UTM

UNIVERSITI TEKNOLOGI MALAYSIA

SECR1213 – NETWORK COMMUNICATION

TASK 2 – INITIAL DESIGN - PRELIMINARY ANALYSIS

SUBMITTED TO:

DR. MUHAMMAD ZAFRAN BIN MUHAMMAD ZALY SHAH (LECTURER)

PREPARED BY:

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

TABLE OF CONTENTS

TASK 2 – INITIAL DESIGN - PRELIMINARY ANALYSIS

a) Questions

1. What factors should we consider when anticipating an increase in users for each lab and classroom?
2. What types of devices (computers, printers, IoT devices, etc.) will be connected to the network in each area?
3. Are there any special security requirements for different rooms, like the Cisco Lab or Server Room?
4. How do we protect and keep important systems running?
5. What equipment is needed to keep things powered and cool?
6. How fast should the internet be?
7. What are the maintenance and support expectations for the network?
8. What type of router is needed for the labs?
9. What kind of network setup works best for the building?
10. Why should we set up smaller networks (subnetting) in the building?
11. What are the primary activities or applications to be supported by the network in each room?
12. How can we ensure the internet works well for everyone in the building?

b) Answers

1. In order to ensure effective learning experiences when anticipating an increase in users for labs and classrooms, several key factors should be considered. First, it is essential to provide sufficient equipment and materials that enhance students' mastery of the subject matter, as larger groups may require more resources for effective understanding. Additionally, planning for resources that support scientific reasoning is crucial, including software and equipment necessary for designing and analyzing experiments. As user numbers grow, addressing the inherent complexity and ambiguity of empirical work becomes increasingly important which includes offering additional support for troubleshooting, measurement error, and data handling.

   Furthermore, ensuring access to tools that facilitate the development of practical skills is vital, particularly in hands-on learning environments. It is also necessary to maintain a focus on the nature of science by providing ample resources that help students grasp scientific methods as class sizes increase. Lastly, creating collaborative spaces that foster teamwork and allow students to share equipment and responsibilities will support effective collaboration among peers. By considering these factors, educational quality and safety can be preserved while accommodating more students in laboratory settings (Anderson, 1976).[1]

2. The proposed network will incorporate several key devices to ensure efficient communication and resource sharing. Computers will serve various tasks and applications, providing users with the necessary tools for their work. Shared printers will be integrated into the network to facilitate printing needs across multiple users and departments, enhancing accessibility and efficiency. Internet of Things (IoT) devices, such as cameras and sensors, will connect to the network to enable data collection and control for various applications, contributing to a smarter environment. These devices will work together to support a dynamic and responsive network that adapts to the needs of the users.

   Moreover, in order to support the network infrastructure, switches will connect multiple devices within the Local Area Network (LAN), while managed switches will allow for advanced configuration and monitoring, ensuring optimal performance and reliability. Routers will direct traffic between different networks, enabling seamless communication with external networks. Additionally, firewalls will provide essential security by filtering traffic between trusted internal networks and untrusted external sources, safeguarding sensitive data and maintaining network integrity. Together, these devices will create a robust and secure network environment that supports the goals of the new building while promoting effective collaboration and communication among users (Schrader & Schrader, 2024). [2]

3. The network design features tailored security measures for specific rooms, especially the Cisco Lab and Server Room. A robust security perimeter is established at headquarters to protect valuable business information assets. Central to this security framework is the Cisco ASA 5500-X Series Midrange Adaptive Security Appliance (ASA), which provides multi-gigabit firewall capabilities along with intrusion prevention and detection services. Its compact design allows for easy integration, and it uses dedicated IPS hardware acceleration to monitor application-layer data for threats, enabling proactive blocking of malicious traffic based on content or sender reputation. The Cisco ASA firewall ensures that the network perimeter remains secure, protecting critical infrastructure from unauthorized access and potential attacks.

   Complementing the firewall, an Intrusion Detection System (IDS) enhances security by passively monitoring network traffic directed at protected VLANs. When threats are detected, alerts prompt immediate action from engineering or operational staff. The Cisco IPS can function in either IDS or IPS mode, offering flexibility to align with specific security policies. Given that internal threats can compromise data security, the server room, housing critical assets like customer records and financial data, requires stringent protection. This includes deploying Cisco ASA firewalls in active-standby configuration, alongside a basic firewall security policy and an integrated IPS. Regulatory requirements in certain sectors also necessitate enhanced security controls, underscoring the need for a comprehensive security strategy for the organization's server room and other critical areas (Server Room Technology Design Guide, 2013). [3]

4. To keep systems running efficiently, it's essential to regularly update operating systems with critical security patches, as outdated systems are more vulnerable to threats. Use reliable antivirus software, such as Windows Defender, Norton, or Kaspersky, and keep it updated to protect against malware. Additionally, update all utilities and applications to enhance security, performance, and access new features. Clear unnecessary files and uninstall unused programs using tools like CCleaner to reduce system clutter and prevent slowdowns. Be cautious during software installations to avoid bundled or harmful programs. For systems with hard disk drives (HDDs), perform regular defragmentation to optimize performance, but avoid this step for solid-state drives (SSDs) to preserve their lifespan. Following these steps ensures better system reliability and security over time (Monmouth Cyber, 2018). [4]

5. To keep systems powered effectively, specific equipment is essential. Deep-cycle batteries are vital for stand-alone systems, storing electricity for times when the energy source is inactive. These batteries work best with charge controllers, which regulate the electricity flow to prevent overcharging and extend battery life. Power conditioning equipment, such as inverters, is also crucial for converting direct current (DC) to alternating current (AC), ensuring compatibility with standard appliances. For grid-connected systems, additional meters and instrumentation are required to monitor power usage and comply with utility provider standards.

In order to ensure proper cooling and safety, well-ventilated and temperature-controlled spaces are necessary, especially for batteries and other sensitive components. Climate control prevents overheating and maintains equipment longevity in extreme environments. Safety equipment, such as surge protectors, grounding systems, and safety disconnects, protects the system from power surges, lightning strikes, and electrical faults. These measures are critical for maintaining system reliability and preventing damage (Energy Saver, n.d.). [5]

6. To ensure a fast and reliable internet experience, the recommended download speed is at least 100 Mbps, and the upload speed should be at least 10 Mbps. With these speeds, you can stream movies, attend video conferences, and play games online simultaneously on multiple devices. If you use streaming services or video conferencing apps like Zoom regularly, a minimum of 25 Mbps download speed is advisable. However, gigabit speeds may not be necessary for most households unless there are many users or devices connected, in which case a faster plan can prevent slowdowns and buffering. It's also important to keep your router updated and consider a mesh router system for better coverage (Xfinity, n.d.) [6]

7. The maintenance and support expectations for a network encompass proactive and strategic activities aimed at ensuring the smooth operation of the IT ecosystem, which includes both physical and non-physical assets. Key components include robust cybersecurity measures to protect against threats, ongoing performance analysis to address issues like bandwidth usage and connection lags, and scalability to accommodate growth within the organization. Regular hardware and software updates are essential to enhance performance and security, while compliance with internal and external regulations is a must. Additionally, preemptive repairs should be implemented based on analytics to identify and resolve potential issues before they escalate. These practices ensure that the network continues to operate efficiently and securely (Assoc. Prof. Dr. Norafida binti Ithnin, personal communication, 2024). [13]

   Network maintenance can be conducted by internal IT staff, original equipment manufacturers (OEMs), or through third-party maintenance (TPM) providers, each offering unique advantages. Ultimately, a structured network maintenance plan should include services such as troubleshooting, product installation and configuration, performance monitoring, growth planning, compliance assurance, and establishing robust network security to protect against breaches and ensure business continuity. By addressing these elements, organizations can ensure their networks operate efficiently and effectively, minimizing downtime and maximizing productivity (ITExamAnswers, 2024). [7]

8. For the labs, you will need to consider the type of routers and switches to purchase based on your needs for CCNA practice. Routers such as the Cisco 2900 series are highly recommended because they are affordable and support all necessary commands for both CCNA and CCNP. The Cisco 1800 and 2800 series are older models and may not support all CCNA features, but they can be useful if available for free. It's important to ensure that the router has sufficient flash memory and RAM for the operating system and processes. For switches, the Cisco Catalyst 3650 is a newer, reliable option suitable for both CCNA and CCNP. The router should also support protocols required for CCNA exams and allow you to practice various networking configurations (Real Hardware, n.d.). [8]

9. For the building, the best network setup involves optimizing the main router and access points (APs) for peak performance, ensuring the router is in a central location to cover as much area as possible. To extend the network range to distant areas, Ethernet cabling is the preferred method, as it provides reliable, high-performance connections. A wired Ethernet connection allows for the use of a switch to connect multiple devices in remote locations and can be paired with additional wireless APs to bring Wi-Fi to farther parts of the building. Alternatively, powerline adapters or mesh systems like AmpliFi, Eero, or Linksys Velop can also extend the network wirelessly or through electrical wiring, though Ethernet is always the best option despite its higher cost and potential need for physical modifications to the building. Wireless extenders are not recommended as they only offer the illusion of a better connection without improving performance
(TechTarget, 2024 July 14). [9]

10. In order to ensure efficient communication and resource sharing, the proposed network will integrate several key devices. Computers will provide users with the necessary tools for their work, while shared printers will enhance accessibility across departments. IoT devices, such as cameras and sensors, will contribute to a smarter environment through data collection and control. Switches will connect devices within the Local Area Network (LAN), with managed switches allowing for advanced configuration and monitoring to optimize performance. Routers will direct traffic between networks, ensuring seamless communication with external sources. Firewalls will filter traffic to protect sensitive data and maintain network integrity. Together, these devices will create a robust and secure network environment that supports collaboration and communication among users (Schrader & Schrader, 2024). [10]

11. The application refers to the specific software or program used to interact with and utilize network configurations in various settings, such as educational institutions or corporate environments. Key applications can include network management software, collaboration platforms, and learning management systems.

    Network Management Software allows administrators to configure, monitor, and manage network devices and performance. Examples of such tools include Cisco Prime, SolarWinds, and PRTG Network Monitor, which help ensure optimal network functionality.

    Collaboration Platforms, such as Microsoft Teams, Zoom, or Google Workspace, facilitate communication and collaboration over the network, enabling users to connect and share resources effectively. Similarly, Learning Management Systems (LMS) like Moodle, Canvas, or Blackboard provide access to educational resources, online courses, and assessments, enhancing the learning experience for students.

    In addition, file sharing services such as Dropbox, Google Drive, or OneDrive enable users to store, share, and collaborate on files over the network. Virtual Private Network (VPN) services offer secure remote access to the network for users working offsite, enhancing security and flexibility.

    IoT management platforms play a crucial role in managing and monitoring IoT devices connected to the network, facilitating automation and the integration of smart technologies. Moreover, data analysis tools like Tableau, Microsoft Power BI, or Google Analytics allow users to analyze and visualize data collected from networked systems, providing valuable insights for decision-making (Assoc. Prof. Dr. Norafida binti Ithnin, personal communication, 2024 November 22). [13]

    Lastly, helpdesk and support systems, such as Zendesk or ServiceNow, assist in managing IT support requests and issues related to network performance. Together, these applications leverage network configurations to enhance productivity, communication, and efficiency within various operational frameworks.

    To ensure the internet works well for everyone in the building, it is crucial to address common causes of poor wireless connectivity, such as distance from wireless access points (APs), interference, and outdated equipment. One effective solution is to use Distributed Antenna Systems (DAS), which amplify signals inside the building, overcoming obstacles like concrete or metal structures. For WiFi coverage, wireless repeaters can be deployed to extend the range and stabilize the connection in weak areas. Additionally, ensuring proper AP placement and regularly updating outdated equipment can significantly improve network performance and provide consistent coverage throughout the building (Twin, A. 2024, June 19). [11]

12. In order to ensure the internet works well for everyone in the building, it is crucial to address common causes of poor wireless connectivity, such as distance from wireless access points (APs), interference, and outdated equipment. One effective solution is to use Distributed Antenna Systems (DAS), which amplify signals inside the building, overcoming obstacles like concrete or metal structures. For WiFi coverage, wireless repeaters can be deployed to extend the range and stabilize the connection in weak areas. Additionally, ensuring proper AP placement and regularly updating outdated equipment can significantly improve network performance and provide consistent coverage throughout the building (Chicago Communications, May 14 2024). [12]

c) Feasibility

Technical Feasibility

From a technical point of view, this project is completely doable with the right tools and equipment. Associate Professor Dr. Norafida binti Ithnin (22 November 2024) emphasizes that the availability of necessary technology and resources plays a critical role in the success of such projects [13]. High-performance routers will be placed in busy areas like labs, while more affordable routers will be used in less crowded spaces. To ensure strong, consistent Wi-Fi coverage across the entire building, mesh systems will be used and add extra access points or extenders wherever needed to avoid dead zones. The network is also designed to grow easily, with features like VLANs and SDN that allows it to manage everything from one central point and scale up without needing new hardware. Uses reliable cabling like CAT6a and fiber optics to ensure fast speeds and a future-proof setup. To keep everything running smoothly, there will be dual routers for backup, so there's no downtime if one fails. Firewalls and VPNs will protect sensitive data, making sure everything stays secure in the academic environment. With a bit of careful planning and staff training, even older systems will fit in seamlessly, making the network both reliable and ready for future growth.

Economic Viability

Economic feasibility looks at whether a project is financially practical by comparing its costs to the benefits it will bring. Associate Professor Dr. Norafida binti Ithnin (22 November 2024)[13] highlighted that the RM3 million budget for this project is more than enough to cover everything needed for success. With this strong financial support, there is no worry about running out of funds, allowing every part of the project to be completed effectively. This budget ensures there are enough resources to hire skilled developers, use advanced tools, and create high-quality, engaging educational content for students and learners.

The funding also covers important costs like web hosting, server maintenance, and regular updates, making sure the system runs smoothly over time. It even allows for promoting the tools to schools, teachers, and astronomy enthusiasts, ensuring they reach the right audiences. With such a generous budget, the project can be managed well, meeting deadlines and maintaining high standards. By making good use of the RM3 million, the project not only remains financially stable but also supports SDG 4 by promoting quality and inclusive education.

Operational Feasibility

This project is designed to support the daily needs of students, staff, and faculty by providing reliable network coverage in labs, classrooms, lounges, and workspaces. With scalability in mind, features like VLANs make it easy to add more users and devices as needed. Backup paths are included to prevent downtime, so there's always a stable connection, even if one link fails. Firewalls will be managed carefully to maintain security without slowing down the network, and VPNs will ensure data privacy and provide safe remote access, which is especially important for hybrid and remote learning. With enough bandwidth to handle peak usage smoothly, the network is built to be efficient, user-friendly, and ready to adapt as demands grow.

To sum up, the network design project is doable when considering the technical, financial, and operational aspects. With careful planning and execution, the project will create a dependable and scalable network that meets the growing needs of the labs and classrooms. This improvement will make things run more smoothly for both students and staff, making it a worthwhile and beneficial investment.

MEETING MINUTES

Meeting minutes should follow this sample, filled with meaningful input. *Note: The red font is a suggestion.

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.

REFERENCES

1. Anderson, R.O. (1976). The experience of science: A new perspective for laboratory teaching. New York: Columbia University, Teachers College Press. Retrieved November 4, 2024. https://nap.nationalacademies.org/read/11311/chapter/5#77

2. Schrader, D., & Schrader, D. (2024, October 16). *Common types of network devices and their functions*. Netwrix Corporation. Retrieved November 4, 2024. https://blog.netwrix.com/network-devices-explained

3. *Server Room Technology Design Guide*. (2013). Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Retrieved November 4, 2024. https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2013/CVD-ServerRoomDesignGuide-AUG13.pdf

4. Monmouth Cyber. (2018, December 3). *How to maintain and keep your computer systems running properly.* Monmouth Cyber. Retrieved November 18, 2024, from https://www.monmouthcyber.com

5. Energy Saver. (n.d.). *Balance-of-system equipment required for renewable energy systems*. U.S. Department of Energy. Retrieved November 21, 2024, from https://www.energy.gov

6. Xfinity. (n.d.). *What is a good internet speed?* Retrieved November 21, 2024, from https://www.xfinity.com

7. ITExamAnswers. (2024, May 14). 10.4.4 Lab - Build a switch and router network (Answers). *ITExamAnswers.net*. Retrieved November 4, 2024. https://itexamanswers.net/10-4-4-lab-build-a-switch-and-router-network-answers.html#google_vignette

8. Real Hardware. (n.d.). *Real Hardware for CCNA and Networking Labs*. Retrieved November 22, 2024, from https://www.realhardware.com

9. TechTarget. (2024, July 10). *Tips for setting up a home network*. Retrieved November 20, 2024,from https://www.techtarget.com/searchnetworking/tip/Tips-for-setting-up-a-home-network#:~:text=Ethernet%20cabling%20is%20always%20the,connecting%20it%20to%20one%20client

10. Cisco Learning Network. (2020, February 16). *Single large vs multiple small subnets*. Retrieved from https://learningnetwork.cisco.com/s/question/0D53i00000Kt3RBCAZ/single-large-vs-multiple-small-subnets

11. Twin, A. (2024, June 19). *Internet Service Provider (ISP): What they do and examples*. Investopedia. Retrieved November 4, 2024. https://www.investopedia.com/terms/i/isp.asp

12. Chicago Communications. (2024, May 14). *Solving Poor In-Building Connectivity: Causes and Solutions*. Retrieved November 22, 2024, from https://www.chicomm.com/blog/solving-poor-in-building-connectivity-causes-and-solutions

13. 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