, flexible, and easy-to-manage solution, FS could be the better fit. It’s all about balancing performance, cost, and ease of use based on your needs

Patch Panel 48

(NKPP48FMY and PR175SC48-SM)

The decision regarding devices from various brands ultimately depends on the particular requirements of our network. We selected the NKPP48FMY patch panel due to its high port capacity, robust build, and compatibility with standard rack mounts, making it perfect for medium to large networks.

Although other brands may present comparable features, the NKPP48FMY distinguishes itself with its sturdy construction and dependability, delivering an economical option for effective Ethernet network management. This decision guarantees long-lasting performance, user-friendliness, and smooth incorporation into current infrastructure.

Ethernet Cable

(RS PRO,Cat8, Black RJ45 Terminated LSZH Sheath, RS PRO, Cat6, RJ45 UTP and RS PRO Terminated PVC Sheath, Cat6a, RJ45, S/FTPShielded)

The RS PRO 10m Cat8 Ethernet cable distinguishes itself from other choices because of its exceptional blend of high bandwidth, rapid transmission speeds, and strong shielding. Although other brands might provide Ethernet cables with comparable characteristics, the RS PRO cable stands out with a bandwidth of 2000 MHz, the highest in this category.

The RS PRO cable is built for high-speed, high-performance tasks. With speeds of 25/40 Gbps, it ensures quick and efficient data transfer, making it perfect for modern data centers and busy network environments. The cable's S/FTP shielding provides extra protection against electromagnetic interference (EMI), helping to keep the signal clear and strong, even in areas with a lot of electrical noise.

The LSZH sheath makes the RS PRO cable safer and more environmentally friendly. These important features make it the best choice, as it meets the high standards required for fast and reliable network setups, offering better performance and dependability than other brands

Ethernet Connector

(Cat8 Ethernet Cable Connector RJ45 and J00-0045NL PulseJack Right Angle 1x1 Modular Connectors)

We chose the Cat8 Ethernet Cable Connector RJ45 because it offers the best combination of high bandwidth, effective shielding, and durable materials, ensuring optimal performance in demanding network environments. Its ability to support high data rates and frequencies makes it ideal for high-speed networking, while its enhanced protection against electromagnetic interference (EMI) ensures stable performance even in noisy settings. The connector's reliable and long-lasting materials preserve signal integrity and reduce loss, making it a strong, uninterrupted choice for high-performance networking setups. These key features make it the best option for meeting the rigorous demands of high-speed, high-performance applications.

Faceplate

(NK1FWHY, NK2FNIW and RJ45 Face Plate Premium Socket)

We chose the RJ45 Face Plate Premium Socket due to its ideal combination of functionality, quality, and aesthetics. The dual-port capability offers versatility by accommodating several Ethernet connections in a single area, making it perfect for sophisticated configurations that need effective space utilization.

We chose the RJ45 Face Plate Premium Socket due to its ideal combination of functionality, quality, and aesthetics. The dual-port capability offers versatility by accommodating several Ethernet connections in a single area, making it perfect for sophisticated configurations that need effective space utilization.

Keystone Jack Panel

(RJ45 Cat 8.1 Tool-less Keystone Jack and SKMCBKPM)

We chose the RJ45 Cat 8.1 Tool-less Keystone Jack because it provides the perfect combination of high performance, ease of use, and durability. With its ability to support speeds up to 25 Gbps, it meets the demands of high-speed, high-performance networks, unlike lower-bandwidth alternatives. The tool-less design makes installation quick and easy, saving time and effort compared to other jacks that need special tools. It also has excellent shielding to protect against electromagnetic interference (EMI), ensuring the signal stays strong and clear even in noisy environments. Built with durable, fire-resistant

materials, it’s designed to last longer and perform reliably, making it a smart, future-proof choice for high-demand networking setups.

Network Management Devices

(APC SRT8KXLI 230V Input Rack Mount UPS - 8000VA and SMART1500LCDT)

We chose the APC SRT8KXLI 230V Rack Mount UPS because it offers the perfect combination of high power, smart monitoring, and space efficiency. With an 8000VA capacity, it’s built to support large systems like servers and network hardware in demanding environments such as data centers. The 230V input makes the APC SRT8KXLI perfect for use anywhere, so it’s always ready no matter where you are. With its smart processor and real-time monitoring, you can easily keep track of power usage, battery health, and the overall status of the UPS—helping to ensure everything runs smoothly in a business setting. The rack-mountable design is a great space-saver in server racks, and its strong shielding keeps your sensitive equipment safe from power surges and interruptions. With all these features, the APC SRT8KXLI is a trustworthy and efficient choice for managing power in large network environments.

REFLECTION TASK 3

For task 3, it is involved in deep research and decision making to select the appropriate network and end user devices to meet the objectives of the Faculty of Computing. This process required us to understand the various network devices such as routers, switches, patch panels, wireless devices, and cables, and to compare different brands like Cisco, Huawei, and Asus. Our goal is to select devices that have a best fit in an academic institution and balance technical requirements with budget constraints. By conducting thorough research and discussions, we identified key devices and gathered detailed information about their specifications, capabilities, and pricing, and made informed decisions. This task highlighted the importance of meticulous research, clear documentation, and strategic thinking in project planning and execution. It also emphasized the need to consider cost as a critical factor and to understand the major differences between similar devices from different brands. Overall, the experience gave us the ability to effectively plan and implement network infrastructure, reinforcing the importance of collaboration and thorough preparation in achieving project objectives.

6.0 MAKING THE CONNECTION

6.1 WORK AREA ON THE FLOOR PLAN

6.1.1 GROUND FLOOR

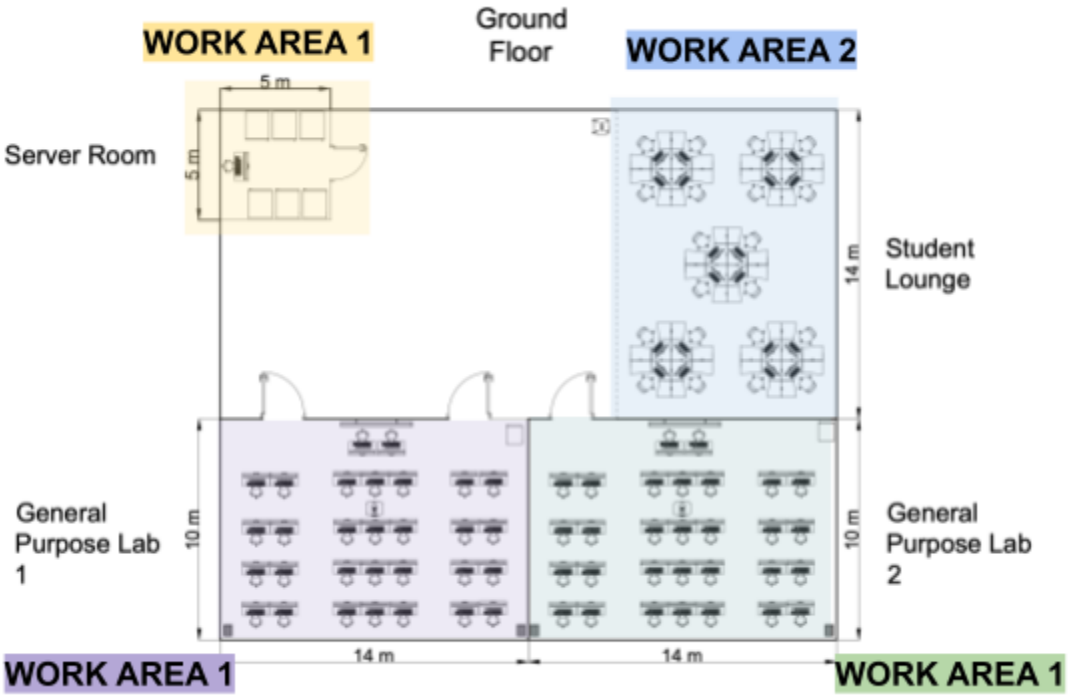


Figure 6.1.1 Work Area Ground Floor

The ground floor plan of the new building of Faculty Computing comprises four distinct work areas with its own specific function. These areas include Server Room which is the first work area, Student Lounge which is the second work area, General Purpose Lab being the third work area, and lastly the general purpose lab 2 being the fourth work area. The Server Room houses critical IT equipment like servers and networks to ensure smooth computing operations. The Student Lounge provides a comfortable space for students to relax, socialize, or collaborate informally. General Purpose Lab 1 and General Purpose Lab 2 are computer labs equipped for classes, projects, and research, offering ample space for academic activities. Together, these areas support the faculty's teaching, learning, and technical requirements.

6.1.1.1 SERVER ROOM

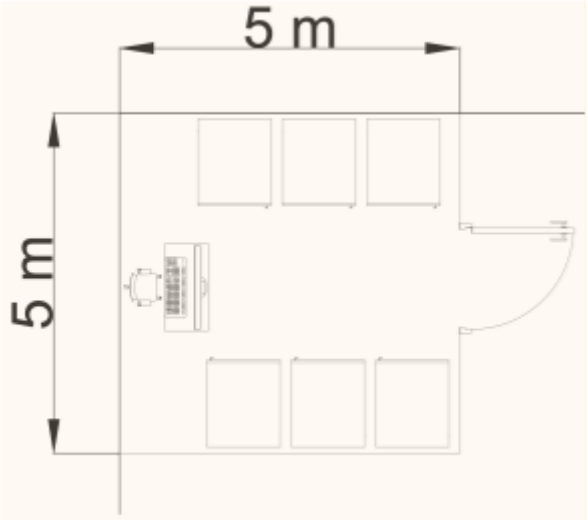


Figure 6.1.1.1 Work Area 1, Server Room

Work Area 1, known as the Server Room, serves as the main network hub for the building and is equipped with a Dell EMC PowerEdge T640 Tower Server. This is due to its dependability and ability to manage challenging tasks. The server provides centralized storage, data organization, and effective resource allocation for all linked workstations

A Cisco C8500-12X switch manages the data flow between devices, enhancing network efficiency and ensuring seamless communication. Additionally, a dedicated management PC is available for monitoring and controlling server operations. The Server Room is designed to provide a stable and secure networking environment, supporting the faculty's teaching, learning, and administrative activities.

6.1.1.2 STUDENT LOUNGE

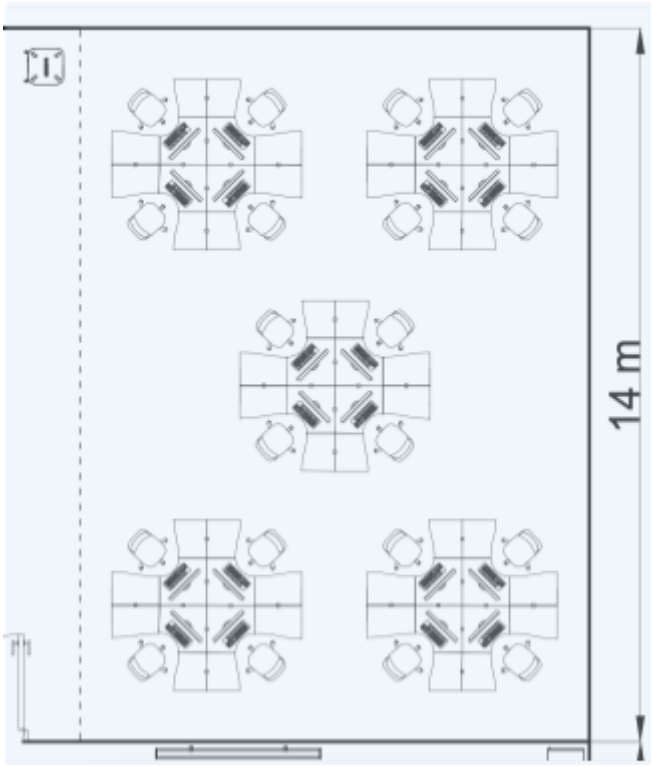


Figure 6.1.1.2 Work Area 2, Student Lounge

For Work Area 2, student lounges serve as shared workspaces with multiple devices requiring network access. There are a total 10 PCs, a network-enabled NETGEAR WEB 758-111 NAS WiFi 7 and charging station for mobile devices. The network layout utilizes cables RS PRO 7m Cat6 cables for horizontal connections which ensuring reliable speed up to 1 Gbps per devices that link to a WS-C3850-48XS-S Catalyst 3850 Switch SFP+, placed in the nearby telecommunications room to minimize cable lengths while maintaining an organized structure. Estimated total cable length is approximately 60 meters include allowances for wall-mounted routing and corner adjustments

Each device connects to the network through RJ45 Cat 8.1 Tool-less Keystone Jacks, plugged into wall jacks linked to the switch via structured cabling. An Access Point could be deployed to support mobile users and provide robust dual-band Wi-Fi coverage for the lounge. The NETGEAR NAS and USB charging stations add functionality, making the lounge suitable for collaborative and individual work. This setup ensures a high-performance, future-proof network for student activities.

6.1.1.3 GENERAL LAB 1

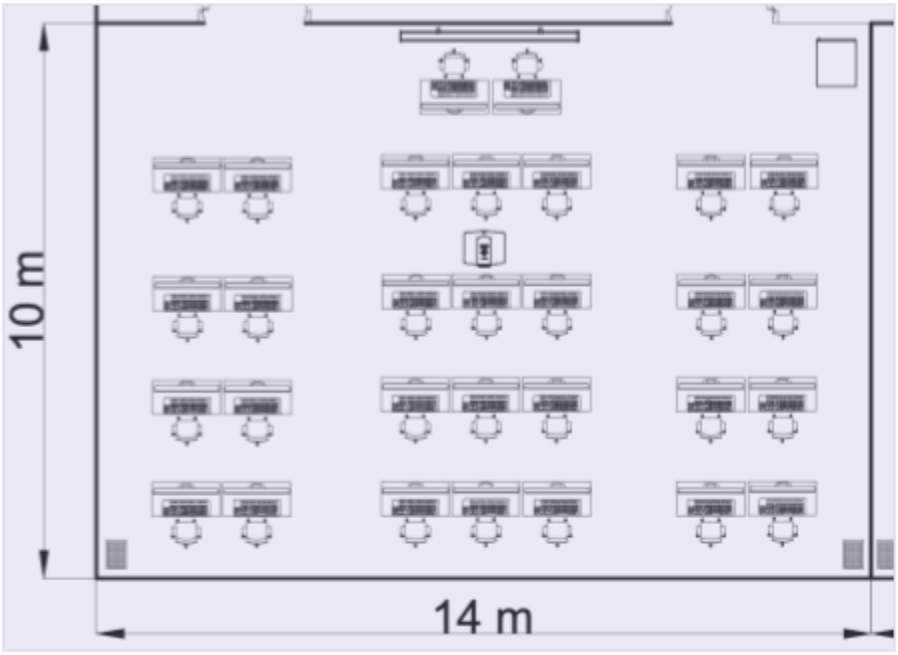


Figure 6.1.1.3 Work Area 3, General Lab 1

This lab is equipped with 30 PCs, a projector, and a speaker system, all designed to support an engaging and productive learning environment. The PCs provide individual workstations for students, enabling access to educational software, online resources, and collaborative tools. The projector facilitates visual presentations, making it ideal for lectures, demonstrations, and media sharing. The speaker system enhances audio quality for presentations and multimedia content, ensuring clear communication and an immersive experience during sessions. A server on top right corner, Dell EMC PowerEdge T640 Tower Server, which acts as the backbone, hosting files, applications, and centralized resources to ensure efficient data management and accessibility.

In addition to these components, the lab network is designed for seamless connectivity. The PCs are connected to the server and a NETGEAR PR175SC48-SM Wireless Access Point (WiFi 7) through a Cisco Catalyst WS-C3850-48XS-S Switch SFP+ and a patch panel, which simplifies cable management and future network expansions. The server provides centralized storage and resource management for both students and lecturers. The Wireless Access Point Supports Wi-Fi-enabled devices such as laptops and tablets, while the patch panel organizes connections efficiently. Together, this setup creates a robust and versatile environment to support diverse educational activities.

6.1.1.4 GENERAL LAB 2

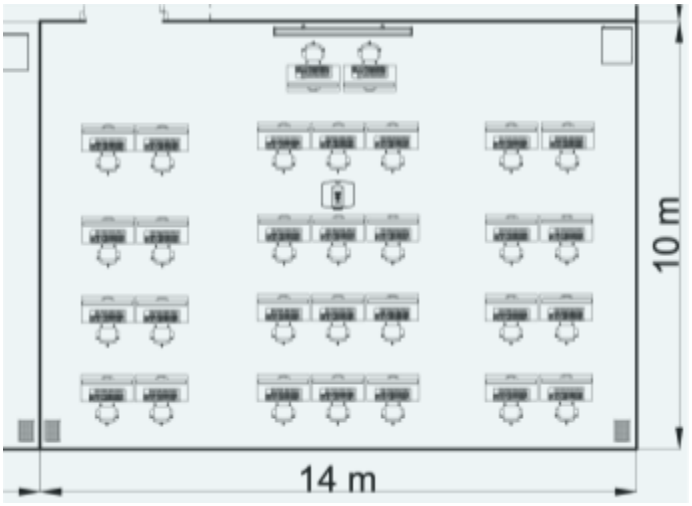


Figure 6.1.1.4 Work Area 4, General Lab 4

This lab is equipped with 30 PCs, a projector, and a speaker system, all designed to support an engaging and productive learning environment. The PCs provide individual workstations for students, enabling access to educational software, online resources, and collaborative tools. The projector facilitates visual presentations, making it ideal for lectures, demonstrations, and media sharing. The speaker system enhances audio quality for presentations and multimedia content, ensuring clear communication and an immersive experience during sessions. A server on the top right corner, Dell EMC PowerEdge T640 Tower Server, which acts as the backbone, hosting files, applications, and centralized resources to ensure efficient data management and accessibility.

In addition to these components, the lab network is designed for seamless connectivity. The PCs are connected to the server and a NETGEAR PR175SC48-SM Wireless Access Point (WiFi 7) through a Cisco Catalyst WS-C3850-48XS-S Switch SFP+ and a patch panel, which simplifies cable management and future network expansions. The server provides centralized storage and resource management for both students and lecturers. The Wireless Access Point Supports Wi-Fi-enabled devices such as laptops and tablets, while the patch panel organizes connections efficiently. Together, this setup creates a robust and versatile environment to support diverse educational activities.

6.1.2 FIRST FLOOR

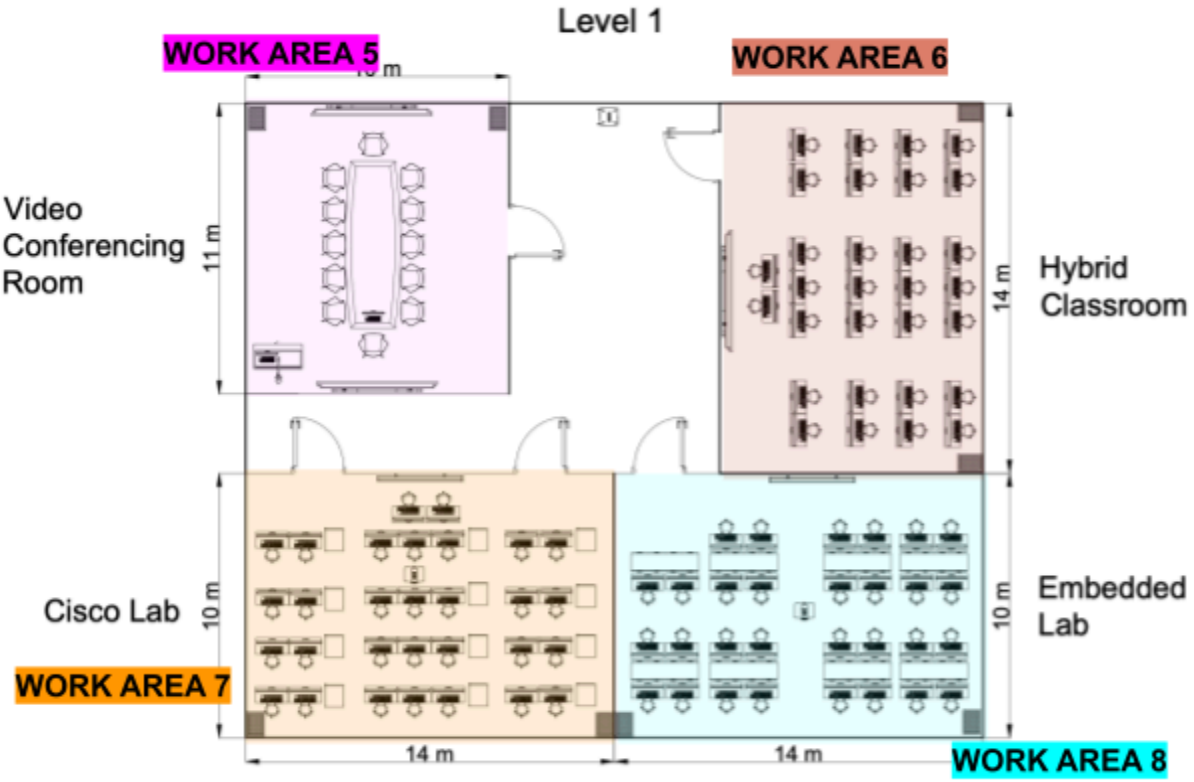


Figure 6.1.2 Work Areas First Floor

On the first floor, the new faculty building features another four work areas. Work Area 5 is the Video Conferencing Room, Work Area 6 is the hybrid classroom, Work Area 7 is the Cisco Lab, and work area 8 is the embedded lab. The Video Conferencing Room is equipped for virtual meetings, online classes, and remote collaboration. The Hybrid Classroom supports both in-person and online learning with interactive tools for effective teaching. The Cisco Lab provides hands-on training in networking, including configuring and troubleshooting Cisco equipment. The Embedded Lab focuses on embedded systems, offering resources for projects like microcontrollers and IoT devices. These areas are designed to support advanced learning and practical skills in technology.

6.1.2.1 VIDEO CONFERENCING ROOM

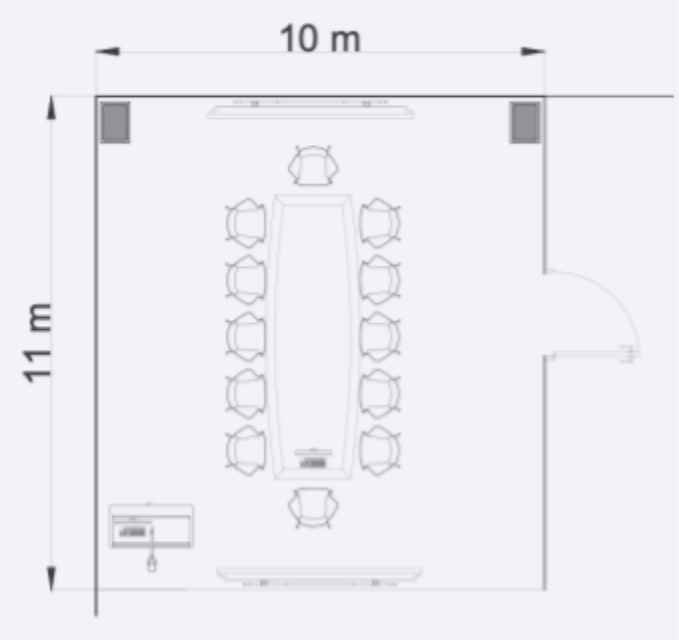


Figure 6.1.2.1 Work Area 5, Video Conferencing Room

Work Area 5, Video Conferencing Room is equipped with two PCs, two smartboards, and two speakers to ensure smooth communication. The two PCs allow for multitasking, such as managing presentations and troubleshooting. The two monitors enable viewing the conference on one screen while displaying additional content on the other. The two speakers provide clear, balanced audio for all participants.

A wireless access point, positioned 4 meters from the top-right corner, ensures strong and reliable Wi-Fi coverage. The NETGEAR WEB 758-111 NAS WiFi 7 supports high-speed connections for video calls, while the WS-C3850-48XS-S Catalyst 3850 Switch SFP+ expands the network and offers additional ports for connecting devices, maintaining a stable, efficient network for the room.

6.1.2.2 HYBRID CLASSROOM

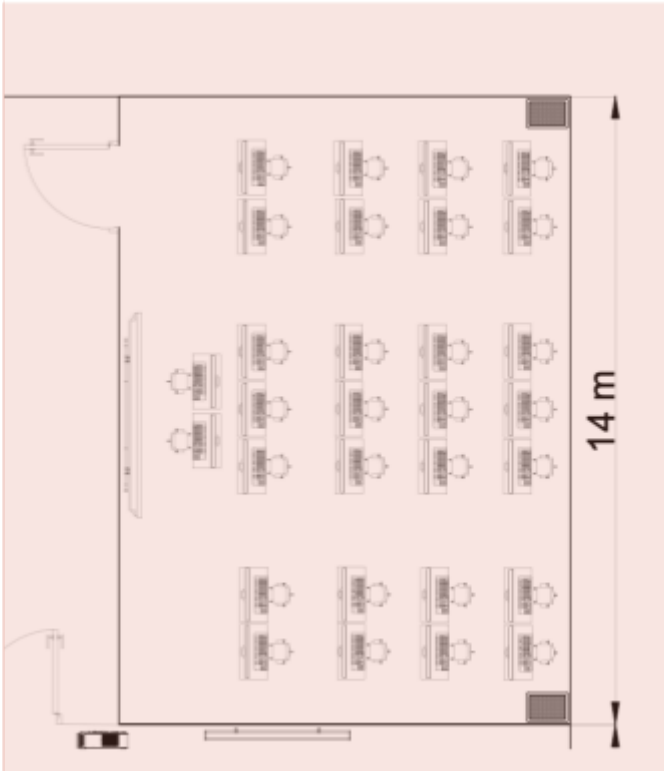


Figure 6.1.2.2 Work Area 6, Hybrid Classroom

In Work Area 6, the Hybrid Classroom, there are 30 PCs, two speakers, and one smartboard to support both in-person and remote learning. The 30 PCs give students access to the tools they need for coursework and collaboration. The two speakers ensure clear audio for remote communication and multimedia. The smartboard allows the instructor to interact with content, making lessons more engaging.

The Wi-Fi access point, located less than 4 meters from the top-left corner, provides strong connectivity for all devices. The NETGEAR WEB 758-111 NAS WiFi 7 ensures fast and reliable wireless connections, while the WS-C3850-48XS-S Catalyst 3850 Switch SFP+ manages network traffic and provides extra ports for devices, ensuring a stable, efficient network for the classroom.

6.1.2.3 CISCO LAB

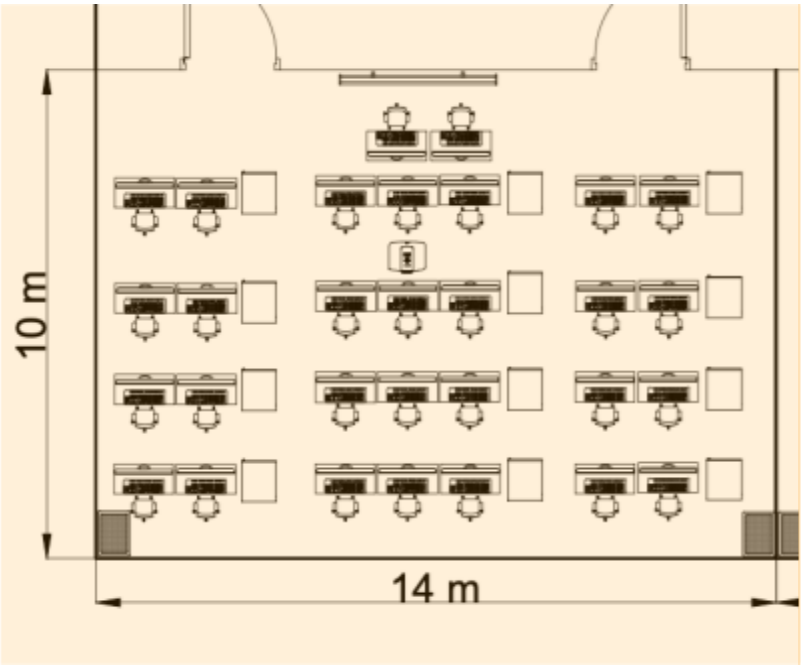


Figure 6.1.2.3 Work Area 7, Cisco Lab

In the Cisco lab , there are 30 workstations that are designed for teaching and practicing networking concepts using Cisco technologies. This cisco lab consists of server, Wifi, projector, speaker, switch, router.

To support all workstations, we are using Dell EMC PowerEdge T640 Tower Server which supports centralized storage, enabling the lab to handle large datasets and configurations efficiently. For Wifi we are using Netgear Web 758-111 Nas Wifi 7 as implementation and testing of wireless security protocols and performance analysis. In addition, WS-C3850-48XS-S Catalyst 3850 Switch SFP+ is the one that we used for enabling communication and data transfer between workstation, server and other network devices. Last but not least, router C8500-12X is being used to ensure that data sent from one device reaches its destination efficiently.

6.1.2.4 EMBEDDED LAB

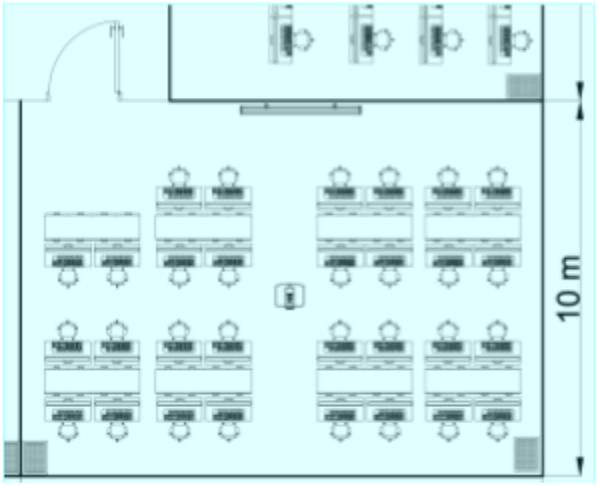


Figure 6.1.2.4 Work Area 8, Embedded Lab

For embedded labs, 30 workstation is a specialized environment designed for learning, experimenting and developing embedded systems. It typically includes hardware components like microcontroller, sensors and actuators, as well as software tools for programming and simulation. The lab consists of a projector, speaker, Wifi, server and also a switch.

The lab also features a projector and speaker for instructional content, connected through a WS-C3850-48XS-S Catalyst 3850 Switch SFP+ Switch and patch panel to the NETGEAR WEB 758-111 NAS WiFi 7 for robust wireless connectivity. Additionally, Dell EMC PowerEdge T640 Tower Server supports development tools, file storage, and network management, creating an efficient and collaborative learning environment.

6.2 NETWORK DIAGRAM

6.2.1 GROUND FLOOR

6.2.1.1 SERVER ROOM

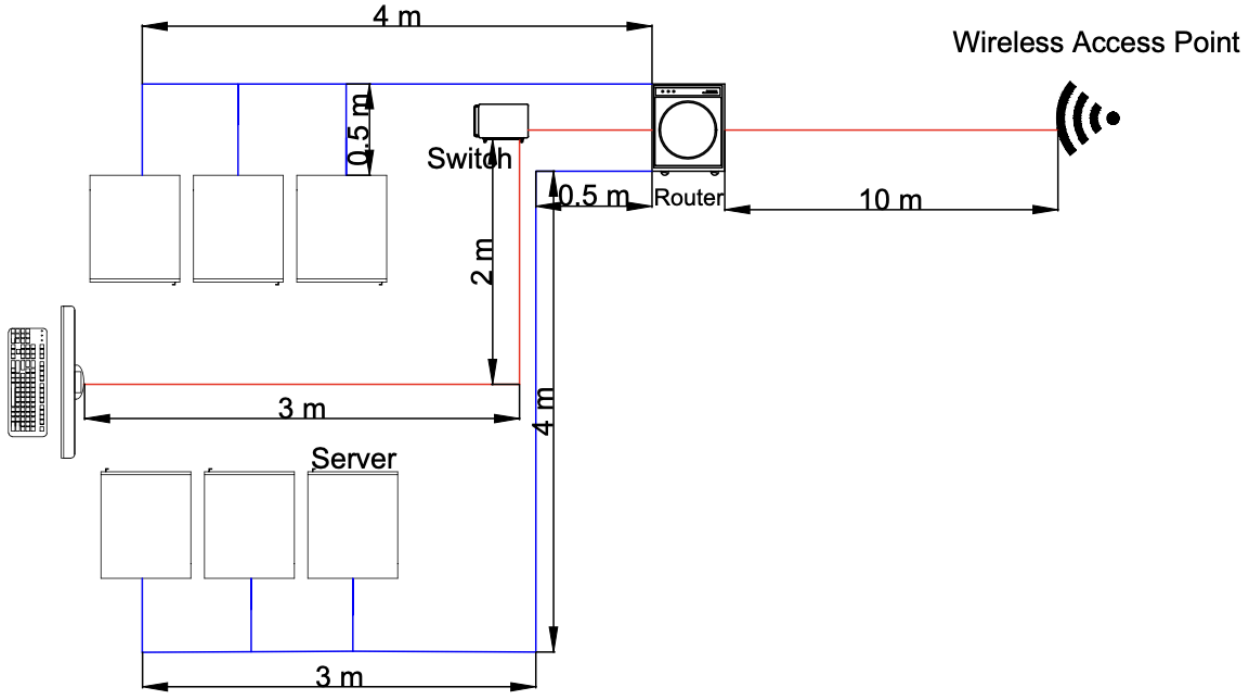


Figure 6.2.1.1 Server Room

In the server room, the PC and all six servers are connected to the switch, which facilitates communication within the local network. The switch is then connected to a router, which acts as the gateway to the internet, managing traffic between your local network and the wider web. This ensures that internal devices can access the internet while also protecting them with network security features. Additionally, Wireless Access Point (WAP) connected to the switch, providing Wi-Fi connectivity for wireless devices such as laptops, smartphones, and tablets. This setup allows for both wired and wireless devices to communicate efficiently within the network and access the internet, ensuring a robust and flexible IT infrastructure.

6.2.1.2 STUDENT LOUNGE

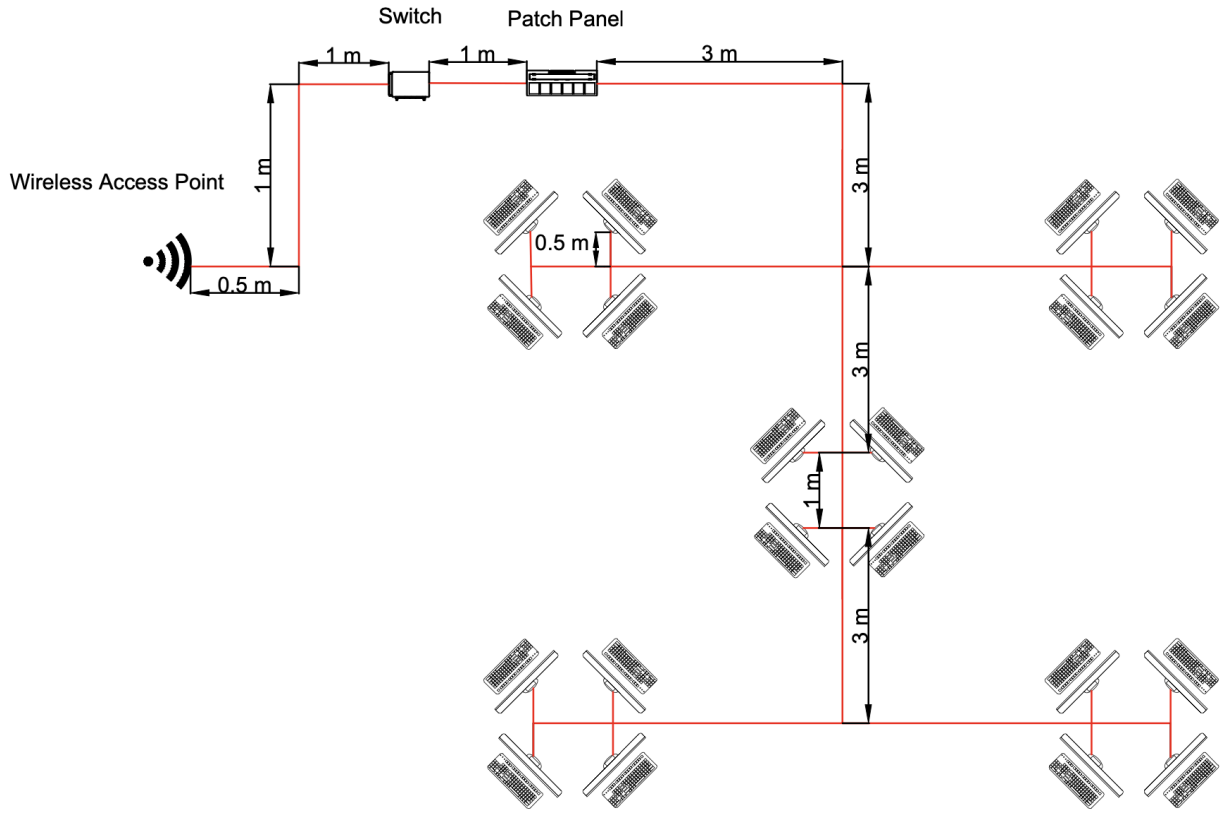


Figure 6.2.1.2 Student Lounge

In the student lounge there is a Wireless Access Point that is connected through a Patch Panel and Switch. The Patch Panel serves as a central hub for organizing and managing network cables to make it easier to arrange and maintain the connections. Data traffic can be managed efficiently by having Switch connect with Multiple devices in Local Area Network (LAN) then could have smooth communication between devices.

Wireless devices are able to connect to the network without requiring physical cables due to the existence of Wireless Access Point.It links to the Switch via a cable to support the Wi-Fi network. It links to the Switch via a cable to support the Wi-Fi network. As illustrated in the diagram, the red lines represent CAT8 cables, chosen for their ability to handle greater bandwidth and faster data transfer speeds, which are essential for demanding activities like internet surfing, streaming, and group projects in the lounge.

6.1.1.3 GENERAL PURPOSE LAB 1

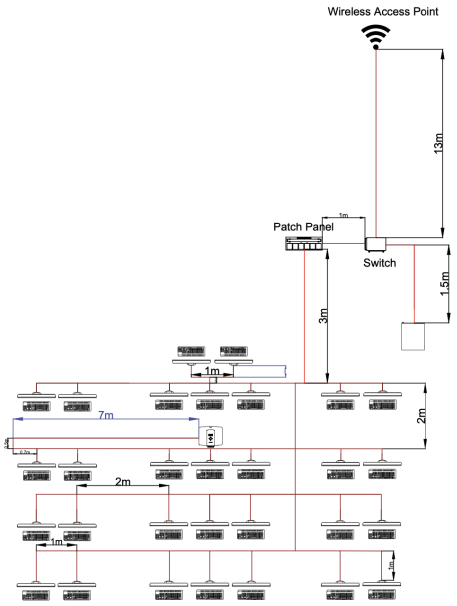


Figure 6.2.1.3 General Purpose Lab 1

In this general-purpose lab network setup, each networking device plays a specific role in facilitating communication and connectivity as shown in the figure. The total of 30 PCs are connected to the server and Wireless Access Point (WAP) through the patch panel and switch by Cat 8 cable with a total length of approximately 89.1 meters, represented by the red lines in the figure. The choice of Cat 8 cable ensures higher data transmission speeds and minimizes signal degradation. The server is responsible for providing services and resources to the network, hosting files, applications, or services required by both students and lecturers. This allows students and lecturers to access centralized resources and data, ensuring efficient management and storage of educational materials. The switch acts as a central networking device that connects all computers, the server, and other devices within the network, directing data only to the intended device to improve network efficiency. The Wireless Access Point enables wireless connectivity for Wi-Fi-enabled devices such as laptops, tablets, and smartphones used by students and lecturers. Additionally, the projector is connected to the patch panel for wireless access via the Wireless Access Point, enabling presentations and other media sharing in the lab. Cables from computers, the server, switch, and WAP are terminated at the patch panel, which centralizes cable management and simplifies modifications or expansions to the network.

6.1.1.4 GENERAL PURPOSE LAB 2

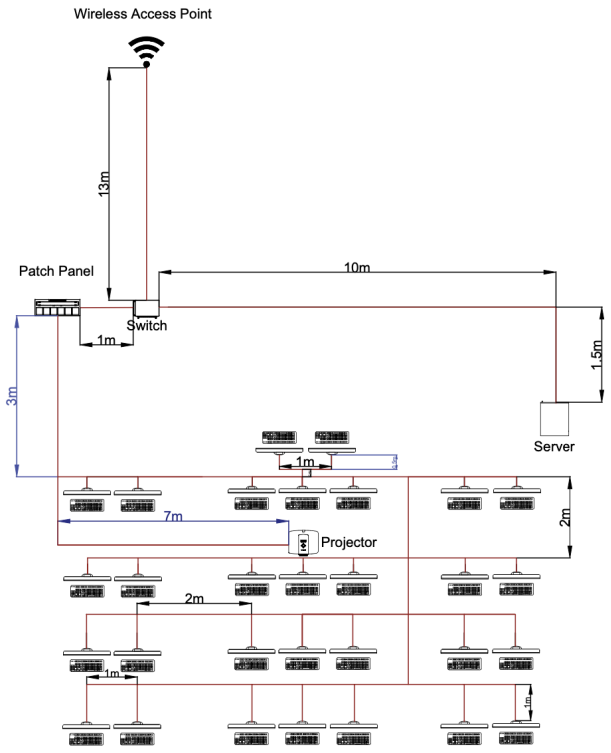


Figure 6.2.1.4 General Purpose lab 2

In this network setup for the general-purpose lab, each device serves a specific function to ensure effective communication and connectivity, as illustrated in the diagram. A total of 30 PCs are linked to the server and Wireless Access Point (WAP) through the patch panel and switch, using approximately 97.9 meters of Cat 8 cable, represented by the red lines in the diagram. The use of Cat 8 cable ensures optimal data transmission speeds and reduces the likelihood of signal degradation. The server plays a crucial role in providing the network with essential services and resources, including hosting files, applications, and other tools necessary for both students and lecturers. This centralized system allows easy access to data and ensures efficient storage and management of educational materials. The switch connects all network devices, such as computers, the server, the projector, and others, and directs traffic only to the appropriate device, enhancing overall network performance. The Wireless Access Point provides wireless connectivity for mobile devices like laptops, tablets, and smartphones, commonly used by both students and lecturers. In addition, the projector is connected through the patch panel, enabling seamless media sharing and presentations via the Wireless Access Point. All network cables, including those for the computers, server, switch, and WAP, are routed through the patch panel, streamlining cable management and allowing for easy network modifications or expansions.

6.2.2 FIRST FLOOR

6.2.2.1 VIDEO CONFERENCING ROOM

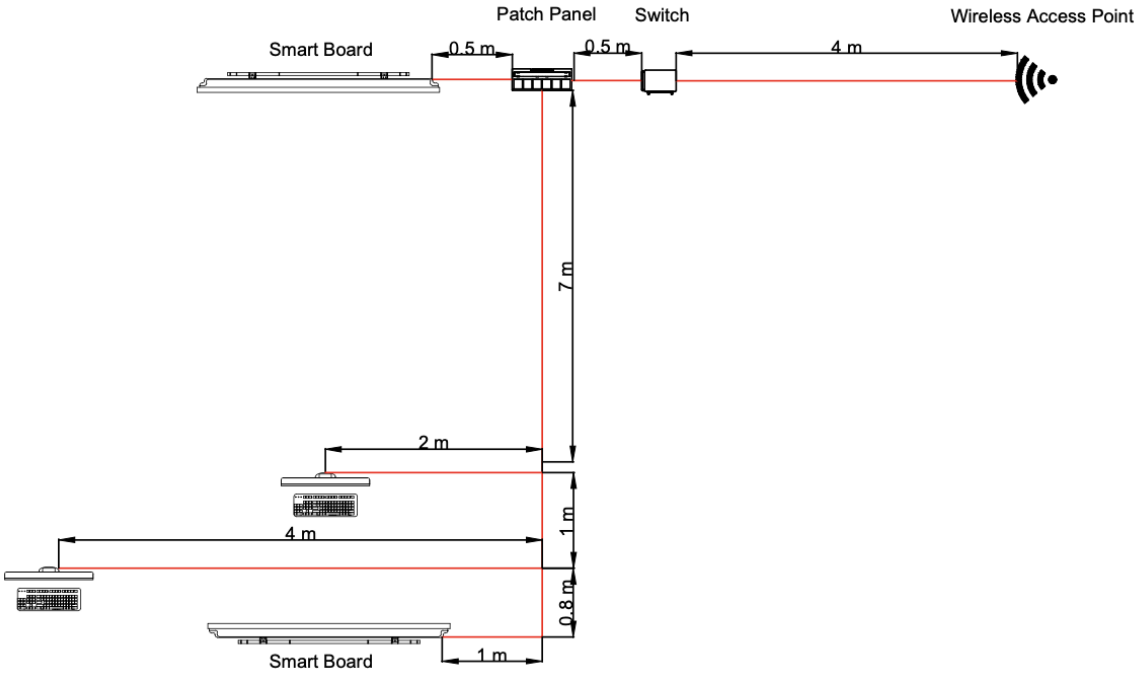


Figure 6.2.2.1 Video Conferencing Room

In the video conferencing room, the switch will be connected to both the Wireless Access Point (WAP) and the patch panel. The projector will be linked to the switch through the patch panel. All devices are connected using Cat 8 cables, which support high data transfer rates and meet the bandwidth demands of Wi-Fi 7 technology. With a length of 20.8 meters, the Cat 8 cables ensure minimal signal degradation while maintaining optimal performance. The switch serves as the central networking device, managing both wired and wireless connections efficiently. The WAP is responsible for providing reliable wireless connectivity, allowing devices in the room to seamlessly connect to the network. This setup is designed to support the creation of a video conferencing room with robust and dependable connectivity, ensuring excellent performance during virtual meetings.

6.2.2.2 HYBRID CLASSROOM

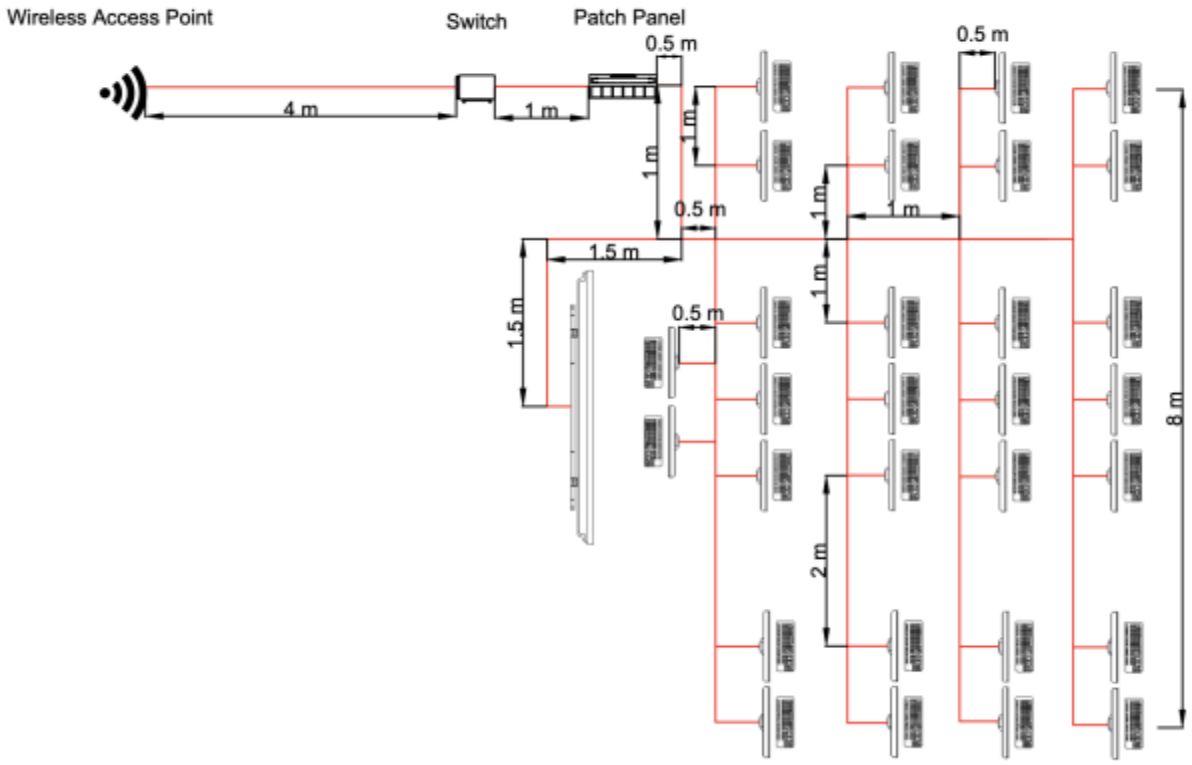


Figure 6.2.2.2 Hybrid Classroom

For the hybrid classroom, each of the 30 workstations is connected via Ethernet cables to the patch panel, which helps to organize and manage the network connections. The patch panel is then connected to the switch, which serves as the central hub for the network, allowing all the workstations to communicate with each other.The smart board is also connected to the switch to ensure it can communicate with all workstations and access the internet if needed. The wireless access point is connected to the switch to provide Wi-Fi coverage for wireless devices such as laptops, tablets, and smartphones, ensuring flexibility for students and lecturers.The switch controls routing data between the workstations, smart board, and WAP, ensuring smooth and efficient communication within the classroom network. This setup allows it as an ideal environment for a hybrid classroom where students can use a variety of devices and access both local and online resources seamlessly.

6.2.2.3 CISCO LAB

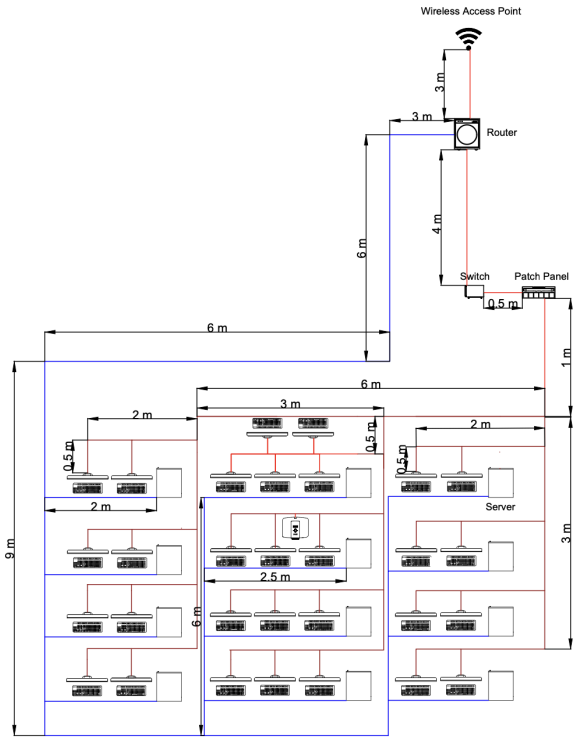


Figure 6.2.2.3 Cisco Lab

These 30 workstations are connected to a central hub represented by the Dell EMC PowerEdge T640 Tower Server, which acts as the central repository for data storage, processing, and overall network management in the labs. Wireless connectivity is provided by the strategically placed Netgear WEB 758-111 NAS Wi-Fi 7 Access Point, offering high-speed wireless coverage throughout the lab. This Wi-Fi 7 access point ensures seamless connectivity and improved performance for devices within its range, enhancing mobility and flexibility. The wired data traffic is efficiently managed by the WS-C3850-48XS-S Catalyst 3850 Switch, equipped with SFP+ ports for high-speed fiber optic connections. This switch facilitates smooth communication between workstations, the server, and other networked devices, ensuring optimized performance of the wired connections. The network's physical connections are organized and managed through a patch panel, which serves as the centralized interface. Each workstation, server, Wi-Fi access point, and Catalyst 3850 Switch are connected via structured Cat 8 cabling with a total length of 122 meters. This ensures high-speed data transmission with minimal signal degradation, supporting the advanced bandwidth requirements of Wi-Fi 7 technology. This setup guarantees a tidy, maintainable network configuration with flexibility for easy adjustments or expansions as necessary.

6.2.2.4 EMBEDDED LAB

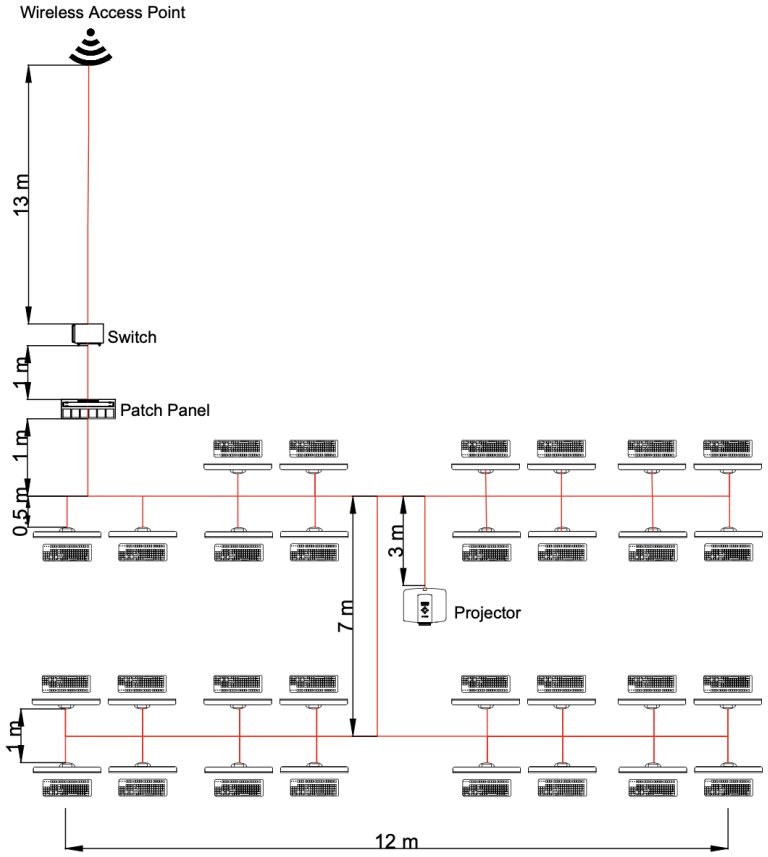


Figure 6.2.2.4 Embedded Lab

In the embedded lab, Each workstation is equipped with a computer connected to a central network switch via Ethernet cables to ensure stable and fast data communication. The patch panel is being used to organize and manage all the network cables and link to the switch. The switch then will connect to the wireless access point to allow mobile devices and workstation to access the network wirelessly. A projector is installed to display instructional content and presentations. It is connected to one of the workstations, which acts as the source for the content. The projector can also connect to the switch via the patch panel, enabling it to access networked content directly ensuring all components in the lab are well-connected and can communicate effectively,

6.3.1 FLOOR PLAN

6.3.1.1 GROUND FLOOR

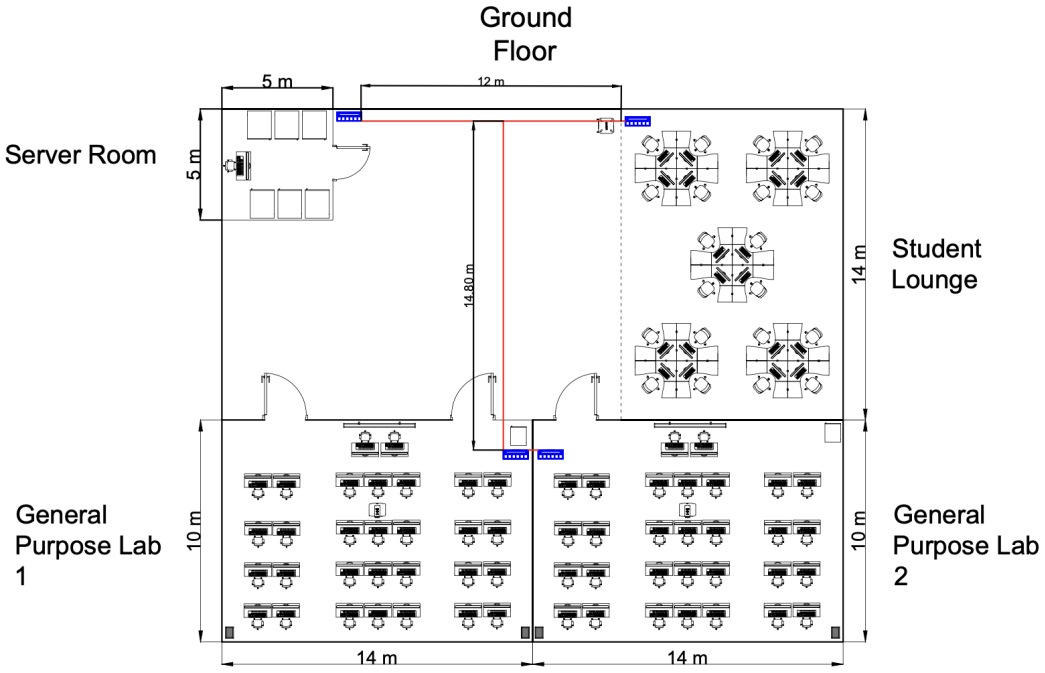


Figure 6.3.1.1.1 floor plan for ground floor

For floor plan Ground floor above, connection cable 8 is being used to connect from the server room, student lounge, general purpose lab 1 and general purpose lab 2. Each of these areas has its own switch, which acts as an intermediary, facilitating network communication. The cabling is neatly installed along the walls and connects to the switches in every work area, ensuring all devices have network access. From the server to the student lounge is 12 meters, from it then 14.8 m to general purpose lab one and two. This structured cabling system not only supports robust network performance but also allows for easy future expansions.

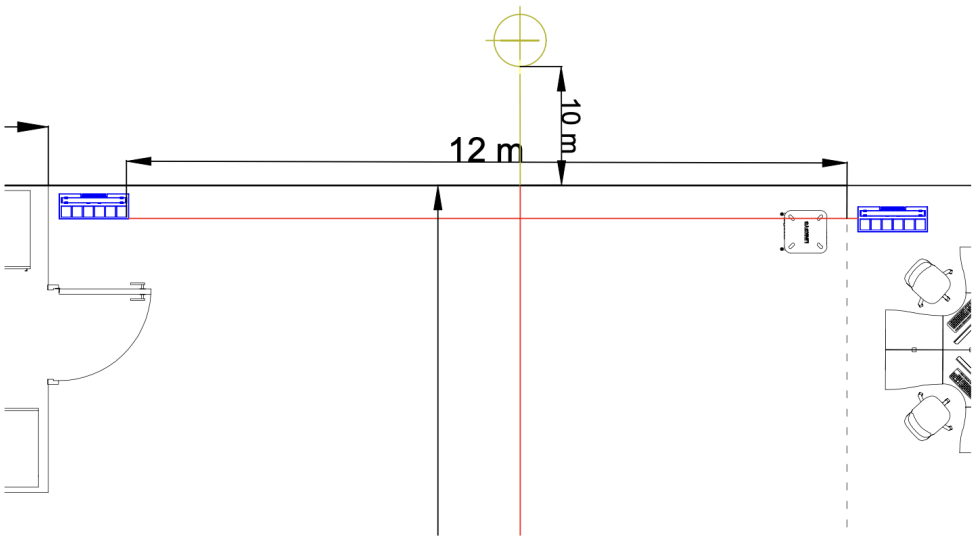


Figure 6.3.1.1.2 Backbone Cabling for ground floor

On the ground floor, backbone cabling connects the server room, which serves as the central hub, to the student lounge and general-purpose labs 1 and 2. Using Cat 8 cables, the backbone cabling spans 12 meters from the server room to the student lounge and an additional 14.8 meters to the general-purpose labs. Each area has its own switch, which facilitates network communication and ensures reliable access to centralized resources. Horizontal cabling within each work area connects local devices like PCs, wireless access points, and projectors to their respective switches. This structured cabling supports robust data transfer, efficient organization, and easy maintenance.

6.3.1.2 FIRST FLOOR

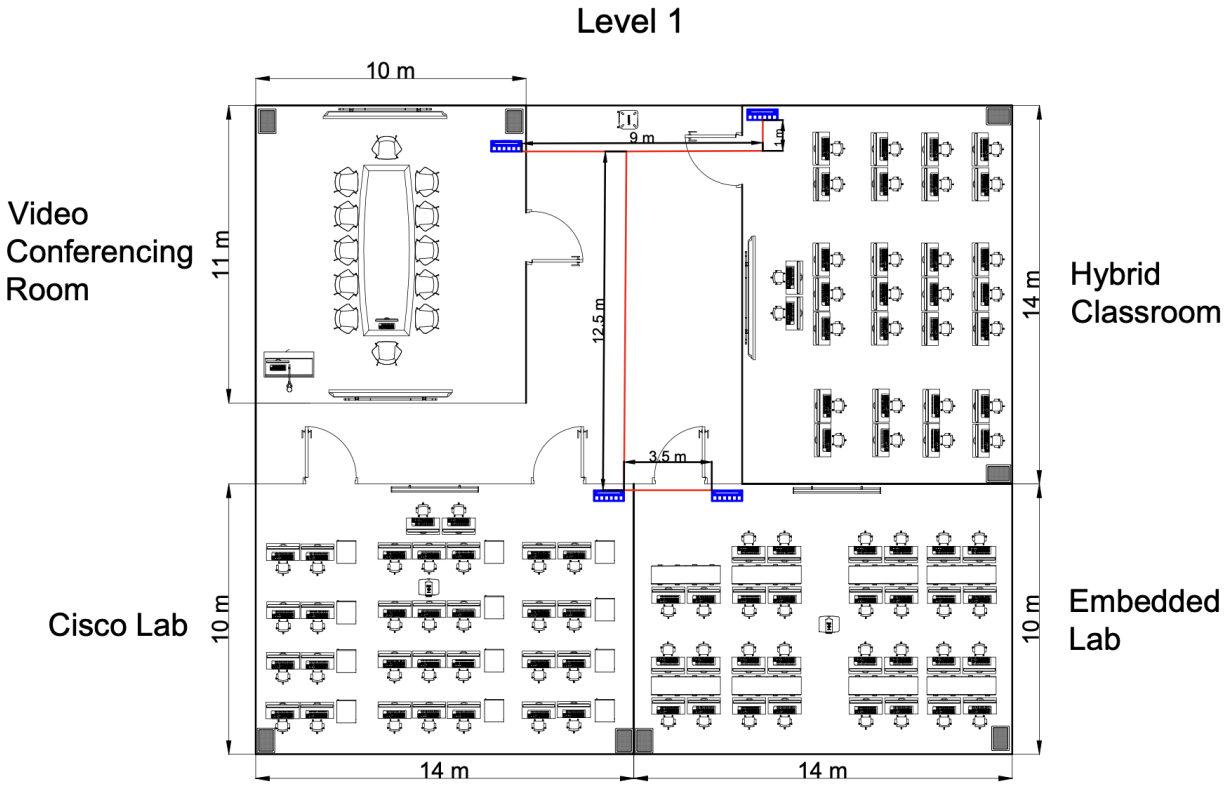


Figure 6.3.1.2.1 Floor Plan for First Floor

For the first floor, connection cable 8 is used to connect the video conferencing room, hybrid classroom, embedded lab, and Cisco lab. Each of these areas has its own switch, which acts as an intermediary to facilitate network communication. The cabling is neatly installed along the walls and connects to the switches in every work area, ensuring all devices have network access. From the video conferencing room to the hybrid classroom it is 9 meters. Then from it it is 12.5 meters to connect cisco lab and embedded lab. This structured cabling system not only supports robust network performance but also allows for easy future expansions.

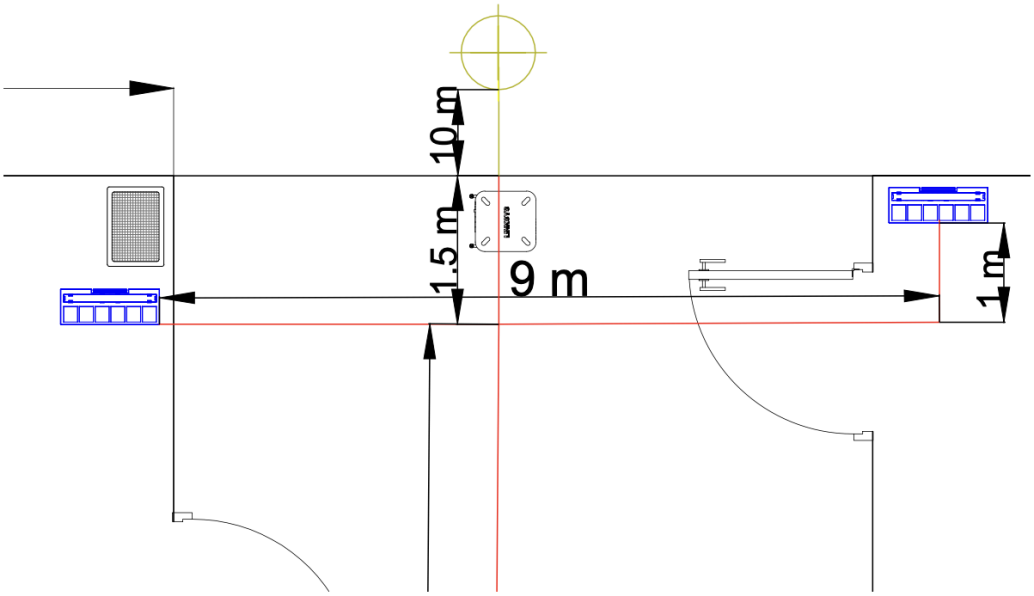


Figure 6.3.1.2.2 Backbone Cabling for 1st floor

On the first floor, backbone cabling extends from the server room to connect the video conferencing room, hybrid classroom, Cisco lab, and embedded lab. The backbone connections span 9 meters from the video conferencing room to the hybrid classroom and another 12.5 meters to the Cisco and embedded labs. Local switches in each area manage horizontal cabling, which links devices such as PCs, smartboards, and wireless access points to the network. This arrangement ensures seamless communication within each room and reliable access to the central network for advanced learning and research activities.

6.4 IDENTIFYING THE CABLE LENGTH AND TYPE

6.4.1 CONNECTION, PATCH CORDS AND SWITCH

The number of patch cords matches the cables connected to the patch panel, and the number of switch ports corresponds to the cables entering and exiting the switch. The total number of connections is directly related to the number of switch ports. This setup ensures that every cable is properly accounted for to provide network connectivity across the building, with patch cords enabling the connections and switch ports serving as entry and exit points. The overall number of connections equals the number of active switch ports.

Work Area	Number of connection	Number of Patch Cords	Number of Switch Ports
Server room	1	1	1
Student Lounge	10	10	12
General Purpose Lab 1	30	30	32
General Purpose Lab 2	30	30	32
Floor 1	101	101	112
Video Conference room	2	2	4
Hybrid Classroom	30	30	32
CISCO Lab	30	30	32
Embedded Lab	30	30	32
Floor 2	92	92	100
Total	193	193	212

6.4.2 CABLE TYPE AND LENGTH

The RS PRO 100m Cat8 Ethernet cable (SFTP Shielded, Unterminated) is chosen for its unparalleled performance in high-speed networking. With support for data transfer speeds of up to 40 Gbps and a bandwidth of 2000 MHz, Cat 8 ensures fast and efficient data transmission, making it ideal for demanding applications such as data centers, high-performance computing, and industrial environments. Its shielded and foil twisted pair construction provides excellent protection against electromagnetic interference and crosstalk, ensuring stable and reliable performance even in electrically noisy surroundings. Additionally, the durability and robust design of RS PRO cables make them a reliable choice for long-term use in critical network infrastructure.

Although Cat 8 is certified for a maximum segment length of 30 meters, it is the best choice for scenarios requiring top-tier speed and minimal latency within short to medium distances. By segmenting the total length of 522.8 meters using switches or repeaters, the network can fully leverage the capabilities of Cat 8 while maintaining optimal performance. This ensures a future-proof solution capable of handling modern high-speed demands and emerging technologies, making Cat 8 the preferred option for high-performance and interference-sensitive environments.

Work Area	Cable Type	Length(m)
Ground Floor		
Server	CAT 8 Cable	28.5 m
Student Lounge	CAT 8 Cable	43.5 m
General Purpose Lab 1	CAT 8 Cable	89.1 m
General Purpose Lab 2	CAT 8 Cable	97.9 m
Total Length(m)		259 m
First Floor		
Video Conference room	CAT 8 Cable	20.8 m
Hybrid Classroom	CAT 8 Cable	57 m
CISCO Lab	CAT 8 Cable	122 m
Embedded Lab	CAT 8 Cable	64 m
Total length(m)		263.8 m
Total length of cable used		522.8 m

REFLECTION TASK 4

For task 4, we designed and implemented a comprehensive network for the new building focusing on creating a scalable network, high performance and future proof infrastructure. We carefully planned the work areas, identifying the number of connections, patch cords, and switch ports needed, ensuring efficient connectivity. Our choice of Cat 8 cables ensures high-speed data transmission with minimal signal degradation, which is crucial for the network's overall performance. We calculated the number of patch cords to match the cables connected to the patch panel, and the number of switch ports corresponding to the cables entering and exiting the switch. This setup ensures that every cable is properly accounted for to provide network connectivity across the building, with patch cords enabling the connections and switch ports serving as entry and exit points. By using switches or repeaters to divide the total length of 522.8 meters, the network can fully use Cat8's capabilities while keeping performance high. This provides a long-lasting solution that can support fast speeds and new technologies, making Cat8 one of a top choice for high-performance setups where interference is a concern.

7.0 IP ADDRESSING SCHEME

7.1 NETWORK ADDRESS

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 7.1.1 IP address

The IP address 192.16.0.0 serves as the base address for a network. This address specifically identifies the network itself, establishing the foundation for all communications within it. The notation "/8" refers to the subnet mask, which in this case is 255.0.0.0. This subnet mask dictates how much of the 32-bit IP address is dedicated to the network portion, and how much is allocated for individual host addresses. In this case, the "/8" mask means that the first 8 bits (the first octet) are used to identify the network, leaving the remaining 24 bits (or three octets) to be used for the host portion of the address. This configuration allows for a large number of hosts within the network, as it enables a range of IP addresses for each individual device connected to the network. The "/8" subnet mask indicates that this address belongs to a Class A network. Class A networks are typically characterized by their capacity to support a vast number of hosts, as the network portion only occupies the first 8 bits of the 32-bit IP address. The Class A range in IPv4 addressing spans from 1.0.0.0 to 127.255.255.255, with the first octet used to define the network and the remaining three octets used to assign unique addresses to devices within that network. In the case of the address 192.16.0.0, the first octet (192) is designated for the network portion, while the next two octets (16.0) specify a more particular subnet within the broader network. The final portion (0.0) can be used for further subnetting, or it can represent the addresses assigned to individual hosts within that specific subnet. This flexibility allows network administrators to allocate IP addresses

efficiently, ensuring sufficient addresses are available for all devices, while also maintaining room for expansion as the network grows.

7.2 SUBNETTING

7.2.1 SUBNET MASK

A subnet mask is a 32-bit number that helps divide an IP address into two segments which is the network portion and the host portion. In the subnet mask, the bits assigned to the network are set to 1s, while the bits assigned to the host are set to 0s. The primary role of the subnet mask is to determine the network an IP address belongs to and to distinguish between the network and host parts of the address. Subnet masks are frequently used in IPv4 networking, especially when subnetting, which involves splitting a large network into smaller, more manageable sub-networks. For example, with the network address 192.16.0.0/8, the /8 indicates that the first 8 bits of the IP address are dedicated to the network portion, while the remaining 24 bits are available for host addresses. This configuration enables a wide range of possible host addresses within the network. Below is a detailed breakdown of the 192.16.0.0 IP address, showing it in both decimal and binary formats.

IP address (Decimal)	192.	16.	0.	0
IP address (Binary)	1100 0000	0001 0000	0000 0000	0000 0000
Subnet Mask (Decimal)	255.	0.	0.	0
Subnet Mask (Binary)	1111 1111.	0000 0000.	0000 0000.	0000 0000

Subnet Mask: 255.0.0.0

By converting each octet of the IP address 192.16.0.0 to binary, we get the result “1100 0000. 0001 0000. 0000 0000. 0000 0000” as shown above. Additionally, the "/8" in CIDR notation signifies that the first 8 bits of the IP address are allocated for the network portion, while the remaining 24 bits (32 bits - 8 bits = 24 bits) are available for host addresses. In binary, this corresponds to the subnet mask “11111111.00000000.00000000.00000000”, which represents the subnet mask in binary format. When we convert this binary representation back into dotted-decimal notation, we obtain the subnet mask “255.0.0.0”. This subnet mask allows for a large number of host addresses within the network, making it ideal for a broad range of devices.

7.2.2 SUBNET ADDRESS

Subnet addressing is a versatile and scalable technique used to design and manage IP networks efficiently. It works by dividing a network into smaller, more manageable subnets. In the case of the IP address 192.16.0.0/8, we are working with 24 host bits, which results in a total of 2^{24} = 16,777,216 possible host addresses. These addresses range from 192.16.0.1 to 192.16.255.254. The first address, 192.16.0.0, is reserved as the network address, which represents the network itself and cannot be assigned to individual devices. Similarly, the last address, 192.16.255.255, serves as the broadcast address, used for sending data to all devices in the subnet, and is also unavailable for assignment to hosts. To determine the subnet address, we perform a bitwise AND operation between the given IP address 192.16.0.0 and the subnet mask /8 (which is 255.0.0.0). Converting both the IP address and subnet mask into binary, the IP address becomes 11000000 00010000 00000000 00000000, and the subnet mask becomes 11111111 00000000 00000000 00000000. By applying the AND operation to the corresponding bits, we obtain the subnet address in binary: 11000000 00000000 00000000 00000000, which converts back to decimal as 192.0.0.0. Thus, the subnet address for 192.16.0.0/8 is 192.0.0.0.

Calculation of Subnet Address

IP Address (Decimal)	192	16	0	0
IP Address (Binary)	1100 0000	0001 0000	0000 0000	0000 0000
AND				
Subnet Mask (Decimal)	255	0	0	0
Subnet Mask (Binary)	1111 1111	0000 0000	0000 0000	0000 0000
RESULT				

Subnet Address (Binary)	1100 0000	0000 0000	0000 0000	0000 0000
Subnet Address (Decimal)	192	0	0	0

As shown in the table, the process begins by converting both the IP address 192.16.0.0 and the subnet mask 255.0.0.0 into binary. The binary representation of the IP address is 1100 0000.0001 0000.0000 0000.0000 0000, and the subnet mask is 1111 1111.0000 0000.0000 0000.0000 0000. Next, we apply the AND operation bit by bit between the corresponding bits of the IP address and the subnet mask. After performing the AND operation, the resulting binary subnet address is 1100 0000.0000 0000.0000 0000.0000 0000. Finally, we convert this binary result back to decimal, which gives us the subnet address 192.0.0.0. Therefore, the subnet address obtained by applying the AND operation between the IP address 192.16.0.0 and the subnet mask /8 is 192.0.0.0.

IP address = 192.16.0.0/8

IP Address	**Network Portion**	**Host Portion**
192.16.0.0/8	1100 0000	0001 0000 0000 0000 0000 0000

For the Network portion, there are 8 bits while the Host Portion is 24 bits.

Faculty of Computing which has 8 work areas:

1. Server Room
2. Student Lounge
3. General Purpose Lab 1
4. General Purpose Lab 2
5. Video Conferencing Room
6. Hybrid Classroom
7. Cisco Lab
8. Embedded Lab

Since this faculty has 8 work areas, the network needs to have 8 major subnets.

192.16.0.0/8 to be divided into 8 subnets (2^3)

$n = \log_2(8) = 3$

Thus, we need to borrow 3 bits from the host portion

IP address = 192.16.0.0/11

IP Address	Portion
192.16.0.0/11	1100 0000.0001 0000.0000 0000.0000 0000

No of bits borrowed from the host portion (in red) = 3 bits

Network portion = 11 bits

Host portion = 21 bits

Subnet Address for each Work Area

Subnet	Work Area	Subnet Address (Decimal)	Subnet Address (Binary)
0	Server Room	192.0.0.0/11	1100 0000.0000 0000. 0000 0000. 0000 0000
1	Student Lounge	192.32.0.0/11	1100 0000.0010 0000. 0000 0000. 0000 0000
2	General Purpose Lab 1	192.64.0.0/11	1100 0000.0100 0000. 0000 0000. 0000 0000
3	General Purpose Lab 2	192.96.0.0/11	1100 0000.0110 0000. 0000 0000. 0000 0000
4	Video Conferencing Room	192.128.0.0/11	1100 0000.1000 0000. 0000 0000. 0000 0000

5	Hybrid Classroom	192.160.0.0/11	1100 0000.1010 0000. 0000 0000. 0000 0000
6	Cisco Lab	192.192.0.0/11	1100 0000.1100 0000. 0000 0000. 0000 0000
7	Embedded Lab	192.224.0.0/11	1100 0000.1110 0000. 0000 0000. 0000 0000

7.3 IP ASSIGNATION

7.3.1 NETWORK AND BROADCAST ADDRESS FOR EACH SUBNET

To find the network and broadcast addresses for each subnet, we perform the AND operation between the IP address and the subnet mask. The broadcast address is then determined by setting all the host bits to '1' in the network address. The usable IP address range for hosts within each subnet is from the network address plus one, up to the broadcast address minus one. For instance, in the General Purpose Lab 1 subnet, the range of usable IP addresses spans from 192.0.0.1 to 192.31.255.254. The table below illustrates the network address, broadcast address, and the range of usable IP addresses for each work area, based on the calculations and performance.

Subnet	Work Area	Network Address	Broadcast Address	Range of usable address
0	Server Room	192.0.0.0	192.31.255.255	192.0.0.1 - 192.31.255.254
		1100 0000. 0000 0000. 0000 0000. 0000 0000	1100 0000.0001 **1111. 1111 1111. 1111 1111**	1100 0000. 0000 0000. 0000 0000. 0000 0001 - 1100 0000. 0001 1111. 1111 1111. 1111 1110
1	Student Lounge	192.32.0.0	192. 63.255.255	192.32.0.1 - 192.63.255.254
		1100 0000.0010 0000. 0000 0000. 0000 0000	1100 0000.0011 **1111. 1111 1111. 1111 1111**	1100 0000.0010 0000. 0000 0000. 0000 0001 - 1100 0000.0011 1111. 1111 1111. 1111 1110

2	General Purpose Lab1	192.64.0.0	192.95.255.255	192.64.0.1 - 192.95.255.254
		1100 0000.0100 0000. 0000 0000.0000 0000	1100 0000.0101 **1111. 1111 1111. 1111 1111**	1100 0000.0100 0000. 0000 0000.0000 0001 - 1100 0000.0101 1111. 1111 1111. 1111 1110
3	General Purpose Lab2	192.96.0.0	192.127.255.255	192.96.0.1 - 192.127.255.254
		1100 0000.0110 0000. 0000 0000.0000 0000	1100 0000.0111 **1111. 1111 1111. 1111 1111**	1100 0000.0110 0000. 0000 0000.0000 0001 - 1100 0000.0111 1111. 1111 1111. 1111 1110
4	Video Conferencing Room	192.128.0.0	192.159.255.255	192.128.0.1 - 192.159.255.254
		1100 0000.1000 0000. 0000 0000.0000 0000	1100 0000.1001 **1111. 1111 1111. 1111 1111**	1100 0000.1000 0000. 0000 0000.0000 0000 - 1100 0000.1001 1111. 1111 1111. 1111 1110
5	Hybrid Classroom	192.160.0.0	192.191.255.255	192.160.0.1 - 192.191.255.254
		1100 0000.1010 0000. 0000 0000.0000 0000	1100 0000.1011 **1111. 1111 1111. 1111 1111**	1100 0000.1010 0000. 0000 0000.0000 0001 - 1100 0000.1011 1111. 1111 1111. 1111 1111
6	Cisco Lab	192.192.0.0	192.223.255.255	192.192.0.1 - 192.223.255.254
		1100 0000.1100 0000. 0000 0000.0000 0000	1100 0000.1101 **1111. 1111 1111.**	1100 0000.1100 0000. 0000 0000.0000 0001 -

			1111 1111	1100 0000.1101 1111. 1111 1111. 1111 1110
7	Embedded Lab	192.224.0.0	192.255.255.255	192.224.0.1 - 192.225.255.254
		1100 0000.1110 0000. 0000 0000.0000 0000	1100 0000.1111 **1111. 1111 1111. 1111 1111**	1100 0000.1110 0000. 0000 0000.0000 0001 - 1100 0000.1111 1111. 1111 1111. 1111 1110

7.3.2 IP ASSIGNATION FOR EACH WORK AREA

Each area is assigned a specific range of IPs to ensure unique identification, efficient communication, and simplified management. In the Server Room, critical devices like servers, switches, routers, and a wireless access point are assigned IPs within 192.0.0.1 - 192.0.0.10. Similarly, the Student Lounge uses 192.32.0.1 - 192.32.0.24 for its switch, wireless access point, and 20 workstations. The General Purpose Labs are allocated ranges 192.64.0.1 - 192.64.0.34 and 192.96.0.1 - 192.96.0.34, respectively, for 30 workstations, supporting devices, and a server in each lab.

Specialized areas like the Video Conferencing Room, Hybrid Classroom, Cisco Lab, and Embedded Lab also follow organized IP ranges. For example, the Cisco Lab uses 192.192.0.1 - 192.192.0.47 for workstations, servers, and networking devices, while the Hybrid Classroom allocates IPs from 192.160.0.1 - 192.160.0.34. This structured assignation ensures seamless device communication, minimizes conflicts, and supports effective network administration, with routers positioned strategically in the Server Room and Cisco Lab for network management at different levels.

Work Area	**Hosts**	**Range IP Address**
Server Room	6 server	192.0.0.1 - 192.0.0.7

	Wireless Access Point	192.0.0.8
	Switch	192.0.0.9
	Router	192.0.0.10
Student Lounge	Switch	192.32.0.1
	Wireless Access Point	192.32.0.2
	20 workstation	192.32.0.3 - 192.32.0.24
General Purpose Lab 1	30 workstations	192.64.0.1 - 192.64.0.31
	Switch	192.64.0.32
	Wireless Access Point	192.64.0.33
	Server	192.64.0.34
General Purpose Lab 2	30 workstations	192.96.0.1 - 192.96.0.31
	Switch	192.96.0.32
	Wireless Access Point	192.96.0.33
	Server	192.96.0.34
Video Conferencing Room	2 workstations	192.128.0.1 -192.128.0.3
	Switch	192.128.0.4
	Wireless Access Point	192.128.0.5
	2 Smartboard	192.128.0.6 - 192.128.0.8
Hybrid Classroom	30 workstations	192.160.0.1 - 192.160.0.31
	Wireless Access Point	192.160.0.32
	Switch	192.160.0.33

	Smartboard	192.160.0.34
Cisco Lab	30 workstations	192.192.0.1 - 192.192.0.31
	12 server	192.192.0.32 - 192.192.0.44
	Switch	192.192.0.45
	Router	192.192.0.46
	Wireless Access Point	192.192.0.47
Embedded Lab	30 workstations	192.224.0.1 - 192.224.0.31
	Switch	192.224.0.32
	Wireless Access Points	192.224.0.33

Network Management	**Host**
Level 1 (Server Room)	Router
Level 2 (Cisco Lab)	Router

REFLECTION TASK 5

For task 5, we use the IP address that has been given which is IP address 192.16.0.0/8 to divide the network into subnets for different work areas, such as labs, classrooms and video conferencing rooms. This ensured that each of the hosts had a unique IP address. We gained valuable insights through the process of subnetting and address calculation, as well as scalability considerations. This task prepared us to handle future network design challenges with greater confidence and technical proficiency.

8.0 CONCLUSION

Understanding of both the theoretical and practical elements of networking has significantly improved with the finalization of the network design project for the new two-floor structure at the Faculty of Computing. Through careful planning and execution, we successfully developed a network architecture that is secure, scalable, and efficient, fulfilling the requirements of modern academic and research environments.The architecture guarantees smooth connectivity across a variety of work environments, including labs, classrooms, and video conference rooms, by putting strong IP addressing, efficient subnetting, and suitable networking devices into place.

The project highlighted the importance of addressing future scalability. We ensured that the infrastructure not only meets current demands but is also adaptable to accommodate future technological advancements and growing user traffic by creating a network capable of supporting expanding user requirements and innovations. This innovative method demonstrates a comprehensive grasp of the changing needs of networking in educational settings.

Furthermore, this project enhanced our technical, collaborative, and analytical skills. We possess direct experience with subnetting, IP addressing, and selecting networking equipment to ensure the network design was both cost-effective and efficient. Collaborating enhanced our communication and project management skills, while tackling design issues boosted our flexibility and creativity. Due to these experiences, we are now ready to address more complex network design issues in the future, making this project a worthwhile learning experience.

Besides its technical achievements, the project highlighted the importance of meticulous documentation and engagement with stakeholders. We ensured that the network infrastructure was capable of managing current operations and future growth by customizing our solution to the Faculty of Computing's particular needs. Feedback from stakeholders guided our design choices, guaranteeing that the solutions we suggested were practical and meaningful.

Considering all factors, this project aligns with the current needs of the Faculty of Computing and simultaneously lays the groundwork for future development and innovation. Our

strong and expandable network architecture will boost the institution's operational productivity while also creating an environment that encourages academic and research achievement.

The network architecture equips the Faculty of Computing to meet the challenges of a rapidly evolving technological landscape through the integration of new technologies and ensuring reliable connectivity.

9.0 TEAM MEMBERS AND RESPONSIBILITIES

No.	Member	Responsibilities
1	NAZATUL NADHIRAH BINTI SABTU	**Network Architect -** Tan Li Min ● Managed the project's financial budget, ensuring cost-effectiveness without compromising quality. ● Tracked expenditures on devices, materials, and services, ensuring alignment with the allocated budget. ● Prepared financial reports detailing costs and remaining funds for stakeholders. ● Recommended adjustments to financial plans to optimize resource allocation for long-term benefits.
2	NURUL ATHIRAH SYAFIQAH BINTI MOHD RAZALI	**Project Administrator** ● Coordinated team schedules, meetings, and progress updates throughout the project lifecycle. ● Maintained comprehensive documentation of project decisions, processes, and outcomes. ● Assisted in stakeholder communication to ensure alignment with project objectives. ● Monitored deadlines and ensured that all project deliverables were completed on time.
3	NUR AINA SYAFINA BINTI KAMASUAHADI	**Project Manager** ● Oversaw the entire project, ensuring that goals were met within the allocated time frame and resources. ● Delegated tasks among team members based on their expertise and project requirements. ● Identified and mitigated risks during the design and implementation phases. ● Conducted final reviews of all deliverables to ensure they met quality standards and stakeholder

		expectations.
4	WAN NUR RAUDHAH BINTI MASZAMANIE	**Network Architect** ● Designed the overall network architecture, ensuring scalability, security, and efficiency. ● Developed the IP addressing scheme and subnetting plan to optimize network performance. ● Researched and selected networking devices suitable for the project's requirements. ● Ensured the integration of modern technologies to meet the institution's future needs.

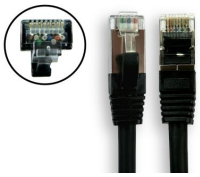
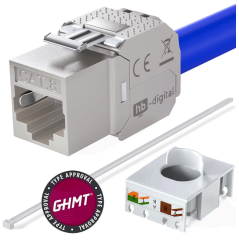
REFERENCES

1. CBT Nuggets. (2020). *5 Best Network Simulators for Cisco Exams: CCNA, CCNP, and CCIE*. Retrieved from https://www.cbtnuggets.com/blog/career/career-progression/5-best-network-simulators-for-cisco-exams-ccna-ccnp-and-ccie (Retrieved on December 1, 2024)
2. Networkise. (n.d.). *Comparison Between Cisco Switch and Huawei Switch*. Retrieved from https://networkise.com/comparison-between-cisco-switch-and-huawei-switch/ (Retrieved on December 2, 2024).
3. Gartner. (n.d.). *Compare Cisco Systems vs Huawei Technologies*. Retrieved from https://www.gartner.com/reviews/market/data-center-and-cloud-networking/compare/cisco-systems-vs-huawei-technologies (Retrieved on December 1, 2024).
4. Router-Switch. (n.d.). *Compare Cisco and Huawei Next Generation Firewall*. Retrieved from https://www.router-switch.com/compare/cisco-and-huawei-next-generation-firewall.html (Retrieved on December 2, 2024).
5. Lia. (2020). *Cisco vs Huawei: Which One is the Better Choice for Ethernet Switches?* Retrieved from https://medium.com/@lia640230/cisco-vs-huawei-which-one-is-the-better-choice-for-ethernet-switches-59ffd324117d(Retrieved on December 2, 2024).
6. Cisco Systems. (n.d.). *Cisco Firepower 2140 NGFW*. Retrieved from https://www.router-switch.com/fpr2140-ngfw-k9.html (Retrieved on December 4, 2024).
7. Fortinet. (n.d.). *FortiGate 500E*. Retrieved from https://www.router-switch.com/fg-500e.html (Retrieved on December 4, 2024).
8. Aruba. (n.d.). *Aruba AP-505 US TAA Unified Access Point R2H39A*. Retrieved from https://www.networkhardwares.com/en-my/products/aruba-r2h39a-aruba-ap-505-us-taa-unified-ap-r2h39a?variant=41672555266253&gad_source=1&gclid=CjwKCAiAmMC6BhA6EiwAdN5iLV8L5Z8Lz_qP5lvJWAeMymBILU484stTJ8CkQIsiXvVohZvsHa04QRoChQAQAvD_BwE(Retrieved on December 4, 2024).
9. D-Link. (n.d.). *Wireless N Access Point*. Retrieved from https://www.dlink.com.my/product/wireless-n-access-point/ (Retrieved on December 4, 2024).
10. NetworkHardwares. (n.d.). *Netgear 1PT Insight Managed WiFi 7 WBE758-111NAS*. Retrieved from https://www.networkhardwares.com/en-my/products/netgear-wbe758-111nas-netgear-1pt-insight-managed-wifi-7-wbe758-111nas?variant=47635341410509&gad_source=1&gclid=CjwKCAiAmMC6BhA6EiwAdN5iLd0jMgXUM2FjAv6FK2HfXXUXO_RrSxnYk4YtL4jRpn5D7A2y-jjlhxoC4ecQAvD_BwE (Retrieved on December 4, 2024).
11. Associate Prof. Dr. Norafida binti Ithnin. (2024, November 22). Discussion on designing network infrastructure for educational institutions. [Personal Interview conducted for research on educational infrastructure]. Associate Prof. Dr. Norafida binti Ithnin, UTM. Email: afida@utm.my, Contact: 019-7443458. Retrieved from https://docs.google.com/spreadsheets/d/1rksqmNnjoR-j5XqmbPXmBRVMQBRgn3EEGIJZq7PKnfE/edit?gid=763833708#gid=763833708

APPENDICES

FINANCIAL BUDGET

Component	Model	Price per unit(RM)	Quantity	Total Price(RM)
 Server	**Dell EMC PowerEdge T640 Tower Server**	28,821.00	50	1,441,050.00
 Router	**S5860-24XB-U is FS**	17,594.00	2	35,188.00
 Firewall	**FPR2140-NGFW-K9 - Cisco Firepower 2100 Series Appliances**	116,195.92	1	116,195.92
 Wireless Access Point (WAP)	**NETGEAR WEB 758-111 NAS WiFi 7**	7,422.00	2	14,844.00

 Switch	**WS-C3850-48XS -S Catalyst 3850 Switch SFP+**	75,615.59	15	1,134,233.85
 Patch Panel	**NKPP48FMY**	525.67	15	7,885.05
 Ethernet Cable	**RS PRO, 10m Cat8, Black RJ45 to Male RJ45 Male, S/FTP, Terminated LSZH Sheath**	162.13	52	8,430.76
 Ethernet Connector	**Cat8 Ethernet Cable Connector RJ45**	8.58	500	4,290.00
 Faceplate	**RJ45 Face Plate Premium Socket**	39.38	70	2,756.60
 Keystone Jack Panel	**RJ45 Cat 8.1 Tool-less Keystone Jack**	37.14	96	3,565.44

 Network Management Devices	**APC SRT8KXLI 230V Input Rack Mount UPS - 8000VA (8kW)**	50,253.54	2	100,507.08
 Cap Rubber Boot	**MTP-88-C8-SR-A 3**	0.45	500	225
			Total	2,869,171.70

Budget	**RM** 3, 000, 000. 00
Total Used	**RM** 2, 869, 171. 70
Balanced	**RM** 130, 828. 70

MEETING MINUTES

TITLE: MEETING TASK 1

MEETING MINUTES

DATE/TIME	11 Oct 2024 10am
LOCATION	MA6 317
AGENDA	To determine what software to use, create floor plan
MEETING MC	Raudhah

ATTENDANCE

NAME	TIME	REASON FOR ABSENCE
NAZATUL NADHIRAH	1015	-
NUR AINA SYAFINA	1015	-
NURUL ATHIRAH SYAFIQAH	1000	-
WAN NUR RAUDHAH	1000	-

MINUTES

NO	ITEM DISCUSSED	IDEAS/SUGGESTIONS AND PERSON GIVING IT	PERSON IN CHARGE & DATE
1.	Software to use	Raudhah suggested Athirah	Athirah (Due : 14/10)
2.	Floor plan ideas	Nazatul suggested initial layout	Raudhah (Due : 12/10)
3.	Floor plan adaptability	Nazatul & Aina suggested making the floor plan adaptable to future changes, including scalable furniture arrangements	Nazatul & Aina (Due: 12/10)
4.	Decide when to consult with Dr Zafran	Athirah suggested date to consult	Athirah (Due : 13/10)

5.	Report	Aina & Athirah will be handle drafting the reports	Aina & Athirah (Due:15/10)
6.	Next Meeting	15/10 - floor ideas should be completed	-
7.	Meeting Ended	1300	-

TITLE: MEETING TASK 2

MEETING MINUTES

DATE/TIME	3 November 2024 8:00pm
LOCATION	317 MA6
AGENDA	Completing task 2
MEETING MC	Nur Aina Syafina

ATTENDANCE

NAME	TIME	REASON FOR ABSENCE
NAZATUL NADHIRAH	20:00	-
NUR AINA SYAFINA	20:00	-
NURUL ATHIRAH SYAFIQAH	20:00	-
WAN NUR RAUDHAH	20:00	-

MINUTES

NO	ITEM DISCUSSED	IDEAS/SUGGESTIONS AND PERSON GIVING IT	PERSON IN CHARGE & DATE
1.	Gather the initial information	Athirah suggested initial information	Athirah
2.	Discussion of key questions to determine project requirement	Raudhah suggested Athirah the key question	Athirah and Raudhah
3.	Preliminary a list of question to clarify requirement	Naza suggested Syafina to clarify requirement	Naza and Syafina
4.	Filtered major questions	Raudhah will help Naza with the task	Naza

5.	Completed the answer with appropriate reference	Naza will help Raudhah in completing the answer	Raudhah
6.	Next Meeting	15/11 - task 2 should have been completed and marked to make a correction	-
7.	Meeting Ended	23:00	-
8.	Consultation with subject-matter expert on network feasibility	Insights provided by Associate Professor Dr. Norafida to enhance the proposed network's scalability and security.	Raudhah to document her feedback by November 22, 2024.

TITLE: MEETING TASK 3

MEETING MINUTES

DATE/TIME	29 November 2024 9:00pm
LOCATION	Online (Google Meet)
AGENDA	Completing task 3
MEETING MC	Nazatul Nadhirah

ATTENDANCE

NAME	TIME	REASON FOR ABSENCE
NAZATUL NADHIRAH	21:00	-
NUR AINA SYAFINA	21:00	-
NURUL ATHIRAH SYAFIQAH	21:00	-
WAN NUR RAUDHAH	21:00	-

MINUTES

NO	ITEM DISCUSSED	IDEAS/SUGGESTIONS AND PERSON GIVING IT	PERSON IN CHARGE & DATE
1.	List of devices and quantities needed	Syafina proposed starting with Cisco, Huawei, and TP-Link devices for routers and switches.	Syafina
2.	Research on device capabilities and requirements	Raudhah highlighted the importance of comparing devices suited for academic institutions.	Raudhah
3.	Inclusion of appropriate references	Athirah suggested using manufacturer websites and reputable tech forums for sourcing references.	Athirah

4.	Assessment of LAN devices to meet organizational needs	Naza suggested matching devices against scalability and cost-effectiveness.	Naza
5.	Reflection on device costs and differences between brands	Athirah noted Cisco is premium-priced, while TP-Link offers budget-friendly alternatives.	Team to collaboratively reflect and include insights in the report by 5 December 2024
6.	Major differences in device features among brands	Raudhah emphasized reliability and warranty policies as critical factors for comparison.	Raudhah
7.	Next Meeting	5/12 - task 3 should have been completed and marked to make a correction	-
8.	Meeting Ended	23:00	-
9.	Consultation with subject-matter expert on network feasibility	Insights provided by Dr. Muhammad Zafran on optimizing the selection of devices and ensuring compatibility with the project goals.	Raudhah to document the insights and integrate them into the report by 2 December 2024

TITLE: MEETING TASK 4

MEETING MINUTE

MEETING MINUTES

DATE/TIME		24/12/2024 2.30pm	
LOCATION		MA6	
AGENDA		Discussion about person in charge	
Meeting MC		Naza	
ATTENDANCE			
NAME		**TIME**	**REASON FOR ABSENCE**
Nazatul		1430	
Raudhah		1430	
Athirah		1430	KFK Meeting
Syafina		1430	Going home
MINUTES			
NO.	**ITEM DISCUSSED**	**IDEAS/SUGGESTIONS AND PERSON GIVING IT**	**PERSON IN CHARGE & DATE**
1	Instruction detail	Give instruction on how to divided work	Naza - 24/12
2	Appoint the person in charge for each work areas	Make a roulette which person is incharge which work area	Raudhah - 24/12
3	Create a detailed explanation for each room.	Start to create a detailed explanation for each room	Naza & Raudhah - 24/12

4	Next meeting	25/12 - determine what room would be considered work area	Raudhah & 25/12
5	Meeting ended	1700	

MEETING MINUTES

DATE/TIME		26/12/2024 8.30am	
LOCATION		MA6 & Online	
AGENDA		Discussion about arrangement device	
Meeting MC		Raudhah	
ATTENDANCE			
NAME		**TIME**	**REASON FOR ABSENCE**
Nazatul		0830	-
Raudhah		0830	-
Athirah		0830	-
Syafina		0830	-
MINUTES			
NO.	**ITEM DISCUSSED**	**IDEAS/SUGGESTIONS AND PERSON GIVING IT**	**PERSON IN CHARGE & DATE**
1	Discussed workflow	Update the incomplete work	Raudhah
2	Complete the Network Diagram	Using autocad to complete diagram with accurate cabling	Raudhah

3	Finalized the work	Clean the report format	Syafina
4	Next meeting	Task 5	Athirah
5	Meeting ended	1500	

TITLE: MEETING TASK 5

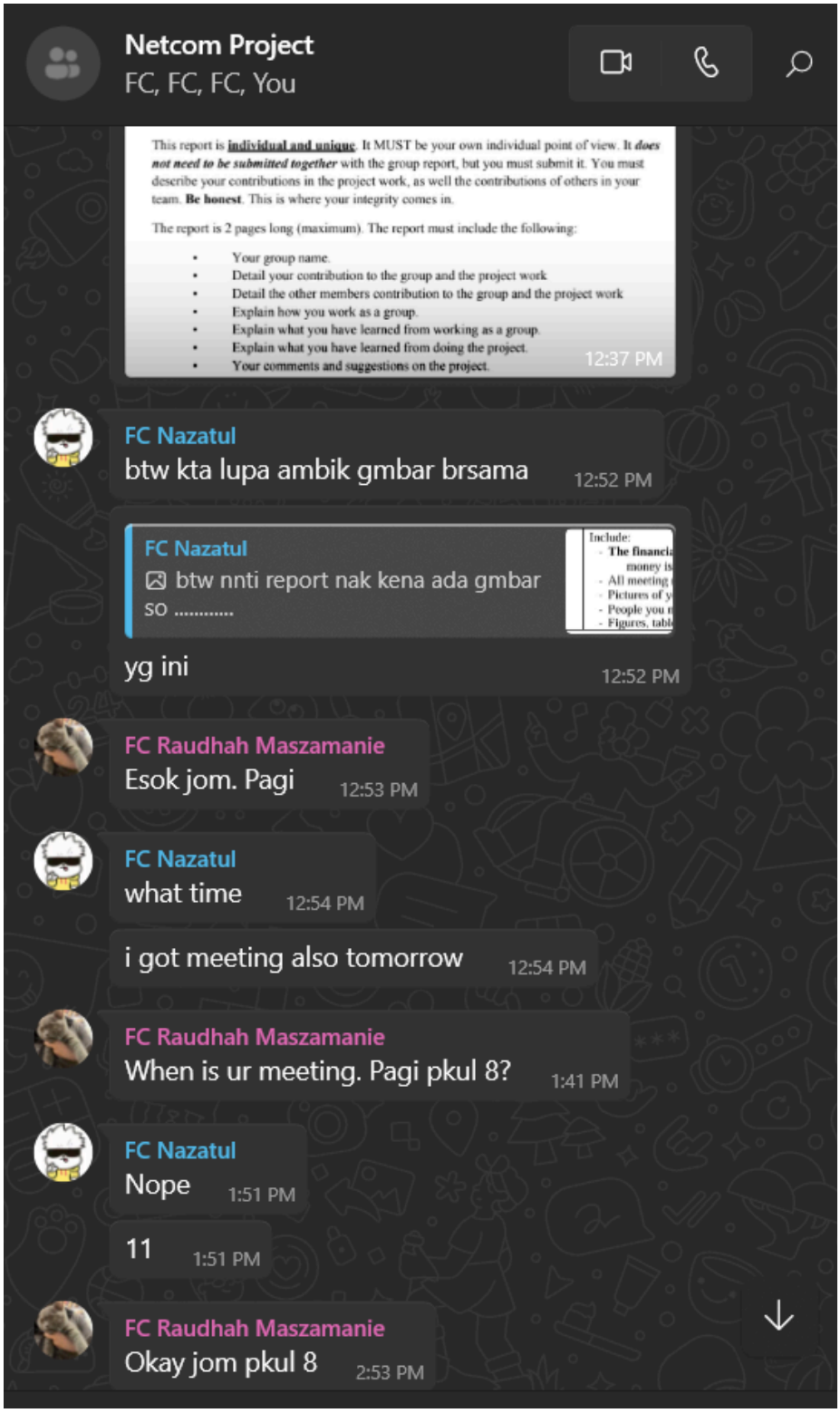
MEETING MINUTES

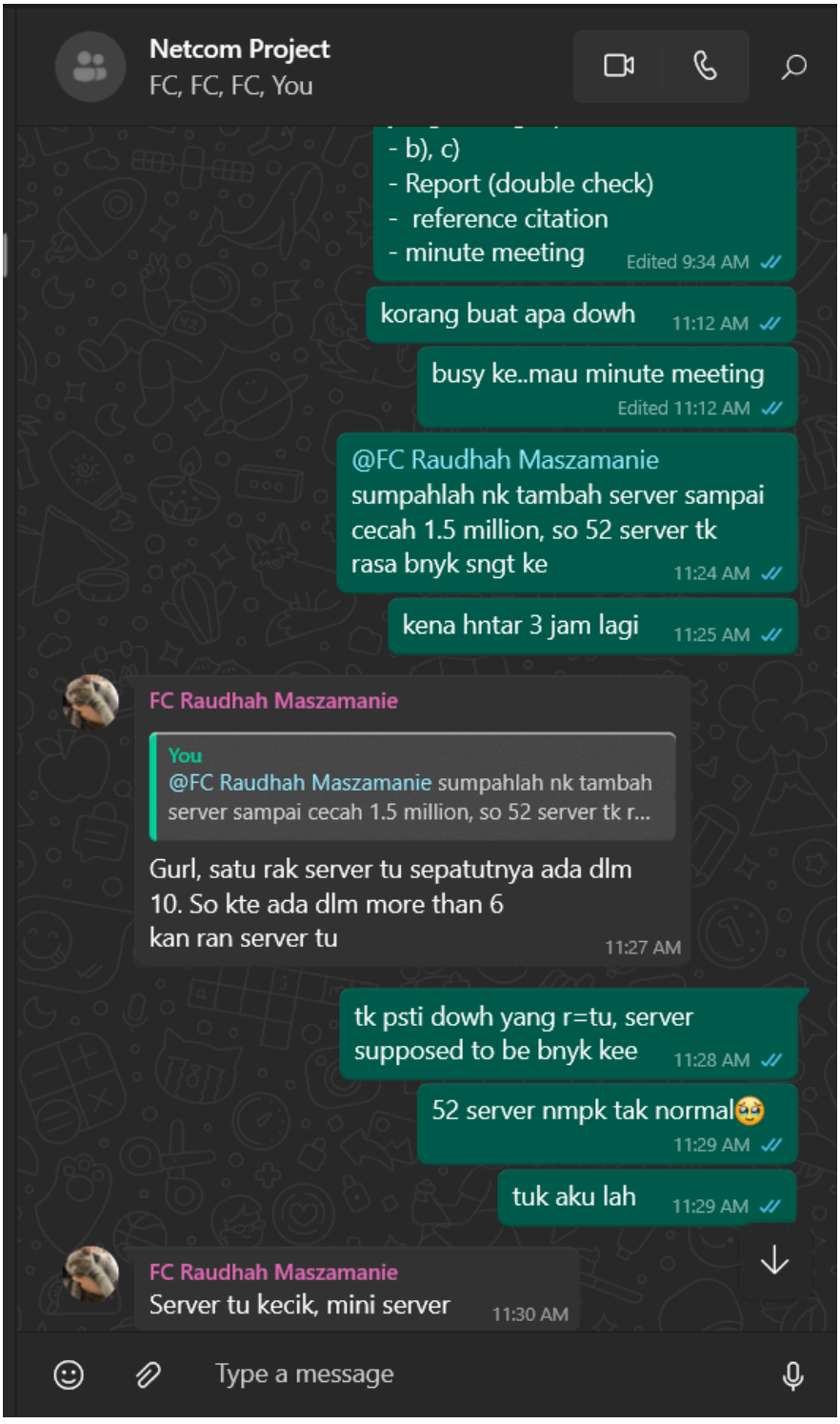
DATE/TIME		13/1/2025 9:30pm	
LOCATION		MA6	
AGENDA		Discussion on IP Addressing Scheme and Subnetting for Network Assignment	
Meeting MC		Athirah	
ATTENDANCE			
NAME		**TIME**	**REASON FOR ABSENCE**
Nazatul		2130	-
Raudhah		2130	-
Athirah		2130	-
Syafina		2130	-
MINUTES			
NO.	**ITEM DISCUSSED**	**IDEAS/SUGGESTIONS AND PERSON GIVING IT**	**PERSON IN CHARGE & DATE**
1	Obtaining Network Address from Lecturer	Naza will contact the lecturer to get the network address for the group.	Naza - 13/01

2	Dividing the Network Address into Subnets for Labs/Rooms	Raudhah suggested dividing the network based on the number of labs and rooms. Each lab/room should have enough addresses for all devices.	Raudhah - 13/01
3	Understanding IP Requirements for Each Lab/Room	Syafina proposed that a list be created for each lab and room, showing the number of hosts needed (computers, printers, etc.).	Syafina - 13/01
4	Subnetting Plan Discussion	Athirah discussed using CIDR notation to create subnets that will efficiently allocate IP addresses based on the required number of hosts.	Athirah - 13/01
5	Assigning IP Address Ranges to Each Lab/Room	The team agreed that Naza will handle assigning the specific IP address ranges to each room/lab once subnetting is completed.	Naza - 13/01
6	Documentation and Report for Submission	Athirah will document the entire subnetting process and IP address	Athirah - 13/01

		allocation for each room and lab. This documentation will be included in the final report.	
4	Next meeting	15/01 - finalize the IP addressing and subnetting details.	All - 15/01
5	Meeting ended	0000	

PICTURES OF TEAM WORKING ON THE PROJECT


Netcom Project
FC, FC, FC, You
This report is individual and unique. It MUST be your own individual point of view. It does not need to be submitted together with the group report, but you must submit it. You must describe your contributions in the project work, as well the contributions of others in your team. Be honest. This is where your integrity comes in.
The report is 2 pages long (maximum). The report must include the following:
Your group name.
Detail your contribution to the group and the project work
Detail the other members contribution to the group and the project work
Explain how you work as a group.
Explain what you have learned from working as a group.
Explain what you have learned from doing the project.
Your comments and suggestions on the project.
12:37 PM
FC Nazatul
btw kta lupa ambik gmbar brsama
12:52 PM
FC Nazatul
btw nnti report nak kena ada gmbar
so .....
yg ini
12:52 PM
FC Raudhah Maszamanie
Esok jom. Pagi
12:53 PM
FC Nazatul
what time
12:54 PM
i got meeting also tomorrow
12:54 PM
FC Raudhah Maszamanie
When is ur meeting. Pagi pkul 8?
1:41 PM
FC Nazatul
Nope
1:51 PM
11
1:51 PM
FC Raudhah Maszamanie
Okay jom pkul 8
2:53 PM


Netcom Project
FC, FC, FC, You
- b), c)
- Report (double check)
- reference citation
- minute meeting
Edited 9:34 AM
korang buat apa dowh
11:12 AM
busy ke..mau minute meeting
Edited 11:12 AM
@FC Raudhah Maszamanie
sumpahlah nk tambah server sampai cecah 1.5 million, so 52 server tk rasa bnyk sngt ke
11:24 AM
kena hntar 3 jam lagi
11:25 AM
FC Raudhah Maszamanie
You
@FC Raudhah Maszamanie sumpahlah nk tambah server sampai cecah 1.5 million, so 52 server tk r...
Gurl, satu rak server tu sepatutnya ada dlm 10. So kte ada dlm more than 6 kan ran server tu
11:27 AM
tk psti dowh yang r=tu, server supposed to be bnyk kee
11:28 AM
52 server nmpk tak normal
11:29 AM
tuk aku lah
11:29 AM
FC Raudhah Maszamanie
Server tu kecik, mini server
11:30 AM
Type a message

PEOPLE YOU MET TO DISCUSS THE PROJECT