FACULTY OF COMPUTING

SECR1213 - NETWORK COMMUNICATIONS

TASK 2: INITIAL DESIGN - PRELIMINARY ANALYSIS

LECTURER:

DR. RAJA ZAHILAH BINTI RAJA MOHD RADZI

GROUP 3: THE PHOENIX

GROUP MEMBER:

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

TASK 2: INITIAL DESIGN - PRELIMINARY ANALYSIS

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

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

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

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

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

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

Instructions to Set Up LAN Network

Create Network

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The Domain Name System (DNS) is the Internet's phone book because humans access information online through domain names. Web browsers interact via Internet Protocol (IP) addresses and DNS translates domain names to IP addresses so that browsers can load Internet resources. The DNS system is not designed with security in mind like most Internet protocols and it may contain some design limitations. These limitations when combined with advances in technology make DNS servers vulnerable to a wide spectrum of attacks, including spoofing, amplification, DoS (Denial of Service), or interception of private personal information. Then, since DNS is part of most Internet requests, it can be a prime target for attacks. We may use tools or software such as DNSSEC used to protect against attacks by digitally signing data to help ensure its validity. A DNS firewall can also be used because it provides some security and performance services for DNS servers.

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

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

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

Question 5: How to ensure network security?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Project Feasibility

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

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

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

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

The equipment that will be used in the building such as routers, modems and assessment points have been identified. Which cable type is suitable for our building has also been identified. All the equipment and floor plan that we plan are able to achieve and we already considered all the things that are quite important for us such as IP address. Thus, it can be said that the floor plan is feasible.

References

1. Cybersecurity & Infrastructure Security Agency (CISA). (2018, June 21). *Security Network Infrastructure Devices*. Retrieved November 7, 2022, from https://www.cisa.gov/uscert/ncas/tips/ST18-001
2. Teodor Topalov. (2015). *An Overview of Essential Security Measures for Competitive Organizations*. Retrieved November 7, 2022 from http://www.inquiriesjournal.com/articles/1269/2/an-overview-of-essential-security-measures-for-competitive-organizations
3. Finn McChuhil. (2018). *How to Set Up IP address for an Office*. Retrieved November 7, 2022, from https://smallbusiness.chron.com/set-up-ip-addressesoffice-51486.html
4. Anthony Novello. (2020). *How a Fiber Optic Backbone Network Can Save You Down Time*. Retrieved November 7, 2022, from https://www.buildingsiot.com/blog/how-a-fiber-optic-backbone-network-can-save-you-down-time-bd#:~:text=Benefits%20include%3A&text=Easier%20to%20install%20due%20to,considerable%20resistance%20to%20electromagnetic%20interference
5. AH Ari Howard Sep 7, & Howard, A. (2022, October 11). *Internet speeds explained: How to pick The speed you need*. Allconnect. Retrieved November 7, 2022, from https://www.allconnect.com/blog/consumers-guide-to-internet-speed
6. Vertiv. (2021, June 30). *What is a server room?*. Retrieved November 7, 2022, from https://www.vertiv.com/en-asia/about/news-and-insights/articles/educational-articles/what-is-a-server-room/
7. Prasanna Bidkar. (2022). *How Do Routers Provide Security?*. Retrieved November 8, 2022 from https://smallbusiness.chron.com/routers-provide-security-70778.html
8. CloudFlare. (2022). *What is a Router?*. Retrieved November 8, 2022 from https://www.cloudflare.com/learning/network-layer/what-is-a-router/
9. John Burke. (2020, June). *Network Switch*. Retrieved November 8, 2022 from https://www.techtarget.com/searchnetworking/definition/switch
10. Jessica Ciesla. (2018, May 29). *Secure Switches Can Defend Against Cyber Attacks*. Retrieved November 8, 2022 from https://www.raritan.com/blog/detail/secure-switches-can-defend-against-cyber-attacks

11. Pearson. (2012, Jan 24). *Basic Switch Security Concepts and Configuration*. Retrieved November 8, 2022 from https://www.pearsonitcertification.com/articles/article.aspx?p=1829347#:~:text=The%20simplest%20form%20of%20switch,Statically
12. CloudFlare. (2022). *What is DNS? | How DNS Works*. Retrieved from https://www.cloudflare.com/learning/dns/what-is-dns/
13. SNIA. (2022). *What Is a Storage Area Network (SAN)?*. Retrieved November 8, 2022 from https://www.snia.org/education/storage_networking_primer/san/what_san
14. CloudFlare. (2022) *What Is DNS Security?*. Retrieved November 8, 2022 from https://www.cloudflare.com/learning/dns/dns-security/
15. Jenna Phipps. (2022, Oct 25). *What Is Storage Area Network Security?*. Retrieved November 8, 2022 from https://www.enterprisestorageforum.com/networking/san-security/
16. Nick Bambulas. (2022, May 10). *10 Proven Ways to Secure a Computer Network*. Retrieved November 8, 2022 from https://www.gflesch.com/elevity-it-blog/ways-to-secure-a-computer-network
17. Logsign Team. (2019, Mar 13). *How to Ensure Network Security?*. Retrieved November 8, 2022 from https://www.logsign.com/blog/how-to-ensure-network-security/
18. Amy Mersch. (2021, Oct 4). *What is Layered Security & How Does it Defend Your Network?*. Retrieved November 8, 2022 from https://blog.totalprosource.com/what-is-layered-security-how-does-it-defend-your-network
19. Fiberplus. (2020, Mar 11). *How Schools and Students Can Benefit From Fiber Optic Technology*. Retrieved November 8, 2022 from https://www.fiberplusinc.com/services-offered/schools-benefit-fiber-optic-technology/

20. Jayasekara, G. P. D. C. M. (2022). *Computer Networks For A School: Case Study Analysis.* Computer Networks For A School: Case Study Analysis (September 13, 2022). Retrieved November 8, 2022 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4217756

21. Kelly, S. & Kumar, K. (2022). *LAN Networking*. In Unity Networking Fundamentals (pp. 239-247). Apress, Berkeley, CA. Retrieved November 8, 2022 from https://link.springer.com/chapter/10.1007/978-1-4842-7358-6_7
22. Raghunandan, K. (2022). *Wireless LAN (Local Area Network).* In Introduction to Wireless Communications and Networks (pp. 223-245). Springer, Cham. Retrieved November 8, 2022 from https://link.springer.com/chapter/10.1007/978-3-030-92188-0_12
23. Leliopoulos, P. & Drigas, A. (2022). *The evolution of wireless mobile networks and the future 5G mobile technology for sustainability*. Technium Sustainability, 2(4), 28-43. Retrieved November 8, 2022 from https://techniumscience.com/index.php/sustainability/article/view/7346