UTM

UNIVERSITI TEKNOLOGI MALAYSIA

FACULTY OF COMPUTING

SEMESTER 1 2024/2025

SECR1213 – NETWORK COMMUNICATIONS

SECTION 12

PROJECT TASK 2

LECTURER: MR. FIROZ BIN YUSUF PATEL DAWOODI

GROUP 12.1 (POWERPUFF)

STUDENT NAME	MATRIC NO
CHRYL CHEONG KAH VOON	A23CS0060
LAU YEE WEN	A23CS0099
CHUA JIA LIN	A23CS0069
GUI KAH SIN	A23CS0080

TABLE OF CONTENTS

QUESTIONS

1. What is the minimum bandwidth required to support the expected number of users of the Faculty of Computing?

Table 1.1 Bandwidth required for different type of activities [1]

Type of Activities	Examples	Bandwidth required	Bandwidth required (Average)
Slow	- VoIP calls - Emails	Up to 1 Mbps	0.5 Mbps
Medium	- Using business software	1 – 4 Mbps	2.5 Mbps
Fast	- Video conferencing - Video streaming in HD - Downloading large files	5 – 15 Mbps	10 Mbps
Very fast	- Application update - File sharing	16 – 25 Mbps	20.5 Mbps
			Total = 33.5 Mbps
			Average bandwidth for all activities = 8.375 Mbps

The expected number of users of Faculty of Computing in next 4 years is approximately 2231 users including both undergraduate and postgraduate students, academic staffs, and supporting staffs. Assuming only 25% (558 people) of the total users will use the network simultaneously, the estimated bandwidth required is 4.7 Gbps. Therefore, a minimum bandwidth of 4.7 Gbps is required for the building to support the expected number of users of the Faculty of Computing.

2. What is the basic hardware's to build a network and how do they work together?

To build a network for the new building of the Faculty of Computing, hardwares such as routers, switches and wireless access points are required. The function of router is to connect different networks and direct data packets between networks [2]. The usage of the switch is to connect devices within a local area network and direct data to necessary devices. The purpose of using a Wireless Access Point is to provide wireless connectivity to a wired network and enable devices to connect to the network wirelessly. With these hardwares, a

situation can be demonstrated to explain how these devices collaborate. A user connects his mobile device to Wi-Fi through the Wireless Access Point. When the user wants to access a website, the wireless access point will send the device's data to the switch and the switch will transfer the data to the router and the router will send the data to the Internet [3]. When the requested data comes back from the Internet, the data will be transferred back to the user's device through the router, switch, and Wireless Access Point.

3. What are the requirements needed to build an effective video conferencing room?

   There are multiple requirements needed to build an effective video conferencing room including a stable Internet connection, sound system and microphone, and display system [4]. A stable Internet connection with bandwidth of 5 – 15 Mbps is crucial to prevent poor audio and video quality and communication delays during the virtual project meeting. Besides, having a loud and clear speaker is important to ensure all the participants can hear the meeting clearly. A microphone is required for participants who have a quiet voice. Moreover, a projector and projector screen are a must for the video conferencing room so that all participants can view the project details clearly. Therefore, the video conferencing room should consist of a stable Internet connection, speaker, microphone, projector, and projector screen to ensure a high-quality meeting experience.

4. How to make sure the whole building gets wireless network coverage?

   There are some ways to make sure the whole building gets wireless network coverage, and they are implementing ceiling-mount Wireless Access Points, use multiple Wireless Access Points, and use Power over Internet [5]. The implementation of ceiling-mount Wireless Access Point is to reduce interference of obstacles on the ground such as tables and chairs. The advantages of using multiple Wireless Access Points are to ensure overlapping coverage of wireless connection in the building to ensure user obtain continuous connectivity while moving to anywhere in the building. Power over Internet is method that connects the Wireless Access Points with Ethernet cables that carries network data to ease the planning of location of implementing Wireless Access Points. In

conclusion, implementing ceiling-mount Wireless Access Points, using multiple Wireless Access Points, and applying Power over Internet can make sure that whole building can get wireless network coverage.

5. How can the network be secured against Internet Worms and denial-of-service attacks?

Several strategies can be used to protect a network from denial-of-service (DoS) attacks and Internet Worms. First, in order to safeguard the network, intrusion detection systems (IDS) must be put in place. Before directing additional actions to counter a DoS attack, detection is a crucial step. [6] Installing personal firewalls on individual systems, for instance, can assist in detecting attacks on devices, particularly in settings with a high computer density, like large organizations or universities. Another essential step is routinely monitoring network activity, which makes it possible to quickly identify traffic irregularities and react to possible threats. Additionally, network security is greatly aided by user education. Users should get training in how to identify irregularities in their systems and be urged to notify the IT support staff right away if they notice any suspicious activity. To evaluate these reports and create efficient countermeasures, an intelligence-gathering system can be set up. Furthermore, security protocols stay strong and current when established best practices and guidelines from reliable organizations like CERT/CC and SANS are followed. Since these packets frequently reveal IP spoofing, firewalls should instantly reject any that contain any RFC 1918 or reserved IP addresses in the IP Source Address or Destination Address fields. [7] We may develop a thorough protection against denial-of-service attacks, Internet Worms, and other cyberthreats in a network by integrating these strategies.

6. What devices are needed to achieve efficiency in the hybrid classroom?

To be efficient in a hybrid classroom, several devices and considerations are required, particularly when integrating a cloud-based video conferencing system. Computers and networking are critical components for smooth operations. If the computer used in the video conferencing system does not have enough processing power and memory, the audio

and video quality may suffer during teaching sessions. While no specific studies have determined the exact specifications for such computers, video conferencing platform websites recommend that a suitable computer have at least 2GB of memory and a quad-core processor capable of supporting 720p video resolution. A slow network can have an equal negative impact. A minimum bandwidth of 2 Mbps is required for effective online video conferencing. Additionally, for hybrid classroom configurations, both the internal distributed network and the campus WAN link must have sufficient bandwidth to handle the load. Since cloud-based video conferencing systems rely heavily on internet connectivity, expanding campus internet bandwidth is an important consideration. It is also recommended that classroom computers be connected to the network via Ethernet cables rather than Wi-Fi, as Ethernet offers more bandwidth and avoids sharing connections with other devices [8]. To ensure efficient data transmission, distribution network switches that connect classroom computers to the campus core network switch should meet Gigabit Ethernet standards.

A visualizer is another useful tool for hybrid classrooms. It can connect to the classroom computer via USB cable and serve as a camera. Instructors can easily switch from video conferencing software to using the visualizer's camera to write or annotate directly on paper, resulting in a more interactive learning experience. These devices, combined with high-speed internet, appropriate computer specifications, and a strong network infrastructure, ensure that hybrid classrooms run smoothly, providing an engaging and seamless experience for both in-person and remote students.

7. What type of network cable is best suited for connecting computers, and why?

Category 6 (Cat 6) Ethernet cable is ideal for connecting computers. CAT6 is the sixth generation of Ethernet cabling used in business and home networks, as well as the current "typical" cabling standard for modern office buildings. These cables can handle Ethernet data rates of up to one gigabit per second. Cat 6 cables can deliver speeds of up to 10 Gbps over short distances (up to 55 meters) and 1 Gbps over longer distances, making them ideal for high-performance labs and classrooms. [9] Furthermore, school environments typically contain many electronic devices, such as computers, projectors, and lab equipment, which

can cause electromagnetic interference (EMI). Cat 6 cables, particularly shielded ones (e.g., F/UTP or S/FTP), provide enhanced EMI protection, resulting in a stable and reliable connection.[10] Lastly, although Cat 6 is more costly than Cat 5e, it is more economical and efficient than fibre optics or more expensive cables like Cat 6a [11]. Apart from that, we also don't recommend fiber optic cables because it is fragile compared to other electrical wires and causing the installation work to be more difficult.

8. Which Internet Service Provider is most suited for developing the building's network?

The best Internet service provider for setting up the network infrastructure in the new building is Telekom Malaysia (TM) Unifi. As the top ISP in Malaysia with the most extensive fiber coverage, TM Unifi guarantees a dependable and effective network connection for every user. It is capable of meeting the demands of academic activities, such as research, video conferencing, and online learning, with speeds of up to 2 Gbps. Furthermore, TM Unifi's extensive service network, featuring over 20 centers in Johor alone, provides reliable technical support and maintenance, ensuring quick resolution of any issues. [12]. TM Unifi is the best option for this project because of its speed, coverage, and customer support.

Collapse Table —	100Mbps	300Mbps (Recommended)	500Mbps	1Gbps	2Gbps
	From RM 129 /mth* RM139 Select	From RM 199 /mth* RM249 Select	From RM 239 /mth* RM299 Select	From RM 319 /mth* RM349 Select	From RM 369 /mth* RM399 Select
User	**Flexible Micro Office** Supports up to 2-3 users on 5 devices.	**Small Outlet Office or Small NGO Office** Supports up to 6 users on 10 devices.	**Virtual Office / Shop** Supports up to 10 heavy users on multiple devices.	**Larger Business Premise Setting** Supports up to 10 power users on multiple devices.	**Larger Business Premise Setting** Ultimate support for up to 10 power users on multiple devices.
Free Business Call Plan (Simple Voice Plus)	SVP50	SVP50	SVP70	SVP70	SVP70

9. What specific redundancy and backup solutions are required?

Data redundancy ensures protection and consistency by repeating information across different systems using techniques such as RAID configurations, database replication, or cloud-based storage [13]. Network redundancy improves reliability by providing

alternative data transmission paths, such as parallel Internet Service Providers (ISPs) or redundant equipment like routers and switches to prevent connectivity failures. For backup, we can choose cloud-based backup solutions, such as Google Drive, to keep data in all labs and faculty up to date and recoverable in the event of a disaster or system failure. Together, these methods provide strong protection, ensure smooth operations, and meet the Faculty of Computing's requirements for a flexible, safe, and efficient infrastructure.

10. How can the network be designed to accommodate future growth?

    The important aspect of network infrastructure planning is to ensure the network can scale with our business. If your organization becomes bigger, the demand for the network will also grow. The modular network design such as modular switches and routers will be the best choice because it can allow us to add devices or users without affecting the performance. The next is the security part to protect our data and users. Security is the most important part of designing the network. We can implement a firewall in our network to block unauthorized users and we can divide the network into segments based on their sensitivity [15].

11. What type of server infrastructure is required to support the faculty's growing needs?

    Hybrid on-premises and cloud-based infrastructure is most suitable to support the faculty's growing needs. The on-premises server is housed within our faculty to protect academic and research data that provide low-latency performance. The cloud-based server is hosted by third-party providers that offer scalability and affordability. The hybrid solution depends on the availability of a public cloud platform from a trusted third-party cloud provider either on-premises or through a hosted private cloud provider [17]. By converting the benefit of both servers, our faculty can achieve optimal security, flexibility and performance.

12. What tools and techniques can be used for real-time monitoring and management of the network to ensure high availability and performance?

To ensure high availability and performance for real-time monitoring and management of the network, we can use some tools such as ManageEngine OpManager. It can provide deep visibility into the performance of our router, switches, firewall, load balancer, wireless LAN controller, servers, VMs, printer and storage devices. It is an easy-to-use and cost-efficacy network monitoring solution that allows us to drill down to the root cause of an issue and eliminate it [18]. Besides, we can also use packet analysis as a technique for real-time monitoring and management to identify traffic patterns, anomalies and performance bottlenecks and ensure high availability.

13. How will the wireless infrastructure integrate with future technologies, such as 5G or beyond?

To future-proof wireless infrastructure, adopting Wi-Fi 6 or Wi-Fi 6E standards is essential, as these offer high data rates, reduced latency and improved efficiency in high-density environments [20]. These access points should be compatible with 5G backhaul connections, allowing seamless connectivity and integration for users in faculty of computing. Additionally, planning for Wi-Fi 7, which is expected to fine-tune Wi-Fi 6/6E features, will bring enhanced throughput and low latency, ensuring longevity [20].

The network design should incorporate software-defined networking (SDN) to enable dynamic reconfiguration, allowing the infrastructure to integrate emerging technologies easily. SDN's concept is based on ideas of generalization network hardware and decoupling the network controls software from the implementation devices [21], enabling the data control from a central and external software entity. The inclusion of edge computing devices will also help offload processing from cloud systems, paving the way smooth transition to advanced IoT and 5g-enabled applications.

14. What strategies will be used to address potential interference in Wi-Fi coverage (e.g., overlapping channels, material obstacles)?

    Effective Wi-Fi design will minimize interference by conducting a comprehensive site survey using tools like AirMagnet, Ekahau or NetSpot. This survey identifies dead zones and overlapping channels of the coverage area by creating heatmaps of the signal, noise, and SNR [22]. Wi-fi 6 access points should be strategically placed using dual-band (2.4 GHz and 5 GHz) channels to reduce congestion. Deploying ceiling-mounted access points avoids physical obstructions such as furniture and ensures even coverage.

    Channel planning will ensure non-overlapping frequencies, while features like MU-MIMO (Multi-user, Multiple Input, Multiple Output) will optimize performance in high density areas [23]. Therefore, signal repeaters or mesh systems can extend coverage to hard-to-reach areas. For material obstructions, Wi-Fi transparent barriers, such as low-e glass panels, can be installed to reduce signal loss.

15. What network configurations will support the specific needs of the Cisco and Embedded Labs?

    The Cisco and Embedded Labs require tailored network configurations to support their specialized function effectively. For the Cisco Lab, which serves as a teaching lab, it needs to be equipped with specific networking devices to facilitate teaching and hands-on practice. Thus, Virtual Local Area Networks (VLANs) are essential to segment network traffic for different devices and enhance both performance and security [24]. Network devices like routers, switches, and firewalls, should be used to allow students to practice industry-standard network configurations [25]. Layer 3 switches for routing between VLANs and QoS to prioritize critical traffic are vital. Besides, simulation tools like Cisco Packet Tracer could provide virtualized environment for students when physical devices are limited.

    While the Embedded Lab, the focus is on IoT devices and sensors, requiring a network that supports low-power, high density devices. IoT protocols like MQTT and CoAP should be supported, and PoE (Power over Ethernet) switches will help power devices through the Ethernet cable. Both labs will benefit from high speed wired connections and Wi-Fi 6 for

mobile access, while VLANs will ensure security by segmenting traffic. Network monitoring tools should be deployed to maintain optimal performance across both labs.

16. How to strengthen network security?

Network security is a rather broad term that essentially focuses on the protections that computer networks have against potential misuse, malfunction, modification, destruction, or improper disclosure of network resources, as well as against illegal access. It covers a wide range of technologies, devices, and procedures intended to protect computer networks and data's accessibility, privacy, and integrity [26]. Therefore, the network security of Faculty of Computing needs to be taken seriously to avoid the ever-growing landscape of cyber threats in the wild today.

First and foremost, we could implement the 802.1X network authentication to the network of our faculty. This is due to the reason that it only opens ports for network access when users' identities have been authenticated and authorized based on their login credentials, such as username and password or certificates. Other than that, it is also used to secure connections to wired and wireless networks via rotating key security and avoiding unencrypted connections. It can secure the user's privacy since 802.1X authentication protects people from walking in and releasing a virus, malware, or man-in-the-middle attack. Furthermore, it is also used on the Extensible Authentication Protocol (EAP), which provides a secure method to send identifying information over-the-air that can prevent outside users from intercepting information and protect user privacy [26].

Furthermore, the fundamental yet crucial network security techniques must be implemented. For instance, firewalls such as stateful firewalls or next-generation firewalls (NGFWs) monitor and control incoming and outgoing network traffic and serve as the barrier between trusted and untrusted networks, blocking unauthorized access [27]. Besides, virtual private networks (VPNs) should also be considered, as they encrypt data transmitted between remote users and the faculty network to ensure secure communication channels over public networks. It also helps safeguard sensitive information, keeping it confidential and secure from eavesdropping or interception [27].

Feasibility Assessment

The feasibility assessment for the Faculty Computing's network project involves evaluating technical, economic and operational viability.

Technical Feasibility:

Based on the information gathered, the project is technically feasible. The hybrid infrastructure method combines on-premises and cloud-based servers to ensure our faculty can achieve optimal scalability, flexibility and security. The modular network design, structured cabling and modern technology such as switches and access points can maintain network performance while the number of users grows fast. The technical plan is suitable for academic and administrative needs since it involves redundancy, high-speed connectivity and reliable cybersecurity.

Economic Feasibility:

The economic feasibility is supported by cost-effective measures such as optimizing network resources, load balancing and integrating cloud-based solutions which can eliminate the need for additional physical infrastructure. The energy-efficient design like a modern cooling system can also lower the operational cost. Thus, cloud-based integration can reduce the initial investment and lead to long-term break even.

Operational Feasibility:

Given that it meets the faculty's present and future operational requirements, the project has a high operational feasibility. The suggested hybrid infrastructure enables seamless integration with current IT resources and procedures by combining cloud-based and on-premises solutions. The network infrastructure's modular design guarantees that it can grow with the faculty, supporting more users and devices without causing any problems. Additionally, the current IT team will be able to efficiently manage the network through staff training and the implementation of user-friendly monitoring tools. Well-defined backup and recovery plans, frequent updates, and system evaluations are all helpful in guaranteeing continuous operation and reducing downtime. User experience is also given top priority in the project's design, which offers stable and smooth connectivity throughout labs, classrooms, and the faculty overall.

MEETING MINUTES #1

DATE/TIME	14 Nov 2024 2pm		
LOCATION	M01, KTDI		
AGENDA	1. Understand details about task 2 2. Suggest possible questions for task 2 3. Select suitable questions from all suggestions 4. Task distribution for all members		
Meeting MC	Cheryl Cheong Kah Voon		
ATTENDANCE			
NAME	**TIME**	**REASON FOR ABSENCE**	
Lau Yee Wen	2:00PM	-	
Cheryl Cheong Kah Voon	2:00PM	-	
Chua Jia Lin	2:00PM	-	
Gui Kah Sin	2:00PM	-	
MINUTES			
NO.	**ITEM DISCUSSED**	**IDEAS/SUGGESTIONS AND PERSON GIVING IT**	**PERSON IN CHARGE & DATE**
1	Discussion for Task 2	- All members opened the word document related to project Task 2 on their respective laptops. - All members read the question and rubric together. - All members discussed the requirements for Task 2.	All members
2	Suggestions for questions	- Jia Lin suggested every member to suggest 5 questions and 16 questions will be picked from 20 questions. - Each member suggested 5 questions that are suitable for Task 2.	All members
3	Select suitable questions	- Kah Sin suggested selecting 16 questions using poll. - 16 questions successfully selected.	All members
4	Task Distribution	- All members need to do research to find a solution for the questions selected. - Yee Wen suggested distributing tasks using “Wheel of Names”. - Cheryl and Yee Wen were assigned to complete the feasibility study.	All Members

		- Jia Lin was assigned to prepare the meeting minutes. - Kah Sin was assigned to arrange the list of references and format the report for Task 2.	
5	Next meeting	Scheduled for November 21, 2024. Tasks 2 need to be completed by then.	
6	Meeting ended	At 4:20 pm, the meeting ended after all discussions had been done.	

MEETING MINUTES #2

DATE/TIME		21 Nov 2024 2pm	
LOCATION		M01, KTDI	
AGENDA		1. Explain answers for selected questions 2. Choose most suitable answers for all selected questions 3. Discuss about feasibility of the project	
Meeting MC		Gui Kah Sin	
ATTENDANCE			
NAME		**TIME**	**REASON FOR ABSENCE**
Lau Yee Wen		2:00PM	-
Cheryl Cheong Kah Voon		2:00PM	-
Chua Jia Lin		2:00PM	-
Gui Kah Sin		2:00PM	-
MINUTES			
NO.	**ITEM DISCUSSED**	**IDEAS/SUGGESTIONS AND PERSON GIVING IT**	**PERSON IN CHARGE & DATE**
1	Explain answers for selected questions	- All members explained the solution they researched for all selected questions.	All members
2	Choose most suitable answers for all selected questions	- After each member explained their answer for the questions, the final answers were decided by voting the most suitable solution. - Jia Lin jotted down the final answer in a word document.	All members
3	Discuss about feasibility of the project	- Cheryl and Yee Wen explained the feasibility of the project to other team members.	All members

		- Kah Sin was confused about the operational feasibility - Cheryl and Yee Wen explained the operational feasibility to Kah Sin in detail.	
6	Meeting ended	At 5:00 pm, the meeting ended after all discussions had been done.	

REFERENCES

1. Palmer, R. (2026, June 21). *How much internet speed do you need? (2024 guide) | Switchful*. Switchful. https://www.switchful.com/service/internet/resource/how-much-internet-speed-you-need
2. *Top network hardware devices and their functions*. (n.d.). https://www.uninets.com/UniNets. https://www.uninets.com/blog/network-hardware-devices
3. IndoClass. (2024, November 13). *Computer Network architecture - Basic concept of transferring data* [Video]. YouTube. https://www.youtube.com/watch?v=EqS2FAse1lg
4. Virtual Meeting World. (2024, May 31). *Video Conferencing Room setup Requirements Checklist* 📋✔. https://virtualmeetingworld.com/equipment/video-conferencing-requirements/
5. Sam. (2023, June 6). *Wireless Access Point Placement best practices*. Cablify. https://www.cablify.ca/wireless-access-point-placement-best-practices/
6. Abliz, M. (n.d.). *Internet Denial of Service Attacks and Defense Mechanisms*. Retrieved from https://blog.oureducation.in/wp-content/uploads/2014/06/Internet-Deniel.pdf
7. Bosworth, S., & Kabay, M. E. (2002). *Computer Security Handbook*. John Wiley & Sons.
8. Triyason, T., Tassanaviboon, A., & Kanthamanon, P. (2020). Hybrid Classroom. *Proceedings of the 11th International Conference on Advances in Information Technology*. https://doi.org/10.1145/3406601.3406635
9. CAT5E, CAT6, CAT7, CAT8: Which To Choose? | Telco Data. (2021, January 11). Retrieved from www.telco-data.com website: https://www.telco-data.com/blog/cat-cables/

10. Martindale, J. (2019, October 17). How to choose an Ethernet cable. Retrieved November 26, 2024, from Digital Trends website: https://www.digitaltrends.com/computing/different-types-of-ethernet-cables-explained/#dt-heading-shielding-and-foil-wrapping
11. luciaclemares. (2023, June 21). What is Ethernet and what kinds of cables exist? Retrieved from Telefónica website: https://www.telefonica.com/en/communication-room/blog/what-is-ethernet-kinds-cables-exist/
12. Explore Nearby Unifi Store/TMpoint for Your Convenience. (2024). Retrieved November 26, 2024, from Unifi website: https://unifi.com.my/support/find-tm-point?query=&state=Johor
13. Talend. (n.d.). *What is Data Redundancy - Definitions and Drawbacks*. Talend - a Leader in Data Integration & Data Integrity. https://www.talend.com/resources/what-is-data-redundancy/
14. https://www.indeed.com/career-advice/career-development/network-redundancy#:~:text=Network%20redundancy%20is%20a%20process,of%20errors%2C%20damage%20or%20shutdowns. (cannot cite)
15. Ramon J Matos. (25 October 2024). *Top 5 Considerations When Planning a New Network Infrastructure.* LinkedIn https://www.linkedin.com/pulse/top-5-considerations-when-planning-new-network-ramon-j-matos-1tzpe/
16. Lauren Ballejos. (11 November 2024). *What is server Infrastructure?* NinjaOne. https://www.ninjaone.com/it-hub/endpoint-management/what-is-server-infrastructure/#:~:text=There%20are%20primarily%20two%20types,the%20function%20of%20the%20server.
17. Aaron Keeports. (2024). *On Premise vs. Cloud: Key Differences, Benefits and Risks* Cleo. https://www.cleo.com/blog/knowledge-base-on-premise-vs-cloud
18. ManageEngine, communications@manageengine.com. (2019). Network Monitoring Software by ManageEngine OpManager. ManageEngine OpManager. https://www.manageengine.com/network-monitoring/network-monitoring-tools.html
19. Cem Dilmegani. (8 Oct 2024) *Real time network performance monitoring: techniques & Tools.* AI Multiple Research. https://research.aimultiple.com/real-time-network-performance-monitoring/

20. Edirisinghe, S., Galagedarage, O., Dias, I., & Ranaweera, C. (2023). Recent Development of Emerging Indoor Wireless Networks towards 6G. Network, 3(2), 269–297. https://doi.org/10.3390/network3020014

21. Imran, Ghaffar, Z., Alshahrani, A., Fayaz, M., Alghamdi, A. M., & Gwak, J. (2021). A Topical Review on Machine Learning, Software Defined Networking, Internet of Things Applications: Research Limitations and Challenges. *Electronics*, *10*(8), 880. https://doi.org/10.3390/electronics10080880

22. Eric_Geier. (2021, February 18). *How to fix Wi-Fi interference*. Network World. https://www.networkworld.com/article/734150/coping-with-wi-fi-s-biggest-problem-interference-2.html

23. Goss, M. (2023, October 18). *Wi-Fi 6 vs. 5G: What's the difference?* Search Networking. https://www.techtarget.com/searchnetworking/feature/A-deep-dive-into-the-differences-between-5G-and-Wi-Fi-6

24. *What is Network Configuration? | VMware Glossary*. (n.d.). https://www.vmware.com/topics/network-configuration

25. Organization, S. (2017). Virtual Local Area Network (VLAN): segmentation and security. *Sdiwc*. https://www.academia.edu/35497133/Virtual_Local_Area_Network_VLAN_Segmentation_and_Security