Overview of the problem (diagram). Discuss possible issues that need to be addressed. Also focus on work-from-home aspects.

This assignment entailed the design of a comprehensive network infrastructure for a single-story detached property spanning approximately 100 x 50 metres. The network that has to be designed must cater to the needs of various staff members, each expected to connect between 1 to 4 Wi-Fi devices, that are all considered untrustworthy.

There are 13 offices, accommodating 2 to 4 individual employees each, they must have a total of 4 wired access points each. The network must also make provision for 2 to 4 devices that should be able to connect to the wifi, for each employee in these offices.The technicians' office, serving 2 technicians, necessitates 2 wired access points for them, as well as direct connectivity to the machine room, and Wi-Fi support for up to 8 devices per technician. In the reception area 2 wired access points, designated for 2 personnel, are needed along with full Wi-Fi coverage and access to a networked printer. The kitchen requires 4 wired access points for IoT devices and Wi-Fi connectivity for the staff.

The meeting room has to accommodate 20 to 30 individuals and should be equipped for teleconferencing, 2 wired access points should be provided are essential for the communication devices alongside the Wi-Fi access for the staff. The machine room, which is exclusively accessed by technicians, houses the servers, the routers, and the bigger switches (switches with more than 8 ports) for the entire building; it also serves as a termination point for the ISP fibre line. The network in the open floor space should be able to provide connectivity for 75 to 120 employees; this means that it should also provide 100 wired access points, Wi-Fi access for each staff member. There are also 5 networked printers positioned adjacent to the machine room.

The overall goal of this network to be designed is to ensure a seamless connectivity, optimal bandwidth allocation, and effective device management across the entire property.

The network should also be able to allow certain employees to work from home, and wirelessly connect to the business network environment. For the network to be able to support this functionality, one needs to address a few potential issues, for example the bandwidth allocation, to ensure the network can handle the demands of both the in-house staff, and the remote workers simultaneously without sacrificing performance or security. The Network also needs to provide remote accessibility, which means to provide secure remote access to the network, whether that be through a VPN Solution or Multi-factor authentication.

With this in mind, the network should be designed to facilitate seamless communication, collaboration, and productivity among all the employees across the entire organisation.

Describe the network topology your group designed. Discuss selection of routers, switches, repeaters, etc. and motivate the selection of each. Do not discuss generic design approaches such as star topology – describe your network's topology.

The network topology we designed is a combination of several different topologies, benefiting from the advantages of these different generic topologies. Our Network design contains a central node, which in this case is two multilayer switches, to which all the other device in the network connect to. We decided that only switches should be able to physically connect to the main multilayer switches, as this makes the device management as well as the device and network allocation easier. We added a second switch to our design, that increases redundancy, but reduces the chances of an error, or a failure in the network, influencing the working of and the connectivity of the other devices in the network. Each of these 9 switches connected to the main multi layered switches then connected to the individual devices in each of their designated areas with their own cable. This ensures that even if the network cable for a specific computer/ section breaks or is damaged, the other devices are unaffected, and can still continue to work as normal.

We have selected switches for the central node due to their ability to manage traffic efficiently, prevent data collisions, and provide high-speed connectivity to all connected devices. They offer better performance and scalability compared to hubs, making them ideal for this scenario. Ethernet cables were chosen to connect the devices in the network for their reliability and affordability. They provide a stable physical connection between the devices and the central switch, ensuring consistent data transmission within the network between the connected devices.A routers was selected to be used in the network, to connect this network to other external networks, such as the internet. They handle the routing of data between different networks, providing the network with access to resources beyond the local network.

Discuss how users of the network would connect remotely. Consider the following: ▪ Which remote software should be used, and why (include choices in the budget); ▪ Security implications (e.g. vulnerability to lateral movement); ▪ Bring Your Own Device considerations; and ▪ Establishment of a cooperative virtual workspace.

For the remote employees to be able to connect remotely to the business network environment, certain aspects and issues should be taken into consideration. These issues should include which remote access software to use, the security implications of having all the network's resources available over the internet. It should also be considered how the business's network will accommodate Bring Your Own Device and the policies to protect the business and employees in this situation, and also how the business will create a cooperative virtual workspace between its employees.

When the business selects a software to use for the remote employees to connect to the business network, the options include VPN's (Virtual Private Network)'s, Cisco AnyConnect or even more simpler Remote Desktop Protocols such as Microsoft Remote Desktop, or even collaboration software platforms like Microsoft Teams or Slack. We would recommend a VPN Software to establish a secure connection between the remote users and the corporate network, ensuring data privacy and integrity during the transmission of data, but still allowing the user to have access to all the resources on or connected to the network.

Giving employees remote access to the network and its resources, introduces great security risks, particularly vulnerability to lateral movement in the network, this is when the attacker gains unauthorised access to one device in the network, and then attempts to move laterally through the network. But these risks can be combated through implementing strong authentication methods such as multi-factor authentication (MFA). Another control that can be implemented is network segmentation which only allows employees access to controls that they require for their role in the business.

If the business implements a Bring Your Own Device practice, certain BYOD policies should be established to govern the use of personal devices for remote work. These policies should outline security requirements such as mandatory device encryption, specific antivirus software and regular security updates. Another control that can be implemented is Device registration and enrollment. This process can ensure that only authorised devices are allowed to connect to the corporate network remotely, greatly reducing the risk of security threats.

If the business allows employees to remotely connect to the business network, certain actions can be taken to create a cooperative virtual workspace between the different employees. For example, collaboration platforms such as Microsoft Teams, Slack or even Google Workspace can enable remote users to collaborate effectively

through messaging, video conferencing, file sharing, and project management tools. Even further, the business can establish shared document repositories and project management dashboard within these platforms to promote transparency, accountability and even teamwork among remote users.

Evaluate the designed network: ▪ Does it fulfil the requirements? ▪ What is good about this setup? ▪ What is problematic about this setup? ▪ Which part of the network is likely to need the most maintenance? Can this part of the network be installed in a way that facilitates maintenance? ▪ Which parts, if any, would remain if the company moves to a virtual office environment completely? Why?

This network design is mainly based on a star topology, but not completely and is rather a combination of more than one generic network topology. This design does fulfil all the specified requirements for this business environment situation that is described in the project.

The advantages of this topology:

- This topology is inherently scalable, allowing easy expansion of the network, and the devices connected to it. Expansion of the network can easily be done by just adding more devices to the central switches, without disrupting any existing connections.
- Since each device in the network communicates directly with the central switch, it recovers the overall data collision and latency in the network, ensuring efficient performance.
- This topology isolates an issue, if one should occur, since for example if one device or cable fails, it typically does not affect the rest of the network, as each device is connected independently to the central switch.
- Since two switches are used in parallel with one another, if one switch fails, there's still a backup switch and all the network activities can continue on as normal. This also reduces the chances of the network becoming overloaded.

The Problems with this setup:

- The devices in this setup must be located within the reach of the Ethernet cables or Wi-Fi signals, which could potentially limit mobility and flexibility within the building, in terms of network design.
- Since two multilayer switches are used, it increases the cost of the network hardware by a lot, and can quickly make the business network setup extremely expensive.

Maintenance:

The open floor space, with its 100 wired access points, is the most likely to require the most maintenance due to the sheer number of connections and potential for cable wear or damage. Installing these access points in a modular and accessible manner can facilitate maintenance tasks. To facilitate maintenance in the open floor

space, structured cabling systems should be implemented, allowing for easy identification and replacement of cables if needed. Additionally, the organizing of access points in zones or clusters can simplify troubleshooting and maintenance efforts, reducing downtime and disruptions to users in this network.

The Transition to a Virtual Office Environment:

In a completely virtual office environment, certain parts of the network would remain very essential and needed for the network to function such as:

1. Machine Room/Server Room: The servers and networking equipment housed in the machine room would remain critical for hosting centralised data and services accessed remotely by employees.
2. Remote Access Infrastructure: Components supporting remote access, such as VPN servers or remote desktop services, would still be necessary to facilitate connectivity for remote workers.
3. Security Measures: Network security measures, including firewalls, intrusion detection systems, and access controls, would remain vital to protect the organisation's digital assets, even in a virtual office environment.

While certain components of the network would still be essential in a virtual office scenario, the physical infrastructure requirements may be reduced, this means that there is less emphasis on wired connections and more reliance on remote access technologies.

Creating the subnet for the network:

The subnet 192.168.0.0/22 spans from 192.168.0.0 to 192.168.3.255. Here are the detailed ranges broken down within this subnet:

1. 192.168.0.0/24
    - Network Address: 192.168.0.0
    - First Usable IP: 192.168.0.1
    - Last Usable IP: 192.168.0.254
    - Broadcast Address: 192.168.0.255
2. 192.168.1.0/24
    - Network Address: 192.168.1.0
    - First Usable IP: 192.168.1.1
    - Last Usable IP: 192.168.1.254
    - Broadcast Address: 192.168.1.255

3. 192.168.2.0/24
    - Network Address: 192.168.2.0
    - First Usable IP: 192.168.2.1
    - Last Usable IP: 192.168.2.254
    - Broadcast Address: 192.168.2.255
4. 192.168.3.0/24
    - Network Address: 192.168.3.0
    - First Usable IP: 192.168.3.1
    - Last Usable IP: 192.168.3.254
    - Broadcast Address: 192.168.3.255

Summary of Usable IP Address Ranges

- 192.168.0.1 - 192.168.0.254
- 192.168.1.1 - 192.168.1.254
- 192.168.2.1 - 192.168.2.254
- 192.168.3.1 - 192.168.3.254

These four /24 subnets collectively provide 1024 addresses, with 1008 usable addresses (excluding network and broadcast addresses for each /24 subnet). This meets the requirement of providing enough addresses for 1000 devices.

Packet Tracer Reflection:

We utilized the given specifications to create the network topology.

The different sections were clearly defined, and we allocated the appropriate devices accordingly. To ensure the devices that are going to use this network can connect smmotly, we determined that a central multilayer switch should be used for the smaller switches to connect to. We added a second muitlayer switch for redundancy and robustness, to ensure we minimise potential riks and downtime the network might encounter. We used Vlans to separate the network logically, we then assigned a dhcp pool to each vlan for the wired and wireless devices.
Static IPs were assigned to the devices in the server room such as the multilayer switches, a server, a router, WLC (Wireless Lan Controller) and the pc that manages it.

This design approach allowed us to establish a scalable and easily manageable network infrastructure. We encountered a challenge regarding the one fibre connection to the Internet. As the project specifications did not provide a specific method, we needed to find a suitable solution and we decided that using a web server to represent the internet was the best.

Working with Cisco Packet Tracer provided us with a valuable learning experience. As a team, we were initially unfamiliar with the environment and had to acquire new network building skills. Through hands-on experimentation and research, we gained a deeper understanding of network design principles and device configurations. Overall, the project allowed us to apply theoretical knowledge to practical scenarios, enhancing our understanding of network design and troubleshooting. The challenges we encountered helped us develop problem-solving skills and adaptability, and prepared us for future networking endeavours.

Text Messaging App Reflection:

Reflecting on the messaging application developed by our group, We are truly impressed by the valuable insights and expertise we acquired throughout the entire process. The project not only expanded our proficiency in various C# methods and features but also deepened our understanding of establishing connections between different machines using their respective IP addresses and ports. Overcoming challenges emerged as an integral part of our journey, notably tackling the intricacies of connecting and enabling seamless communication between devices.

Additionally, configuring the Peer-to-Peer server proved to be a significant hurdle, as we discovered the need to address message routing concerns that could potentially cause confusion when engaged in conversations with multiple users. Ultimately, the experience fostered tremendous personal and professional growth, equipping each team member with a wealth of new knowledge and skills to carry forward.

Text Messaging App Reflection (Jacques):

For the text-messaging app I made 2 rough ideas about how we could approach the chat app's way of communicating. Further along the road we made use of a web server called firebase which eased things. The code from my previous 2 ideas were used in the final ChatSphere text-messaging app. **[Write more]**