

# NWEG5112: FINAL POE

JADIN NAICKER

ST10275486 1 December 1, 2023

## Activity 1

### Original Tasks:

#### **POE PT1:**

## Activity 1

### 1.1

#### A) Scenario: Small printing company

The scenario linked to the question revolving around a printing company ran from a small workshop, with a employment of 20 employees. The company depends significantly on interconnected systems to effectively handle its day-to-day operations. Components required for this company will be as followed:

- **Devices**: There are 20 staff members, each equipped with a laptop or desktop computer and company-provided smartphones.
- **Printers**: The company has five printers connected to the network.
- **Central Server**: The server is responsible for managing print jobs, tracking customer orders, and handling financial data.
- **Networked Communication**: Staff frequently share print orders, design files, and customer requirements over the network. All devices within the company connect to a central wireless router, facilitating seamless communication and data transfer between employees and printers.
- **Financial System**: The central server is also used for financial purposes, such as tracking expenses and revenue, generating invoices, and processing payments received through the company's website.
- **Client Interaction**: Clients can submit print orders and payments directly through the company website, and the server manages these transactions and updates financial records.
- **Printing Functions**: The printers are essential for producing various physical print materials, including marketing, brochures, and other documents requested by clients. Additionally, they are used for internal document printing and specialized items required by employees to streamline the printing process.

(Serpanos, 2011)

B) This is considered as a network system as the components below have the following:

- **Network Protocols**: The scenario relies on network protocols for communication between devices, data transfer between employees and printers, and interactions with the central server. (Serpanos, 2011) Protocols like TCP/IP ensure reliable data exchange. (Goss, 2018)
- **Functional Requirements**: The functional requirements include sharing print orders, tracking orders and financial data, processing payments, and managing print jobs. These functions are fulfilled by the networked devices and central server. (Serpanos, 2011)
- **Performance Requirements**: High-speed printers, a server, and network communication are essential to meet performance requirements, ensuring timely processing of print jobs and financial transactions. (Serpanos, 2011)
- **Network Traffic**: Network traffic involves data flow between devices, such as employees sharing files, clients submitting orders, and the server processing processes. (Serpanos, 2011) Network traffic management is critical for efficient operation. (Gillis, 2023)
- **Implementation Constraints**: Constraints may include security measures to protect financial data and client information, as well as ensuring that the network can handle the volume of print jobs efficiently.
- **Embedded Systems**: Embedded systems might be used within the printers and the server to control and manage their functions, ensuring seamless operation and providing support. (Serpanos, 2011)

1.2)

**A) Wireless Router:**

The wireless router must support a minimum of 20 device connections. should provide wireless connectivity to all devices. The router must have the capability to connect to the internet and share the internet connection with all connected devices. (Rouse, 2023) Security measures, including firewall capabilities and encryption, should be implemented to safeguard company functioning. The router

must provide coverage for the entire building to ensure that workers have a signal in all areas.

### **Network Protocols:**

TCP/IP protocol must be supported for internet communication with clients. HTTP protocol should be used to allow clients to access company websites. VoIP should be implemented to enable employees to have meetings and communicate over the network. (Serpanos, 2011)

### **B) Network Traffic:**

The network should accommodate the traffic generated by 20 staff members' devices, printers, and server. Adequate bandwidth and network capacity should be provided to ensure smooth data transfer and communication. Network traffic should be secured to protect against unauthorized access and data breaches. (Serpanos, 2011)

**C) Computers and Laptops:** All computers and laptops should be capable of connecting to the network, either wirelessly or via an Ethernet cable. Devices must be regularly updated to minimise network security risks. Each device should have firewall and antivirus capabilities to enhance network security.

**Printers:** The embedded systems of the printers must be configured to connect directly to the network. Printers should be activated to automatically receive and print jobs from the computers without manual intervention.

**Central Server:** The server should have a reasonably large capacity to handle network functions effectively. (Kickidler, 2023) It must manage print jobs, track customer orders, and handle financial data securely. The server should also support networked communication between employees and printers.

**Financial System:** The server should be used for financial purposes, including tracking expenses, revenue, generating invoices, and processing payments received through the company's website. Security measures must be in place to protect financial data.

**Client Communication:** Clients should be able to submit print orders and payments through the company website. The server should manage these transactions securely and update financial records accordingly.

**Printing Functions:** The printers should be capable of producing various physical print materials, both for clients and internal use. They should efficiently handle print jobs and be integrated with the network for seamless operation.

1.3) In a small printing company, the relationship between its various products and designs plays a crucial role in creating an efficient network. A secure Internet connection is provided and connected by routers that must be compatible with all connections of employees. Network traffic generated by data exchange between devices, printers, and servers requires a strong network with sufficient capacity and security measures. The system installed on devices ensures seamless integration with the network, while the role of servers in managing printing operations, orders, financial data, and customer transactions through networks ensuring efficient printing processes by printers must work well with it. Understanding these relationships is paramount to creating a seamlessly functional network, while ignoring them can lead to network complexity, security vulnerabilities, and performance issues results, which will ultimately affect company performance and customer satisfaction. (Serpanos, 2011)

## Activity 2

New developments in how we connect computers and devices demonstrate that we should create networks in a different way than the current Internet. The current Internet has difficulties such as not being secure, not providing good quality services, and having difficulties when many people and devices use it. We now have a lot of different types of devices and a new way of thinking about networks, we also need to make new rules for how these networks should operate. This essay will talk about the Next Generation Internet Architecture describing Peer-to-peer networking (P2P) and addressing the shortcomings in internet architecture. (Serpanos, 2011)

The internet's architecture can be regarded as a super-network, where numerous unique networks are formed and communicate through a shared set of rules. It is essentially an interconnected network formed by using the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol. This protocol allows the connection of any two networks, regardless of their hardware, software, or design. (TutorialsPoint, 2023)

Peer-to-peer networking (P2P) enable all peers to function as both clients and servers, making them accessible points for other peers to establish connections with. By using control mechanisms, a peer can easily select which other peer to link with when seeking specific information. What's great about P2P communication is that it can easily work with existing technology. You only need to make changes to the computer programs you're using. (Serpanos, 2011)

P2P networks can address the short comings of internet architecture as it makes it easier to share files over long distances and doesn't require server equipment or a full-time supervisor. They can easily add new users, keep working even if the main server breaks,

avoid traffic jams by using numerous computers, get faster as more people join, and help different devices work together efficiently for the entire network's being. (Herrity, 2023)

In conclusion, the Next Generation Internet Architecture, particularly Peer-to-peer networking, provides a solution for the current internet's issues. P2P is adapted, user-friendly, and addresses issues such as security, quality, and scalability. It eliminates the need for complex servers, maintains its functionality despite server failures, manages traffic congestion effectively, and becomes more efficient as more users join. P2P networking can alter our online experience, making it safer, faster, and more interconnected, resulting in a change in how we connect and share information on the Internet. (Serpanos, 2011)

### Activity 3

- **Link Interface**: This subsystem plays an important role in data communication by using the physical layer and the MAC (Media Access Control) sublayer of the data link layer. The physical layer deals with the actual transmission of data over the network medium, including aspects like encoding, signalling, and physical connectors. The MAC sublayer, on the other hand, controls access to shared network media, ensuring that devices can communicate without interference. (Serpanos, 2011) The link interface provides us with a means to transmit raw packets onto the network, just as we initially received them. (Russel, 2002)
- **Processing element (PE)**: The processing element is the core processing subsystem of the adapter. It manages various tasks, such as data management, data migration, and protocol implementation. Data management includes functions such as data buffering, queuing, and flow control to ensure smooth data transfer. Data migration involves routing data within the adapter and to and from external systems, often involving complex routing decisions. Protocol functions include defining and executing network protocols to facilitate communication between the adapter and the network. (Serpanos, 2011)
- **DMA (Direct Memory Access) unit**: It is specially designed for high-speed data transfer between the Link Interface and the memory of the adapter. It operates independently of the Processing Element, allowing efficient and fast data transfer

without CPU intervention. This is especially important in high-performance networks where high-speed data transfer is critical. (Serpanos, 2011)

- **Memory**: Acts as data storage on the adapter. It contains data types, including network packets, control information, and buffers. Memory plays a key role in storing, processing, and queuing short-term data for transmission or retrieval as needed. (Serpanos, 2011)
- **The End System Interface**: It is the gateway between the adapter and the end user or end system. It facilitates data transfer between the network adapter and the device or application that generates or uses the data. This interface typically includes software components and drivers that provide seamless communication between the adapter and the higher-level protocols used by the end system, allowing applications and users to interact with the network communication. (Serpanos, 2011)

## POE PT2:

### [Question 1](#)

- 1.1) As businesses are constantly evolving, a resilient network structure is essential and cannot be emphasized enough. Mr. Khoza's small business in Midrand, Gauteng, wants a secure and cost-effective network to sustain development and respond to unexpected issues such as Covid 19, economic issues and financial issues. The objective of this report is to explain the importance of developing a resilient network structure and to provide insights into how resilience and redundancy can be implemented into Mr. Khoza's network infrastructure.

Resilient networks are essential for ensuring uninterrupted operations, even if disruptions occur. These disruptions can include everyday network security concerns, potential cyberattacks, or hardware failures, as well as natural disasters. Insufficient preparedness can leave a network susceptible to frequent outages. Network resilience is a critical factor in protecting a company's daily operations and overall productivity against potential disruptions. (Zayo, 2023)

The four factors of considering Network resilience are:

- Failures
- Operating hours
- Virtualization, cloud, and SaaS applications

- Reliable remote connectivity

(Cavanaugh, 2020)

**Failures:** The first step in building strong networks is recognising failure. Every component of the network, such as routers, switches, circuits, cables, and other components, is vulnerable to errors. To ensure network resilience, it is important to implement regular maintenance. This requires continuous software and security updates and careful planning for hardware repairs and replacements. For Mr. Khoza's small business, this means establishing a practical maintenance schedule that includes routine inspections, software updates, and hardware replacements. It's essential to monitor the condition of network components to identify potential issues before they lead to network disruptions. By addressing these vulnerabilities, the business can minimise the impact of failures and reduce downtime.

(Cavanaugh, 2020; Serpanos, 2011)

**Operating hours:** Network teams must take into consideration the business environment's operational hours. While some networks may experience reduced user activity outside of regular working hours, others, like data centres, must maintain continuous operation around the clock. When planning for resilience, it's important to factor in both potential failures and the capacity to function during maintenance. In the case of Mr. Khoza's small business, it operates within standard working hours. To ensure uninterrupted operation, it is crucial to schedule maintenance during periods of minimal user activity, such as evenings or weekends. This strategy not only minimises disruptions but also upholds the dependability and accessibility of essential services. Introducing redundancy in critical systems can help moderate the impacts of unexpected failures during operational hours.

(Cavanaugh, 2020; Serpanos, 2011; Motiso, 2022; Froehlich, 2021)

**Virtualization, cloud, and SaaS applications:** Cloud based applications can impact an organisation's choices. The availability offered by different applications and hosting locations should be taken into consideration. Mr. Khoza should examine service level agreements offered by cloud and SaaS providers and consider the impact of interactions with these services on network resilience. Mr. Khoza should consider network redundancy for connecting to cloud-based applications and SaaS providers as multiple internet connections could provide more resilience.



(Cavanaugh, 2020; Serpanos, 2011; Motiso, 2022; Froehlich, 2021)

**Reliable remote connectivity:** In the modern day of remote work, businesses must secure the dependability of their remote connectivity. This includes inquiries into the structure of remote access systems. In this case VPN's and load balancing should be considered. Mr. Khoza's company should use VPN's and load balancing as employees have continuous network connectivity even when one component of the system is under maintenance.

(Cavanaugh, 2020; Serpanos, 2011; Motiso, 2022; Froehlich, 2021)

Using new devices, channels, and other resources in a business's network is known as network redundancy. Since network redundancy helps the business protect different areas of the network to decrease failures, damage, or downtime, some firms refer to it as a disaster recovery plan. By implementing network redundancy, you can ensure that the network functions properly for both consumers and staff. (Motiso, 2022) Mr. Khoza can build redundancy in his network by providing regular maintenance schedules that include routine checks for potential issues, keeping software and security patches up to date, and planning for hardware maintenance and replacement. When scheduling these maintenance activities, particularly for his business with defined operating hours, it's advisable to select off-peak hours, such as evenings or weekends, to minimise disruptions and maintain continuous network operation. Additionally, when working with cloud and SaaS providers, he should carefully evaluate their Service Level Agreements and opt for those with higher SLAs and redundant infrastructure to ensure constant access to critical applications and data. Implementing network redundancy for connecting to cloud and SaaS services further improves reliability. To support remote workers, choose remote access solutions equipped with redundancy and load balancing, ensuring uninterrupted network access, even in the event of maintenance or failures. This comprehensive approach to redundancy ensures the resilience of Mr. Khoza's network infrastructure and reduces the risk of downtime and disruptions.

(Cavanaugh, 2020; Serpanos, 2011; Motiso, 2022; Froehlich, 2021)

In conclusion, establishing a resilient network structure is importance for Mr. Khoza's small business. This protects the network's ability to withstand disturbances and breakdowns, while maintaining the continuation of essential business operations. By considering the

factors mentioned above Mr. Khoza can improve resilience in his network infrastructure. A well-designed resilient network not only protects against unexpected challenges but also supports future growth and success. It is a valuable investment in the longevity and efficiency of the business. (Zayo, 2023)

1.2) In the process of designing Mr. Khoza's network, it is necessary to follow network design principles to assure the security, efficiency, and scalability of the network. We will discuss ten key network design principles, explaining each one and providing examples of their application in Mr. Khoza's network infrastructure.

Network architecture, commonly known as network topology, involves the complex arrangement of infrastructure in an IT network, including physical, virtual, and logical components. This is essential to provide a secure network environment and effectively meet the specific needs and objectives of an organisation. Whether designing hardware, formulating software, defining communication mechanisms, or defining communication mechanisms, communication is an important aspect of modern digital communication. (Cisco, n.d)

Mr. Khoza needs to consider these principles/laws for his network infrastructure/design:

- Don't make assumptions
- Avoid dangling networks
- Route where needed, not where possible
- Apply network visibility
- Ensure standardisation
- Layer 1 is king
- Simplicity is key
- Power is important
- Embrace documentation
- Design for security

(Jabbusch, 2013; Cisco, n.d)

**Don't make assumptions:** Make sure you have a deep understanding of the existing network infrastructure before making any modifications or changes. Accurate knowledge is essential to avoid mistakes rather than making assumptions. (Jabbusch, 2013) Mr. Khoza's network designer should thoroughly assess the current network and gather accurate information about devices, connections, and configurations. They must avoid making assumptions about the existing network. They must verify and double-check any changes made during the network design process to eliminate assumptions. (Jabbusch, 2013)

**Avoid dangling networks:** Maintain a clear and well-constructed network configuration while avoiding unnecessary complications, ensuring proper VLAN and network segment configuration. (Jabbusch, 2013) In Mr. Khoza's network, the designer should avoid any

unnecessary complexity in network infrastructure. Ensure that all VLANs, especially in open-plan offices, are correctly configured to prevent misconfigurations. (Jabbusch, 2013)

**Route where needed, not where possible:** Prioritise routing to meet the specific needs of the network rather than being too complex in terms of routing. (Jabbusch, 2013) The network designer should focus on routing only where it is necessary. For Mr. Khoza, this means optimising routing for specific purposes, such as internet access or traffic between different offices. By Mr. Khoza doing this, his business can avoid unnecessary complications. (Jabbusch, 2013)

**Apply network visibility:** Use advanced network monitoring and management tools to be fully aware of network devices and their status. (Jabbusch, 2013) In Mr. Khoza's network, this will help in maintaining control and security, ensuring that all devices are tracked. Mr. Khoza must continue to use monitoring tools in the new network design to ensure complete visibility and control. (Jabbusch, 2013)

**Ensure standardisation:** Determine when standardisation can improve network efficiency and interoperability, to ensure consistency with organisational goals. (Jabbusch, 2013) In Mr. Khoza's network, the designer should decide on standardising certain aspects, like security settings, for consistency and better management. For Mr. Khoza's network this will improve network management and flexibility. (Jabbusch, 2013)

**Layer 1 is king:** Ensure that the physical layer such as cables and hardware is strong and maintained as it forms the foundation for network stability. (Jabbusch, 2013) In Mr. Khoza's network, the foundation should be checked to avoid disruptions in Layer 1 that could lead to network outages. Mr. Khoza should incorporate any necessary upgrades into the new network design while maintaining the physical layer. (Jabbusch, 2013)

**Simplicity is key:** Apply simplicity in network design, following the K.I.S.S. model, while maintaining the necessary connectivity and security standards. (Jabbusch, 2013) Mr. Khoza's network should prioritise simplicity in configurations, reducing the risk of errors and complications such as in devices and printers. (Jabbusch, 2013)

**Power is important:** Implement power management solutions to ensure consistent and clean power for network devices as the network evolves with new technologies. (Jabbusch,

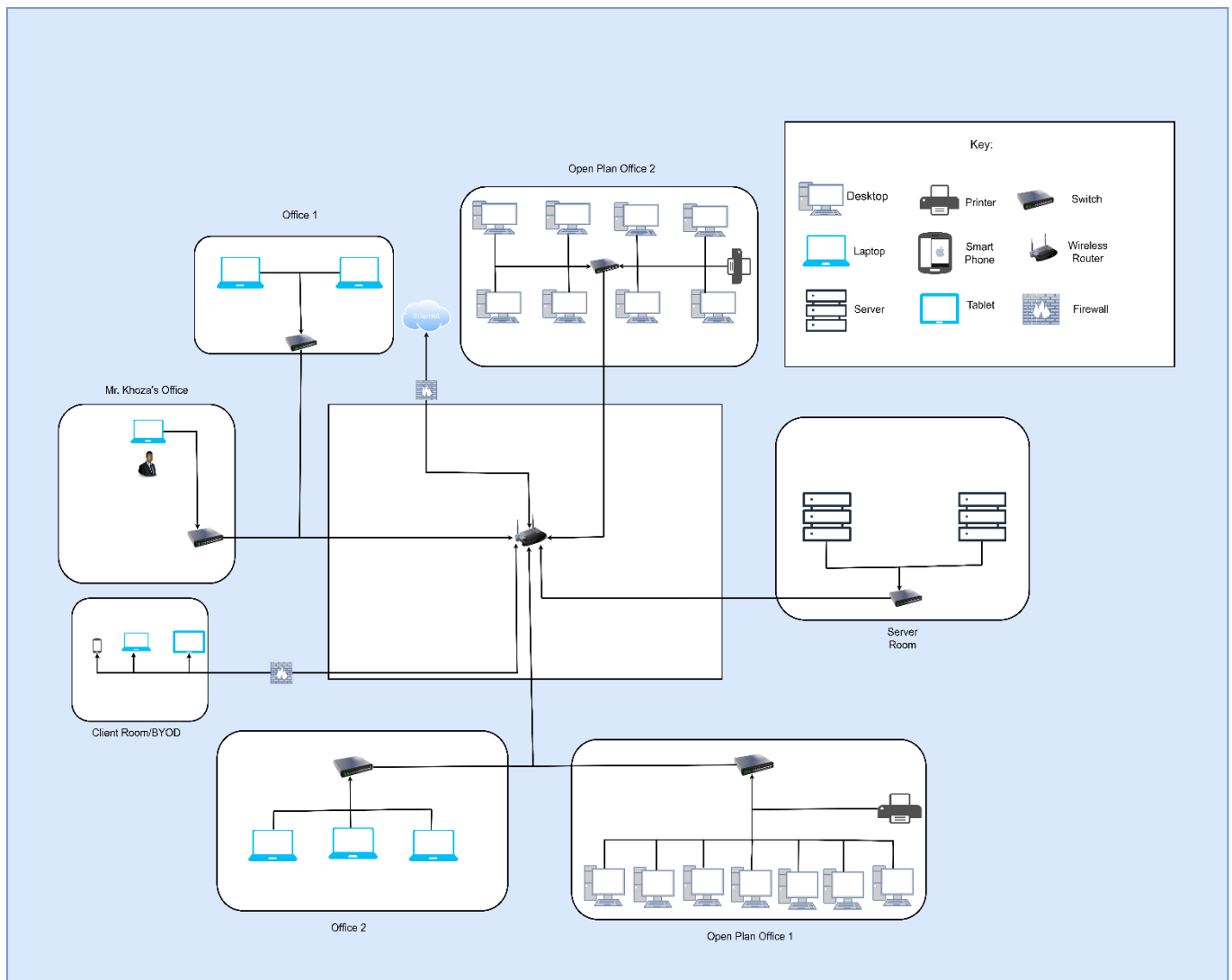
2013) This is important for Mr. Khoza's business/network as additional devices will be added as the network expands. Mr. Khoza should invest in reliable power sources to support the servers and network infrastructure in the storeroom. (Jabbusch, 2013)

**Embrace documentation:** Develop and maintain thorough network documentation to track changes and troubleshoot effectively. (Jabbusch, 2013) In Mr. Khoza's network, documentation will play a vital role in ensuring the network's stability and efficiency. Mr. Khoza should document network configurations in preparation for future problems. (Jabbusch, 2013)

**Design for security:** Network security must be part of the initial design to avoid later issues, like compatibility problems affecting network performance, user experience, and manageability. (Cisco, n.d) Mr. Khoza must identifying any gaps, vulnerabilities, or areas where security measures need improvement. This will help him to minimise risks. Mr. Khoza must ensure that security measures are incorporated into the network's architecture. This includes firewall configurations, access controls, intrusion detection systems, and encryption protocols. (Cisco, n.d)

By following these principles and applying them to Mr. Khoza's network design, a network designer can create a secure, efficient, and cost-effective network that meets the needs of the business at the ready for future development and change.

1.3)



Link to draw.io: [https://drive.google.com/file/d/1nQLyM\\_SoH\\_Uio-yiDqKmBt3PT4aIEtwp/view?usp=sharing](https://drive.google.com/file/d/1nQLyM_SoH_Uio-yiDqKmBt3PT4aIEtwp/view?usp=sharing)

The LAN configuration consists of 3 offices, two open plan offices, a client room, and a server room. Mr. Khoza has his own private office, while two laptop users share one office and the other three have separate offices. The first open office space has seven desktops, with the remaining 8 desktops in the second open office. A small room acts as a server room. The LAN network operates by connecting all devices, such as desktops, laptops, and servers, to a LAN switch, which interconnects them. The servers, located in the server room, manage and store network data. Each office has a wired connection to the LAN switch for communication. Open-plan offices utilise the LAN switch for shared resource access with multiple desktops, while laptop offices connect laptops for resource and data access.

Wireless router is placed enabling wireless connectivity, eliminating the need for wired connections. Laptop users can access the LAN network through their offices wirelessly. The LAN design in place enhances Mr. Khoza's business operations in several ways. It allows for effective communication and data exchange among LAN devices, allows access to shared resources and data from individual offices, offers wireless flexibility and mobility across the premises, centralises data storage and management in the server room, and increases productivity and collaboration by promoting communication and resource sharing among employees. (Serpanos, 2011; Partsenidis, n.d)

IP Address Plan for Mr. Khoza:

**Mr. Khoza's Office:**

Subnet: 10.8.0.0/24

Usable IP Range: 10.8.0.1 - 10.8.0.254

Devices: Laptop and server

**Open Plan Office 1:**

Subnet: 10.8.1.0/24

Usable IP Range: 10.8.1.1 - 10.8.1.254

Devices: PCs, Printer, and server

**Open Plan Office 2:**

Subnet: 10.8.2.0/24

Usable IP Range: 10.8.2.1 - 10.8.2.254

Devices: PCs, Printer, and server

**Office 1:**

Subnet: 10.8.3.0/24

Usable IP Range: 10.8.3.1 - 10.8.3.254

Devices: Laptops and server

**Office 2:**

Subnet: 10.8.4.0/24

Usable IP Range: 10.8.4.1 - 10.8.4.254

Devices: Laptops and server

**Server Room:**

Subnet: 10.8.5.0/29

Usable IP Range: 10.8.5.1 - 10.8.5.6

Devices: Server

**Client Network:**

Subnet: 10.8.6.0/24

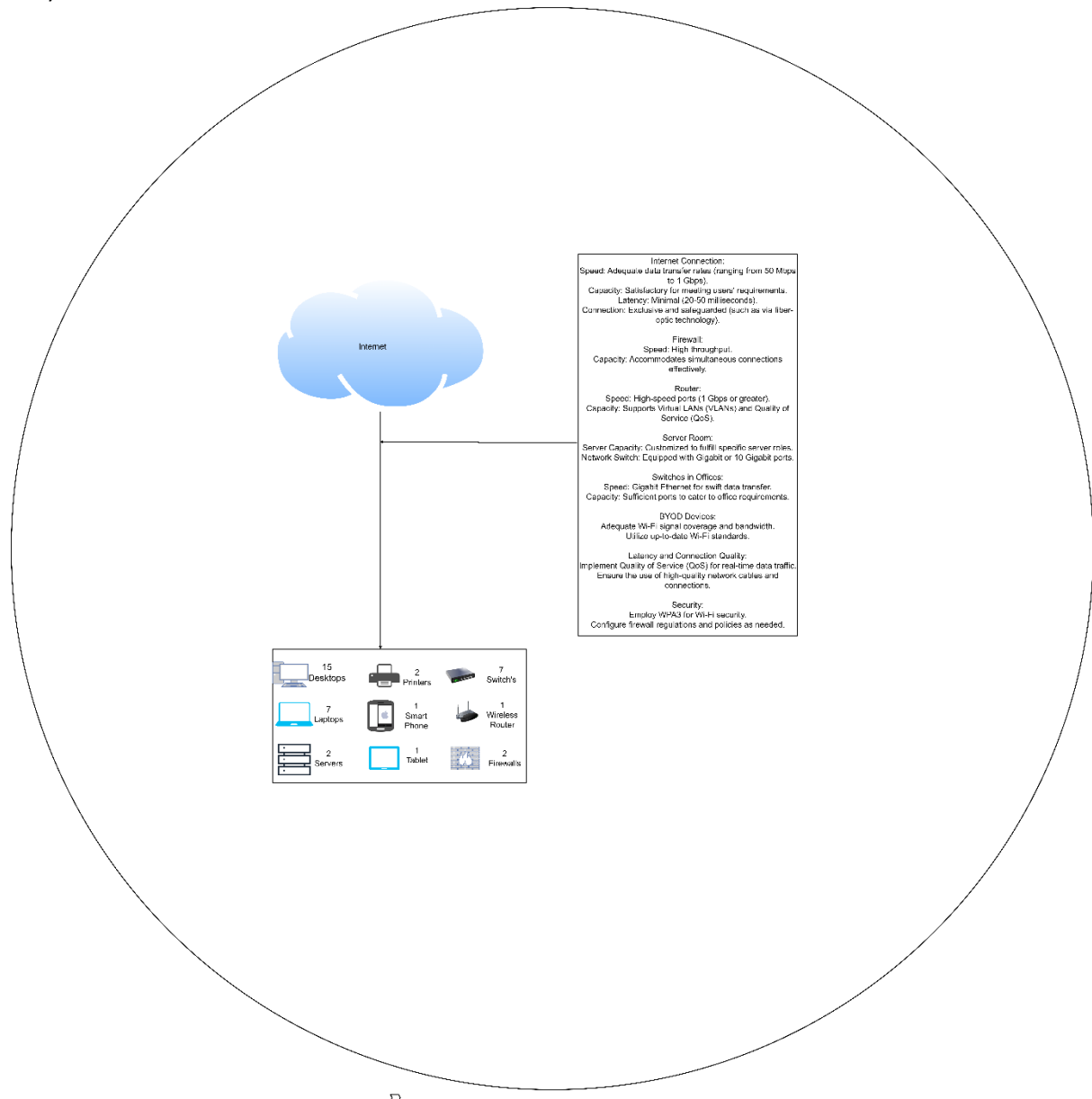
Usable IP Range: 10.8.6.1 - 10.8.6.254

Devices: Smartphone, Tablet, Laptop and Server

(Serpanos, 2011; Cisco, 2010)



1.4)



Due to clarity issues on the diagrams, please use the link below to see the text clearly if so:






<https://drive.google.com/file/d/13V30jAddVbG26rQCQMIOTfyfigizUupd/view?usp=sharing>

The WAN diagram's internet connection delivers sufficient bandwidth, ranging from 50 Mbps to 1 Gbps, to meet Mr. Khoza's business needs as it expands. This ensures data transfer speeds are in line with his requirements. The network is designed to accommodate up to thirty devices, including PCs, laptops, servers, and BYOD devices, with low latency for responsive communication and data transfer. The connection is secure, using technologies like fiber optics for enhanced data privacy and reliability. The firewall in the network design

manages data traffic efficiently, supporting multiple concurrent connections to enhance network security. The high-speed router offers advanced features like VLAN support and Quality of Service to optimise network performance for different applications and services. The server room is made to meet specific requirements like storage needs. Network switches in various offices feature Gigabit Ethernet or 10 Gigabit ports, ensuring fast and reliable connections for desktops and laptops. BYOD devices have sufficient Wi-Fi coverage and bandwidth, with modern standards ensuring efficient and secure connectivity. Quality of Service is implemented for traffic, and quality network cables and connections further improve latency and connection quality. Security measures are strong, ensuring high wireless network security, and firewall rules and policies configured to protect against potential threats, providing extra protection for Mr. Khoza's small business. (Metzler, 2015)

### Feedback screenshot:

### POE PT1:

	Novice	Competent	Proficient
<b>1.1 Scenario</b>	 <b>6</b> (15.00%) ----- 6 (15.00%) - 6 (15.00%)	3 (7.50%) - 5 (12.50%)	0 (0.00%) - 2 (5.00%)
<b>1.2 Requirements</b>	 <b>6</b> (15.00%) ----- 6 (15.00%) - 6 (15.00%)	3 (7.50%) - 5 (12.50%)	0 (0.00%) - 2 (5.00%)
<b>1.3 Relationships</b>	8 (20.00%) - 8 (20.00%)	 <b>5</b> (12.50%) ----- 4 (10.00%) - 7 (17.50%) <b>Feedback:</b> focus on links between concepts	0 (0.00%) - 3 (7.50%)
<b>Next Gen Essay - Intro, Architecture, Next Gen, Shortcomings</b>	10 (25.00%) - 10 (25.00%)	 <b>6</b> (15.00%) ----- 5 (12.50%) - 9 (22.50%) <b>Feedback:</b> P2P is not really next gen, focus on specific shortcomings	0 (0.00%) - 4 (10.00%)
<b>Network Adapter Components</b>	10 (25.00%) - 10 (25.00%)	 <b>7</b> (17.50%) ----- 5 (12.50%) - 9 (22.50%) <b>Feedback:</b> examples needed	0 (0.00%) - 4 (10.00%)

POE PT2:

Name: NWE1B Task 2

Exit

Grid View   List View

	Novice	Competent	Proficient
4 Factors of Design	0 (0.00%) - 3 (5.00%)	<div><div><div>✔✔ 7 (11.66666%)</div><div>4 (6.66666%) - 7 (11.66666%)</div><div>Feedback: Link each concept to practical applications for the network</div></div></div>	8 (13.33333%) - 10 (16.66666%)
10 Principles	0 (0.00%) - 3 (5.00%)	<div><div><div>✔✔ 7 (11.66666%)</div><div>4 (6.66666%) - 7 (11.66666%)</div><div>Feedback: Link each concept to practical applications for the network</div></div></div>	8 (13.33333%) - 10 (16.66666%)
LAN Diagram	0 (0.00%) - 7 (11.66666%)	8 (13.33333%) - 15 (25.00%)	<div><div><div>✔✔ 20 (33.33333%)</div><div>16 (26.66666%) - 20 (33.33333%)</div></div></div>
WAN Diagram	0 (0.00%) - 7 (11.66666%)	8 (13.33333%) - 15 (25.00%)	<div><div><div>✔✔ 20 (33.33333%)</div><div>16 (26.66666%) - 20 (33.33333%)</div></div></div>

## **Updated Tasks:**

### **POE PT 1:**

#### **Activity 1**

##### **1.1**

##### **A) Scenario: Small printing company**

The scenario linked to the question revolving around a printing company ran from a small workshop, with a employment of 20 employees. The company depends significantly on interconnected systems to effectively handle its day-to-day operations. Components required for this company will be as followed:

- **Devices**: There are 20 staff members, each equipped with a laptop or desktop computer and company-provided smartphones.
- **Printers**: The company has five printers connected to the network.
- **Central Server**: The server is responsible for managing print jobs, tracking customer orders, and handling financial data.
- **Networked Communication**: Staff frequently share print orders, design files, and customer requirements over the network. All devices within the company connect to a central wireless router, facilitating seamless communication and data transfer between employees and printers.
- **Financial System**: The central server is also used for financial purposes, such as tracking expenses and revenue, generating invoices, and processing payments received through the company's website.
- **Client Interaction**: Clients can submit print orders and payments directly through the company website, and the server manages these transactions and updates financial records.
- **Printing Functions**: The printers are essential for producing various physical print materials, including marketing, brochures, and other documents requested by clients. Additionally, they are used for internal document printing and specialized items required by employees to streamline the printing process.

(Serpanos, 2011)

B) This is considered as a network system as the components below have the following:

- **Network Protocols**: The scenario relies on network protocols for communication between devices, data transfer between employees and printers, and interactions with the central server. (Serpanos, 2011) Protocols like TCP/IP ensure reliable data exchange. (Goss, 2018)
- **Functional Requirements**: The functional requirements include sharing print orders, tracking orders and financial data, processing payments, and managing print jobs. These functions are fulfilled by the networked devices and central server. (Serpanos, 2011)
- **Performance Requirements**: High-speed printers, a server, and network communication are essential to meet performance requirements, ensuring timely processing of print jobs and financial transactions. (Serpanos, 2011)
- **Network Traffic**: Network traffic involves data flow between devices, such as employees sharing files, clients submitting orders, and the server processing processes. (Serpanos, 2011) Network traffic management is critical for efficient operation. (Gillis, 2023)
- **Implementation Constraints**: Constraints may include security measures to protect financial data and client information, as well as ensuring that the network can handle the volume of print jobs efficiently.
- **Embedded Systems**: Embedded systems might be used within the printers and the server to control and manage their functions, ensuring seamless operation and providing support. (Serpanos, 2011)

1.2)

#### **D) Wireless Router:**

The wireless router must support a minimum of 20 device connections. should provide wireless connectivity to all devices. The router must have the capability to connect to the internet and share the internet connection with all connected devices. (Rouse, 2023) Security measures, including firewall capabilities and encryption, should be implemented to safeguard company functioning. The router must provide coverage for the entire building to ensure that workers have a signal in all areas.

### **Network Protocols:**

TCP/IP protocol must be supported for internet communication with clients. HTTP protocol should be used to allow clients to access company websites. VoIP should be implemented to enable employees to have meetings and communicate over the network. (Serpanos, 2011)

### **E) Network Traffic:**

The network should accommodate the traffic generated by 20 staff members' devices, printers, and server. Adequate bandwidth and network capacity should be provided to ensure smooth data transfer and communication. Network traffic should be secured to protect against unauthorized access and data breaches. (Serpanos, 2011)

**F) Computers and Laptops:** All computers and laptops should be capable of connecting to the network, either wirelessly or via an Ethernet cable. Devices must be regularly updated to minimise network security risks. Each device should have firewall and antivirus capabilities to enhance network security.

**Printers:** The embedded systems of the printers must be configured to connect directly to the network. Printers should be activated to automatically receive and print jobs from the computers without manual intervention.

**Central Server:** The server should have a reasonably large capacity to handle network functions effectively. (Kickidler, 2023) It must manage print jobs, track customer orders, and handle financial data securely. The server should also support networked communication between employees and printers.

**Financial System:** The server should be used for financial purposes, including tracking expenses, revenue, generating invoices, and processing payments received through the company's website. Security measures must be in place to protect financial data.

**Client Communication:** Clients should be able to submit print orders and payments through the company website. The server should manage these transactions securely and update financial records accordingly.

**Printing Functions:** The printers should be capable of producing various physical print materials, both for clients and internal use. They should efficiently handle print jobs and be integrated with the network for seamless operation.

Changes have been made here: 1.3) The relationship between network protocols and fundamental requirements is important. Protocols like TCP/IP and HTTP, as detailed in 1.2, form the framework through which devices communicate, data is exchanged, and clients access the company's services. Understanding this relationship ensures that the necessary functions, like order tracking, financial transactions, and print job management, are efficiently carried out within the network. Network traffic and performance requirements are intrinsically linked. The design must account for the exchange of data between 20 staff members, printers, and the central server. Adequate bandwidth and security measures, emphasised in 1.2, are crucial to prevent congestion and maintain optimal performance. Recognising this linkage guarantees smooth operations and timely execution of tasks within the network. Embedded systems' relationship with implementation constraints is crucial. These systems within printers and servers control vital functions like print job handling and financial data security. Understanding this link ensures proper configuration, enabling automation and seamless integration within the network while meeting security and operational requirement. Comprehending these relationships in network system design is vital. Neglecting the relationship between protocols and fundamental requirements may lead to communication breakdowns or limited access to critical services. Ignoring the traffic performance relationship could result in network congestion and slow performance. Overlooking the embedded systems link with implementation constraints may compromise automation and security measures. Understanding these interdependencies ensures a consistent network design that aligns with the company's operational needs, security measures, and scalability. It prevents potential bottlenecks, security vulnerabilities, and operational inefficiencies, thereby fostering a robust network infrastructure that supports the company's growth and enhances customer satisfaction. (Serpanos, 2011)

## **Introduction**

New developments in how we connect computers and devices demonstrate that we should create networks in a different way than the current Internet. The current Internet has difficulties such as not being secure, not providing good quality services, and having difficulties when many people and devices use it. We now have a lot of different types of devices and a new way of thinking about networks, we also need to make new rules for how these networks should operate. This essay will talk about the Next Generation Internet Architecture describing the Domain Name System (DNS) and addressing the shortcomings in internet architecture. (Serpanos, 2011)

## **What is Internet architecture?**

The internet's architecture can be regarded as a super-network, where numerous unique networks are formed and communicate through a shared set of rules. It is essentially an interconnected network formed by using the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol. This protocol allows the connection of any two networks, regardless of their hardware, software, or design. (TutorialsPoint, 2023)

## **Describing DNS**

The Domain Name System emerges as a crucial component for evolution and adaptation. Within this planned framework, DNS is expected to undergo enhancements focusing on security through features like DNS Security Extensions (DNSSEC) to combat vulnerabilities and potential threats, alongside integrating strong encryption and authentication mechanisms. Scalability and performance optimisation efforts will concentrate on accommodating the expanding internet landscape, possibly incorporating more efficient caching systems, and streamlined query resolutions to support heightened speed and agility. Decentralisation could feature prominently, potentially exploring distributed models or blockchain technology to distribute DNS information, strengthening fault tolerance and reducing reliance on central entities. DNS in this context would adapt to seamlessly integrate with emerging technologies such as IoT, 5G networks, and edge computing. DNS evolution within the next-generation architecture aims to ensure heightened security, improved scalability, adaptability to emerging tech, and accessibility. (Serpanos, 2011)

## **Shortcomings**

Yes, DNS improvements significantly improve security, scalability, and efficiency within Next-Generation Data Centres. Yet, DNS advancements primarily address issues related to cybersecurity threats, offering enhanced threat intelligence and automation. However, these enhancements alone do not widely resolve overarching internet architecture challenges like inherent vulnerabilities in routing protocols, limitations in IPv4 address space, or the lack of built-in security measures in core protocols. The broader internet architecture requires important revisions beyond DNS improvements to undertake weaknesses in routing security,



IP address exhaustion, and protocol-level vulnerabilities. (Serpanos, 2011; Giebelmann, 2019)

## **Conclusion**

The evolution of Internet architecture, including DNS enhancements, aims to tackle security and scalability issues. However, DNS improvements alone cannot fully solve broader concerns like routing vulnerabilities and IPv4 limitations. A thorough approach, integrating emerging tech and strong security measures, is crucial for a more adaptable Internet. (Serpanos, 2011)

### Changes made to: Activity 3

- **Link Interface**: This subsystem plays an important role in data communication by using the physical layer and the MAC (Media Access Control) sublayer of the data link layer. The physical layer deals with the actual transmission of data over the network medium, including aspects like encoding, signalling, and physical connectors. The MAC sublayer, on the other hand, controls access to shared network media, ensuring that devices can communicate without interference. (Serpanos, 2011) The link interface provides us with a means to transmit raw packets onto the network, just as we initially received them. For example, you could use an ethernet cable (Russel, 2002)
- **Processing element (PE)**: The processing element is the core processing subsystem of the adapter. It manages various tasks, such as data management, data migration, and protocol implementation. Data management includes functions such as data buffering, queuing, and flow control to ensure smooth data transfer. Data migration involves routing data within the adapter and to and from external systems, often involving complex routing decisions. Protocol functions include defining and executing network protocols to facilitate communication between the adapter and the network. A Network Interface Controller(NIC) serves as the core processing subsystem, handling data management, migration, and protocol implementation. It manages data, performs routing decisions, and executes network protocols, supporting smooth data transfer. (Serpanos, 2011)
- **DMA (Direct Memory Access) unit**: It is specially designed for high-speed data transfer between the Link Interface and the memory of the adapter. It operates independently of the Processing Element, allowing efficient and fast data transfer without CPU intervention. This is especially important in high-performance networks where high-speed data transfer is critical. An example of this could be a graphics card. (Serpanos, 2011)
- **Memory**: Acts as data storage on the adapter. It contains data types, including network packets, control information, and buffers. Memory plays a key role in storing, processing, and queuing short-term data for transmission or retrieval as needed. (Serpanos, 2011)

- **The End System Interface**: It is the gateway between the adapter and the end user or end system. It facilitates data transfer between the network adapter and the device or application that generates or uses the data. This interface typically includes software components and drivers that provide seamless communication between the adapter and the higher-level protocols used by the end system, allowing applications and users to interact with the network communication. An example of this could be a wireless network adaptor. (Serpanos, 2011)

## Bibliography

Giebelmann, T. (2019). *Next generation networks*. [online] ITWeb. Available at: <https://www.itweb.co.za/content/nWJad7b8DyEqbjO1> [Accessed 30 Nov. 2023].

Gillis, A. S., 2023. *TechTarget*. [Online]

Available at: <https://www.techtarget.com/searchnetworking/definition/network-traffic> [Accessed 9 September 2023].

Goss, M., 2018. [Online]

Available at: <https://www.techtarget.com/searchnetworking/feature/12-common-network-protocols-and-their-functions-explained>

[Accessed 8 September 2023].

Herrity, J., 2023. *Indeed*. [Online]

Available at: [https://www.indeed.com/career-advice/career-development/what-is-a-peer-to-](https://www.indeed.com/career-advice/career-development/what-is-a-peer-to-peer-)  
[peer-](https://www.indeed.com/career-advice/career-development/what-is-a-peer-to-peer-)

[network#:~:text=A%20peer%2Dto%2Dpeer%20network%20is%20an%20information%20tec](https://www.indeed.com/career-advice/career-development/what-is-a-peer-to-peer-)  
[hnology%20](https://www.indeed.com/career-advice/career-development/what-is-a-peer-to-peer-)

[Accessed 10 September 2023].

Kickidler, 2023. *Kickidler*. [Online]

Available at: [https://www.kickidler.com/for-it/docs/the-central-](https://www.kickidler.com/for-it/docs/the-central-server/#:~:text=The%20Central%20Server%20is%20one,violation%20filters.)  
[server/#:~:text=The%20Central%20Server%20is%20one,violation%20filters.](https://www.kickidler.com/for-it/docs/the-central-server/#:~:text=The%20Central%20Server%20is%20one,violation%20filters.)

[Accessed 10 September 2023].

Rouse, M., 2023. *Techopedia*. [Online]

Available at: [https://www.techopedia.com/definition/10065/wireless-](https://www.techopedia.com/definition/10065/wireless-router#:~:text=What%20Does%20Wireless%20Router%20Mean,and%20to%20external%20n)  
[router#:~:text=What%20Does%20Wireless%20Router%20Mean,and%20to%20external%20n](https://www.techopedia.com/definition/10065/wireless-router#:~:text=What%20Does%20Wireless%20Router%20Mean,and%20to%20external%20n)  
[etwork%20environments.](https://www.techopedia.com/definition/10065/wireless-router#:~:text=What%20Does%20Wireless%20Router%20Mean,and%20to%20external%20n)

[Accessed 10 September 2023].

Russel, R., 2002. Attacks on Trusted Identity. In: *Hack Proofing Your Network*. s.l.:Dreamtech Press, p. 789.

Serpanos, D., 2011. *Architecture of Network System*. Burlington: Elsevier.

TutorialsPoint, 2023. *TutotalsPoint*. [Online]

Available at:

[https://www.tutorialspoint.com/computer\\_concepts/computer\\_concepts\\_internet.htm#:~:text=Internet%20architecture%20is%20a%20meta,Protocol%20used%20is%20TCP%2FIP](https://www.tutorialspoint.com/computer_concepts/computer_concepts_internet.htm#:~:text=Internet%20architecture%20is%20a%20meta,Protocol%20used%20is%20TCP%2FIP)

[Accessed 10 September 2023].

## POE PT2:

### Changes made to: Question 1

**1.1)** As businesses are constantly evolving, a resilient network structure is essential and cannot be emphasized enough. Mr. Khoza's small business in Midrand, Gauteng, wants a secure and cost-effective network to sustain development and respond to unexpected issues such as Covid 19, economic issues and financial issues. The objective of this report is to explain the importance of developing a resilient network structure and to provide insights into how resilience and redundancy can be implemented into Mr. Khoza's network infrastructure.

Resilient networks are essential for ensuring uninterrupted operations, even if disruptions occur. These disruptions can include everyday network security concerns, potential cyberattacks, or hardware failures, as well as natural disasters. Insufficient preparedness can leave a network susceptible to frequent outages. Network resilience is a critical factor in protecting a company's daily operations and overall productivity against potential disruptions. (Zayo, 2023)

The four factors of considering Network resilience are:

- Failures
- Operating hours
- Virtualization, cloud, and SaaS applications
- Reliable remote connectivity

(Cavanaugh, 2020)

**Failures:** The first step in building strong networks is recognising failure. Every component of the network, such as routers, switches, circuits, cables, and other components, is vulnerable to errors. To ensure network resilience, it is important to implement regular maintenance. This requires continuous software and security updates and careful planning for hardware repairs and replacements. For Mr. Khoza's small business, this means establishing a practical maintenance schedule that includes routine inspections, software updates, and hardware replacements. It's essential to monitor the condition of network components to identify potential issues before they lead to network disruptions. By addressing these vulnerabilities, the business can minimise the impact of failures and reduce downtime. (Cavanaugh, 2020; Serpanos, 2011)

**Operating Hours:** Network teams must take into consideration the business environment's operational hours. While some networks may experience reduced user activity outside of

regular working hours, others, like data centres, must maintain continuous operation around the clock. When planning for resilience, it's important to factor in both potential failures and the capacity to function during maintenance. In the case of Mr. Khoza's small business, it operates within standard working hours. To ensure uninterrupted operation, it is crucial to schedule maintenance during periods of minimal user activity, such as evenings or weekends. This strategy not only minimises disruptions but also upholds the dependability and accessibility of essential services. Introducing redundancy in critical systems can help moderate the impacts of unexpected failures during operational hours. (Cavanaugh, 2020; Serpanos, 2011; Motiso, 2022; Froehlich, 2021)

**Virtualization, Cloud, and SaaS Applications:** Cloud-based applications can impact an organisation's choices. The availability offered by different applications and hosting locations should be taken into consideration. Mr. Khoza should examine service level agreements offered by cloud and SaaS providers and consider the impact of interactions with these services on network resilience. Mr. Khoza should consider network redundancy for connecting to cloud-based applications and SaaS providers as multiple internet connections could provide more resilience. (Cavanaugh, 2020; Serpanos, 2011; Motiso, 2022; Froehlich, 2021)

**Reliable Remote Connectivity:** In the modern-day of remote work, businesses must secure the dependability of their remote connectivity. This includes inquiries into the structure of remote access systems. In this case, VPNs and load balancing should be considered. Mr. Khoza's company should use VPNs and load balancing as employees have continuous network connectivity even when one component of the system is under maintenance. (Cavanaugh, 2020; Serpanos, 2011; Motiso, 2022; Froehlich, 2021)

Using new devices, channels, and other resources in a business's network is known as network redundancy. Since network redundancy helps the business protect different areas of the network to decrease failures, damage, or downtime, some firms refer to it as a disaster recovery plan. By implementing network redundancy, you can ensure that the network functions properly for both consumers and staff. (Motiso, 2022) Mr. Khoza can build redundancy in his network by providing regular maintenance schedules that include routine checks for potential issues, keeping software and security patches up to date, and planning for hardware maintenance and replacement. When scheduling these maintenance activities,

particularly for his business with defined operating hours, it's advisable to select off-peak hours, such as evenings or weekends, to minimise disruptions and maintain continuous network operation. Additionally, when working with cloud and SaaS providers, he should carefully evaluate their Service Level Agreements and opt for those with higher SLAs and redundant infrastructure to ensure constant access to critical applications and data.

Implementing network redundancy for connecting to cloud and SaaS services further improves reliability. To support remote workers, choose remote access solutions equipped with redundancy and load balancing, ensuring uninterrupted network access, even in the event of maintenance or failures. This comprehensive approach to redundancy ensures the resilience of Mr. Khoza's network infrastructure and reduces the risk of downtime and disruptions. (Serpanos, 2011)

In conclusion, establishing a resilient network structure is importance for Mr. Khoza's small business. This protects the network's ability to withstand disturbances and breakdowns, while maintaining the continuation of essential business operations. By considering the factors mentioned above Mr. Khoza can improve resilience in his network infracstucture. A well-designed resilient network not only protects against unexpected challenges but also supports future growth and success. It is a valuable investment in the longevity and efficiency of the business. (Zayo, 2023)



**1.2)** In the process of designing Mr. Khoza's network, it is necessary to follow network design principles to assure the security, efficiency, and scalability of the network. We will discuss ten key network design principles, explaining each one and providing examples of their application in Mr. Khoza's network infrastructure.

Network architecture, commonly known as network topology, involves the complex arrangement of infrastructure in an IT network, including physical, virtual, and logical components. This is essential to provide a secure network environment and effectively meet the specific needs and objectives of an organisation. Whether designing hardware, formulating software, defining communication mechanisms, or defining communication mechanisms, communication is an important aspect of modern digital communication.

(Cisco, n.d)

Mr. Khoza needs to consider these principles/laws for his network infrastructure/design:

- Don't make assumptions
- Avoid dangling networks
- Route where needed, not where possible
- Apply network visibility
- Ensure standardisation
- Layer 1 is king
- Simplicity is key
- Power is important
- Embrace documentation
- Design for security

(Jabbusch, 2013; Cisco, n.d)

**Don't make assumptions:** Make sure you have a deep understanding of the existing network infrastructure before making any modifications or changes. Accurate knowledge is essential to avoid mistakes rather than making assumptions. (Jabbusch, 2013) Mr. Khoza's network designer should thoroughly assess the current network and gather accurate information about devices, connections, and configurations. They must avoid making assumptions about the existing network. They must verify and double-check any changes made during the network design process to eliminate assumptions. (Jabbusch, 2013)

**Avoid dangling networks:** Maintain a clear and well-constructed network configuration while avoiding unnecessary complications, ensuring proper VLAN and network segment configuration. (Jabbusch, 2013) In Mr. Khoza's network, the designer should avoid any

unnecessary complexity in network infrastructure. Ensure that all VLANs, especially in open-plan offices, are correctly configured to prevent misconfigurations. (Jabbusch, 2013)

**Route where needed, not where possible:** Prioritise routing to meet the specific needs of the network rather than being too complex in terms of routing. (Jabbusch, 2013) The network designer should focus on routing only where it is necessary. For Mr. Khoza, this means optimising routing for specific purposes, such as internet access or traffic between different offices. By Mr. Khoza doing this, his business can avoid unnecessary complications. (Jabbusch, 2013)

**Apply network visibility:** Use advanced network monitoring and management tools to be fully aware of network devices and their status. (Jabbusch, 2013) In Mr. Khoza's network, this will help in maintaining control and security, ensuring that all devices are tracked. Mr. Khoza must continue to use monitoring tools in the new network design to ensure complete visibility and control. (Jabbusch, 2013)

**Ensure standardisation:** Determine when standardisation can improve network efficiency and interoperability, to ensure consistency with organisational goals. (Jabbusch, 2013) In Mr. Khoza's network, the designer should decide on standardising certain aspects, like security settings, for consistency and better management. For Mr. Khoza's network this will improve network management and flexibility. (Jabbusch, 2013)

**Layer 1 is king:** Ensure that the physical layer such as cables and hardware is strong and maintained as it forms the foundation for network stability. (Jabbusch, 2013) In Mr. Khoza's network, the foundation should be checked to avoid disruptions in Layer 1 that could lead to network outages. Mr. Khoza should incorporate any necessary upgrades into the new network design while maintaining the physical layer. (Jabbusch, 2013)

**Simplicity is key:** Apply simplicity in network design, following the K.I.S.S. model, while maintaining the necessary connectivity and security standards. (Jabbusch, 2013) Mr. Khoza's network should prioritise simplicity in configurations, reducing the risk of errors and complications such as in devices and printers. (Jabbusch, 2013)

**Power is important:** Implement power management solutions to ensure consistent and clean power for network devices as the network evolves with new technologies. (Jabbusch,

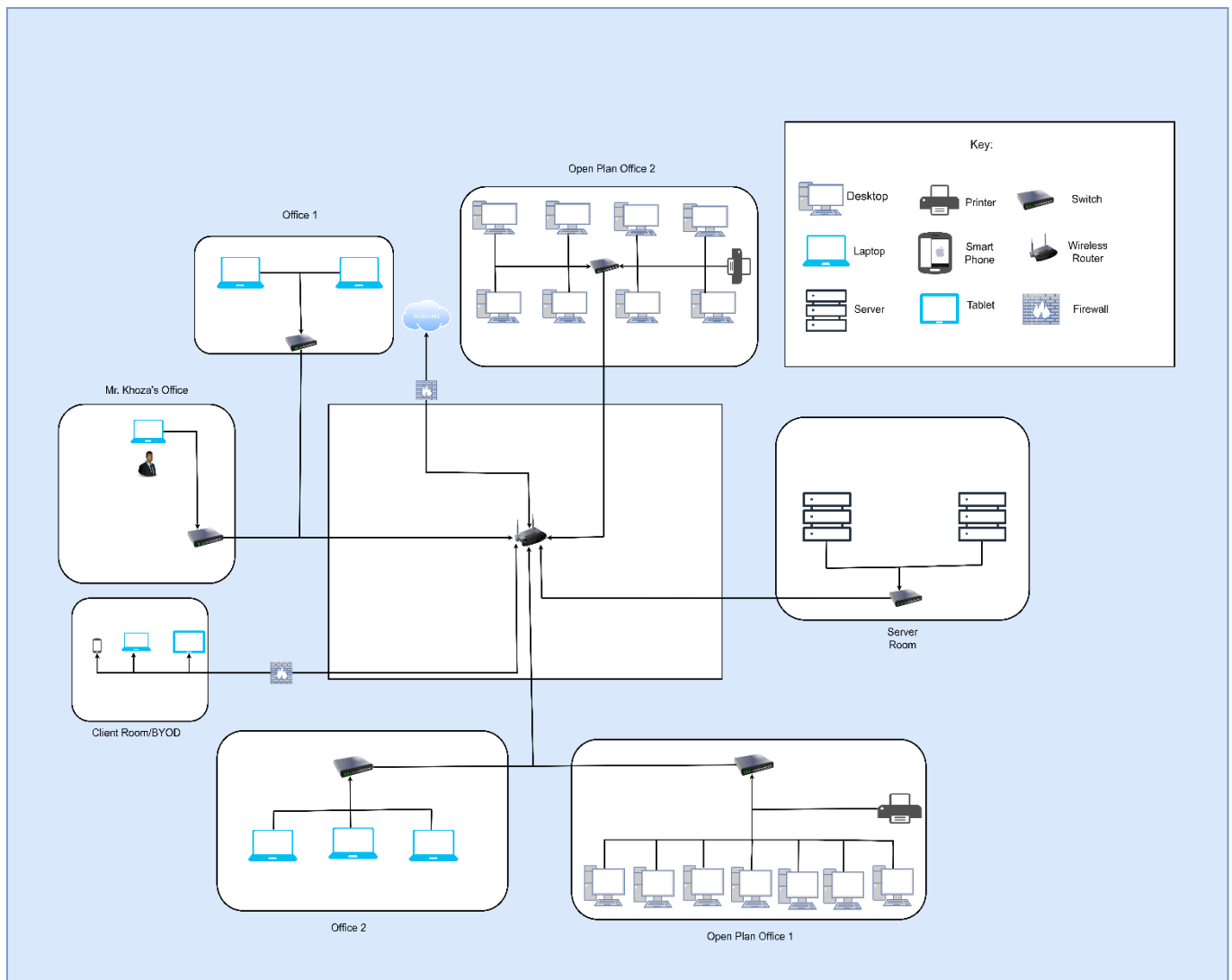
2013) This is important for Mr. Khoza's business/network as additional devices will be added as the network expands. Mr. Khoza should invest in reliable power sources to support the servers and network infrastructure in the storeroom. (Jabbusch, 2013)

**Embrace documentation:** Develop and maintain thorough network documentation to track changes and troubleshoot effectively. (Jabbusch, 2013) In Mr. Khoza's network, documentation will play a vital role in ensuring the network's stability and efficiency. Mr. Khoza should document network configurations in preparation for future problems. (Jabbusch, 2013)

**Design for security:** Network security must be part of the initial design to avoid later issues, like compatibility problems affecting network performance, user experience, and manageability. (Cisco, n.d) Mr. Khoza must identifying any gaps, vulnerabilities, or areas where security measures need improvement. This will help him to minimise risks. Mr. Khoza must ensure that security measures are incorporated into the network's architecture. This includes firewall configurations, access controls, intrusion detection systems, and encryption protocols. (Cisco, n.d)

By following these principles and applying them to Mr. Khoza's network design, a network designer can create a secure, efficient, and cost-effective network that meets the needs of the business at the ready for future development and change.

1.3)



Link to draw.io: [https://drive.google.com/file/d/1nQLyM\\_SoH\\_Uio-yiDqKmBt3PT4aIEtwp/view?usp=sharing](https://drive.google.com/file/d/1nQLyM_SoH_Uio-yiDqKmBt3PT4aIEtwp/view?usp=sharing)

The LAN configuration consists of 3 offices, two open plan offices, a client room, and a server room. Mr. Khoza has his own private office, while two laptop users share one office and the other three have separate offices. The first open office space has seven desktops, with the remaining 8 desktops in the second open office. A small room acts as a server room. The LAN network operates by connecting all devices, such as desktops, laptops, and servers, to a LAN switch, which interconnects them. The servers, located in the server room, manages and stores network data. Each office has a wired connection to the LAN switch for communication. Open-plan offices utilise the LAN switch for shared resource access with multiple desktops, while laptop offices connect laptops for resource and data access.

Wireless router is placed enabling wireless connectivity, eliminating the need for wired connections. Laptop users can access the LAN network through their offices wirelessly. The LAN design in place enhances Mr. Khoza's business operations in several ways. It allows for effective communication and data exchange among LAN devices, allows access to shared resources and data from individual offices, offers wireless flexibility and mobility across the premises, centralises data storage and management in the server room, and increases productivity and collaboration by promoting communication and resource sharing among employees. (Serpanos, 2011; Partsenidis, n.d)

IP Address Plan for Mr. Khoza:

**Mr. Khoza's Office:**

Subnet: 10.8.0.0/24

Usable IP Range: 10.8.0.1 - 10.8.0.254

Devices: Laptop and server

**Open Plan Office 1:**

Subnet: 10.8.1.0/24

Usable IP Range: 10.8.1.1 - 10.8.1.254

Devices: PCs, Printer, and server

**Open Plan Office 2:**

Subnet: 10.8.2.0/24

Usable IP Range: 10.8.2.1 - 10.8.2.254

Devices: PCs, Printer, and server

**Office 1:**

Subnet: 10.8.3.0/24

Usable IP Range: 10.8.3.1 - 10.8.3.254

Devices: Laptops and server

**Office 2:**

Subnet: 10.8.4.0/24

Usable IP Range: 10.8.4.1 - 10.8.4.254

Devices: Laptops and server

**Server Room:**

Subnet: 10.8.5.0/29

Usable IP Range: 10.8.5.1 - 10.8.5.6

Devices: Server

**Client Network:**

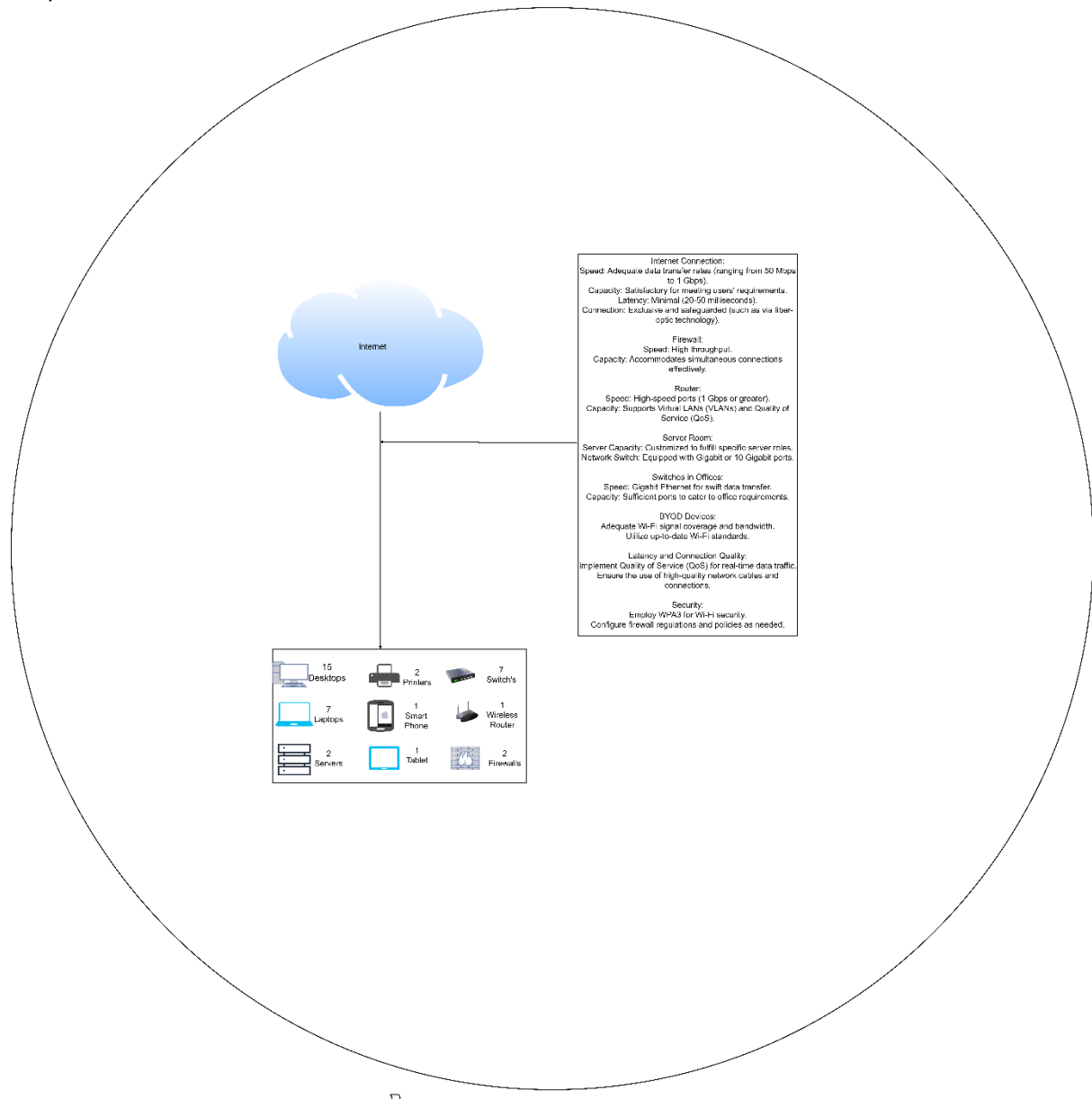
Subnet: 10.8.6.0/24

Usable IP Range: 10.8.6.1 - 10.8.6.254

Devices: Smartphone, Tablet, Laptop and Server

(Serpanos, 2011; Cisco, 2010)

1.4)



Due to clarity issues on the diagrams, please use the link below to see the text clearly if so:

<https://drive.google.com/file/d/13V30jAddVbG26rQCQMIOTfyfigizUupd/view?usp=sharing>

The WAN diagram's internet connection delivers sufficient bandwidth, ranging from 50 Mbps to 1 Gbps, to meet Mr. Khoza's business needs as it expands. This ensures data transfer speeds are in line with his requirements. The network is designed to accommodate up to thirty devices, including PCs, laptops, servers, and BYOD devices, with low latency for responsive communication and data transfer. The connection is secure, using technologies like fiber optics for enhanced data privacy and reliability. The firewall in the network design

manages data traffic efficiently, supporting multiple concurrent connections to enhance network security. The high-speed router offers advanced features like VLAN support and Quality of Service to optimise network performance for different applications and services. The server room is made to meet specific requirements like storage needs. Network switches in various offices feature Gigabit Ethernet or 10 Gigabit ports, ensuring fast and reliable connections for desktops and laptops. BYOD devices have sufficient Wi-Fi coverage and bandwidth, with modern standards ensuring efficient and secure connectivity. Quality of Service is implemented for traffic, and quality network cables and connections further improve latency and connection quality. Security measures are strong, ensuring high wireless network security, and firewall rules and policies configured to protect against potential threats, providing extra protection for Mr. Khoza's small business. (Metzler, 2015)



## Bibliography

Cavanaugh, J., 2020. *How to build a resilient network design..* [Online]

Available at: <https://www.techtarget.com/searchnetworking/tip/How-to-build-a-resilient-network-design>

[Accessed 25 September 2023].

Cisco, 2010. *IP Addressing Guide*. [Online]

Available at:

[https://www.cisco.com/c/dam/global/en\\_ca/solutions/strategy/docs/sbaBN\\_IPv4addrG.pdf](https://www.cisco.com/c/dam/global/en_ca/solutions/strategy/docs/sbaBN_IPv4addrG.pdf)

[Accessed 10 October 2023].

Cisco, n.d. *What Is Network Design?*. [Online]

Available at: <https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-design.html>

[Accessed 30 September 2023].

Jabbusch, J., 2013. *9 Immutable Laws of Network Design*. [Online]

Available at: <https://www.networkcomputing.com/networking/9-immutable-laws-network-design>

[Accessed 30 September 2022].

Metzler, D. J., 2015. *Guide to WAN architecture and design*. [Online]

Available at: <https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/intelligent-wan/wan-architecture-and-design.pdf>

[Accessed 25 October 2023].

Motiso, D., 2022. *Network Redundancy: Definition, Types and How To Improve It..* [Online]

Available at: <https://www.indeed.com/career-advice/career-development/network-redundancy>

[Accessed 25 September 2023].

Partsenidis, C., n.d. *Guidelines for designing a LAN*. [Online]

Available at: <https://www.techtarget.com/searchnetworking/answer/Guidelines-for-designing-a-LAN>

[Accessed 10 October 2023].

Serpanos, D., 2011. *Architecture of Network System*. Burlington: Elsevier.

Zayo, 2023. *What is Network Resilience?*. [Online]

Available at: <https://www.zayo.com/resources/what-is-network-resilience/#:~:text=A%20resilient%20network%20is%20one.failed%20equipment%20to%20natural%20disasters%20can%20be%20avoided,failed%20equipment%20to%20natural%20disasters%20can%20be%20avoided>

20disasters.

[Accessed 25 September 2023].

### **Report on changes:**

For POE PT1 I was required to improve on question 1.3, activity 2 and activity 3. For 1.3 I used more practical examples related to Mr. Khoza's network design for each factor. I spoke about these practical examples in detail as well. For activity 2 I had to change my next generation architecture which was Peer 2 Peer(P2P) as it wasn't really a next generation, so I looked for more examples of next gen architecture in my textbook and found Domain Name System(DNS) which was more of a next generation architecture. With the change to DNS, I was able to find, focus and improve on shortcomings of DNS. For Activity 3 I did not include example for what was being asked however, now there are detailed examples provided.

For POE PT 2 I was required to improve on Question 1(1.1 and 1.2). For 1.1 I linked each factor to practical application with in Mr. Khoza's design. For 1.2, I linked the 10 principles to practical application with in Mr. Khoza's design. With these changes it helped me get a better understanding on what they were exactly asking for in the questions of the POE.

## Activity 2

This proposal covers various factors, including a network description, an updated LAN and WAN diagrams of Mr. Khoza's business, main considerations, office connectivity strategies outlining the routing approach, a justification for necessary devices and protocols involved, and involved QoS specifications designed for Mr. Khoza.

### Description:

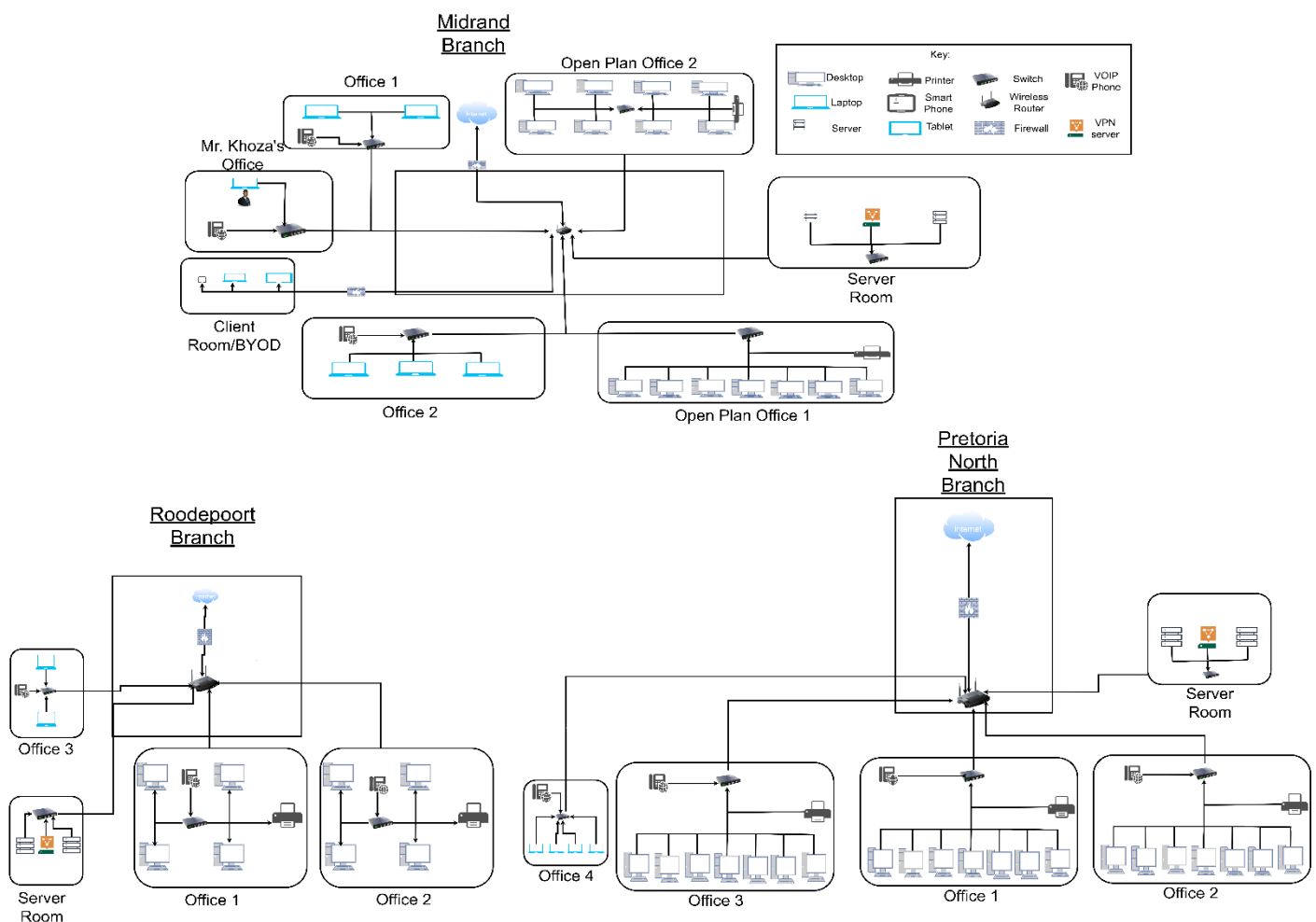
For Mr. Khoza to have a strong network infrastructure it must include:

- A Local Area Network(LAN) (Serpanos, 2011)
- A Wide Area Network(WAN) (Serpanos, 2011)
- Servers and VPN servers (Serpanos, 2011)
- A secure network (Serpanos, 2011)
- Remote Access (Serpanos, 2011)

With this, Mr. Khoza network infrastructure will be strong and well secured allowing offices to connect, work remotely, share information, resources, and communicate. (Serpanos, 2011)

### LAN And WAN Network Diagrams

LAN Diagram(Serpanos, 2011):



## IP Address Plan for Mr. Khoza:

### Midrand branch

#### **Mr. Khoza's Office:**

Subnet: 10.8.0.0/24

Usable IP Range: 10.8.0.1 - 10.8.0.254

Devices: VoIP phone, Laptop, and server

#### **Open Plan Office 1:**

Subnet: 10.8.1.0/24

Usable IP Range: 10.8.1.1 - 10.8.1.254

Devices: PCs, Printer, and server

#### **Open Plan Office 2:**

Subnet: 10.8.2.0/24

Usable IP Range: 10.8.2.1 - 10.8.2.254

Devices: PCs, Printer, and server

#### **Office 1:**

Subnet: 10.8.3.0/24

Usable IP Range: 10.8.3.1 - 10.8.3.254

Devices: VoIP phone, Laptops, and server

#### **Office 2:**

Subnet: 10.8.4.0/24

Usable IP Range: 10.8.4.1 - 10.8.4.254

Devices: VoIP phone, Laptops, and server

#### **Server Room:**

Subnet: 10.8.5.0/29

Usable IP Range: 10.8.5.1 - 10.8.5.6

Devices: Server, VPN server

#### **Client Network:**

Subnet: 10.8.6.0/24

Usable IP Range: 10.8.6.1 - 10.8.6.254

Devices: Smartphone, Tablet, Laptop and Server

(Serpanos, 2011; Cisco, 2010)

## Roodepoort Branch:

### **Office 1:**

Subnet: 10.9.1.0/24

Usable IP Range: 10.9.1.1 - 10.9.1.254

Devices: VoIP phone, PCs, Printer, and server

### **Office 2:**

Subnet: 10.9.2.0/24

Usable IP Range: 10.9.2.1 - 10.9.2.254

Devices: VoIP phone, PCs, Printer, and server

### **Office 3:**

Subnet: 10.9.3.0/24

Usable IP Range: 10.9.3.1 - 10.9.3.254

Devices: VoIP phone, Laptops, and server

### **Server Room:**

Subnet: 10.9.4.0/25

Usable IP Range: 10.9.5.1 - 10.9.5.6

Devices: Server, VPN server

(Serpanos, 2011; Cisco, 2010)

## Pretoria Branch:

### **Office 1:**

Subnet: 10.10.1.0/24

Usable IP Range: 10.10.1.1 - 10.10.1.254

Devices: VoIP phone, PCs, Printer, and server

### **Office 2:**

Subnet: 10.10.2.0/24

Usable IP Range: 10.10.2.1 - 10.10.2.254

Devices: : VoIP phone, PCs, Printer, and server

### **Office 3:**

Subnet: 10.10.2.0/24

Usable IP Range: 10.10.2.1 - 10.10.2.254

Devices: VoIP phone, PCs, Printer, and server

### **Office 4:**

Subnet: 10.10.4.0/24

Usable IP Range: 10.10.4.1 – 10.10.4.254

Devices: VoIP phone, Laptops and server

**Server Room:**

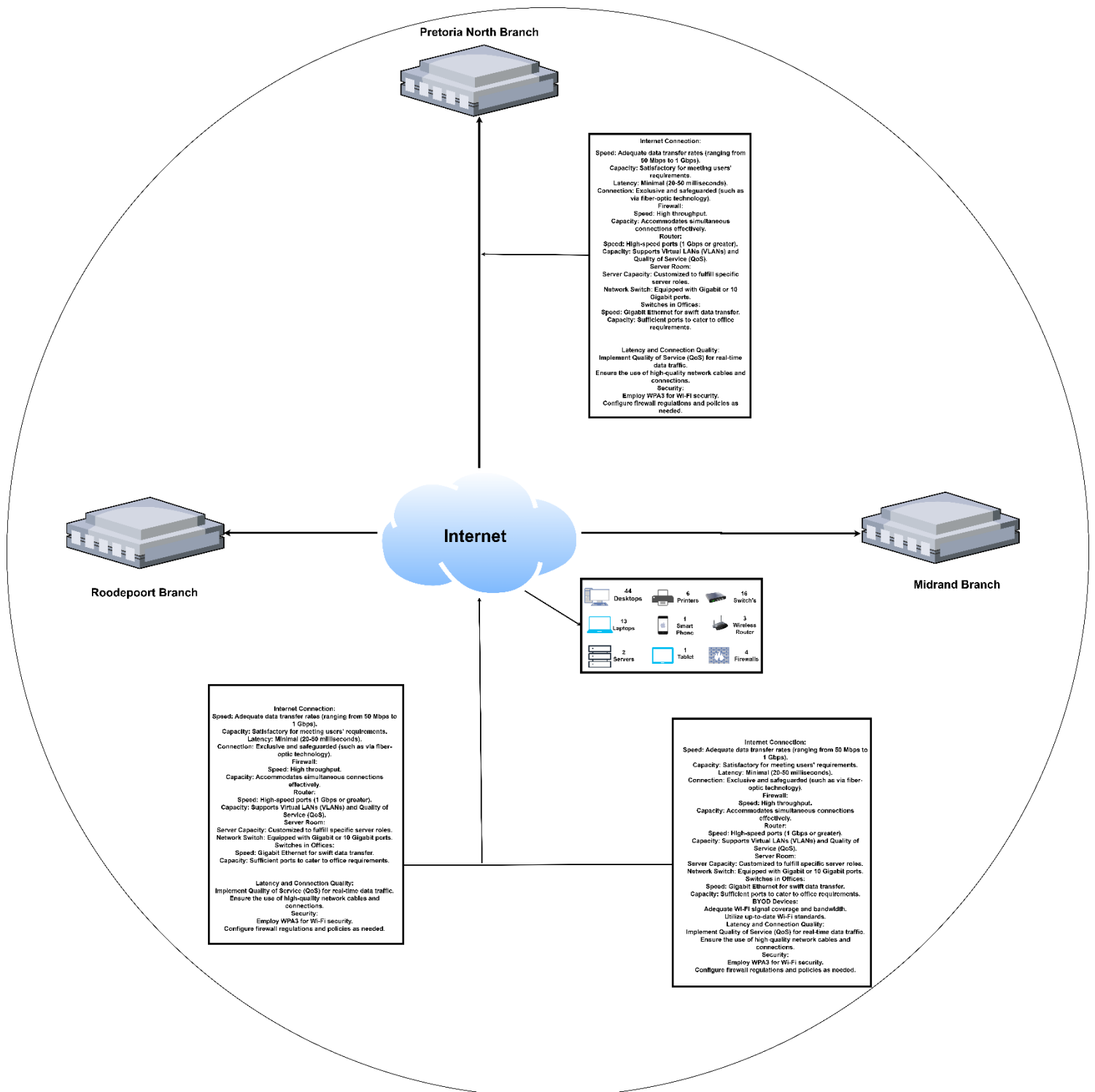
Subnet: 10.10.5.0/29

Usable IP Range: 10.10.5.1 - 10.10.5.6

Devices: Server, VPN server

(Serpanos, 2011; Cisco, 2010)

## WAN Diagram(Serpanos, 2011):



### **Main considerations:**

Scalability, Server Redundancy, Network Performance and Security are taken into consideration. Network scalability should be a main consideration in designing Mr. Khoza's network infrastructure, allowing for future expansion. Utilise scalable hardware and architecture, such as VLANs and strong routing, to support increased users and branches. Use security across all network levels by implementing firewalls and wireless routers, access controls and strong encryption methods for data transmission. Regularly updating software and conducting security checks are essential to promptly address vulnerabilities. Ensure high availability and integrate redundant server configurations such as clustering, RAID configurations, or backup servers, while preserving this redundancy in critical services to prevent disruptions caused by hardware failures. In terms of network performance, employ advanced technologies and recommended methods to enhance network efficiency. Use quality of service (QoS) tools to prioritise essential data, secure sufficient bandwidth, and reduce delays. Apply effective network protocols like ethernet, and consistently supervise and control network flow to uphold peak performance. With this Mr. Khoza's infrastructure will have a high network performance. (Fortinet, n.d.; Serpanos, 2011; Team, 2023; Gillis, 2021)

### **Connectivity and Justification:**

For Mr. Khoza's business, an infrastructure will be established with ethernet cabling for internal connections and a firewall for security measures. Each office in Midrand will have switches, and ethernet connectivity for VoIP phones, PCs, laptops, printers, and servers. Interconnecting offices will be achieved through VPNs, including VPN Servers for the Roodepoort and Pretoria North branches, ensuring connectivity.(Serpanos, 2011)

### **Quality Of Service(QoS) Details involved:**

To assure network performance, Mr. Khoza's network design requires focused attention on QoS. This involves prioritising applications such as VoIP(VoIP phones) and video conferencing(Laptops and computers) to minimise latency, allocating sufficient bandwidth specifically for server operations while restricting guest network bandwidth, implementing traffic shaping to prevent individual users or applications from exploiting resources without compromising network efficiency. These steps form a strong and efficient network that provides to Mr. Khoza's current business needs. (Fortinet, n.d.; Serpanos, 2011)

In conclusion the proposed network infrastructure for Mr. Khoza's business prioritises scalability, security, and performance. It includes LAN/WAN diagrams, IP planning, and strong security measures like firewalls and access controls. Utilising VLANs and redundancy ensures scalability and high availability. Ethernet, VPNs, and VoIP enable connectivity between offices. Prioritising QoS for essential applications optimises network performance, organising to current needs and enabling future growth across branches, ensuring a strong and adaptable infrastructure. (Serpanos, 2011)



### Activity 3

1) From my understanding, examining one's ideas, experiences, or behaviours while condensing several illustrative aspects and examples is what reflection includes. It is complete in all aspects, ensuring that each component is fully examined and skilfully expressed. It's about going deep into comprehension and providing an extensive analysis that doesn't leave any detail unexamined or unchecked. (Health and Care Professions Council, 2021)

2) This POE taught me network designs, practical implementations, to reflect on my corrections from the feedback given by the lecturer and proposal writing. It expanded my understanding of network structures.

3) Updating Part 1 and Part 2 using feedback from the lecturer taught me the value of improving my work. It showed me other possible answers to approach a specific question allowing me to use different ideas in what I write in my answers.

4) Using the updated POE Part 1 and Part 2, it taught me better network designs and how feedback improves on my mistake. Looking at my previous work, it helped me improve my skills for better POE overall.

5) The tasks in POE Part 1, Part 2, and the final POE showed how projects are managed from start to finish. They helped me see the steps from planning to completion, giving a clear indication of how a project progresses from beginning to end.

## Self-Evaluation Rubric:

20

2023

### Activity 3 Rubric

This section is the reflection report on the learning experience. The self-evaluation must be completed by the student and included in the submission.

### SELF-EVALUATION

Student Number: ST10275486

(Each student must complete one of these rubrics as part of their POE submission. Review their self-evaluation and if you disagree then change the marks accordingly)

Criteria	1 You have learned something – but you are not proving it.	2 You are on the right track, but you can do better.	3 Well done. You have done exceptionally well.	Score
Reflection	<ul style="list-style-type: none"> <li>Reflection shows no thoughtfulness;</li> <li>Reflection has no details;</li> <li>Reflection is incomplete.</li> </ul>	<ul style="list-style-type: none"> <li>Reflection shows little thoughtfulness;</li> <li>Reflection has few details or examples;</li> <li>Most parts of the reflection are incomplete.</li> </ul>	<ul style="list-style-type: none"> <li>Reflection shows thorough thoughtfulness;</li> <li>Reflection has several supporting details and examples;</li> <li>All parts of the reflection are complete and done well.</li> </ul>	2
Demonstration of learning	<ul style="list-style-type: none"> <li>Reflection does not move beyond the description of the event/experience.</li> </ul>	<ul style="list-style-type: none"> <li>The reflection demonstrates the student's attempt to analyse the event/experience but fails to demonstrate depth of analysis.</li> </ul>	<ul style="list-style-type: none"> <li>Clearly explains what was learned;</li> <li>Reflection is beyond a simple description of an event/experience to an analysis of how it contributed to learning and understanding.</li> </ul>	2

20

2023

Criteria	1 You have learned something – but you are not proving it.	2 You are on the right track, but you can do better.	3 Well done. You have done exceptionally well.	Score
The organisation of report and clarity of the report	<ul style="list-style-type: none"> <li>Ideas are disorganised;</li> <li>Language is unclear and confusing throughout.</li> </ul>	<ul style="list-style-type: none"> <li>Ideas are organised but paragraphs are not well constructed;</li> <li>Frequent lapses in clarity.</li> </ul>	<ul style="list-style-type: none"> <li>Ideas are very well organised with well-constructed paragraphs;</li> <li>The language is clear and expressive;</li> <li>The reader can create a mental picture of the situation being described;</li> <li>Explanation of concepts makes sense to an uninformed reader.</li> </ul>	3
Demonstration that learning has taken place by addressing comments and feedback provided by the lecturer (1 mark)				
<b>TOTAL</b>				<b>7 /10</b>

## Bibliography

Cisco (2010). *IP Addressing Guide*. [Online] Available at:

[https://www.cisco.com/c/dam/global/en\\_ca/solutions/strategy/docs/sbaBN\\_IPv4addrG.pdf](https://www.cisco.com/c/dam/global/en_ca/solutions/strategy/docs/sbaBN_IPv4addrG.pdf)

[Accessed 10 October 2023].

Fortinet (n.d.). *What is Quality of Service (QoS) in Networking?* [online] Fortinet. Available

at: [https://www.fortinet.com/resources/cyberglossary/qos-quality-of-](https://www.fortinet.com/resources/cyberglossary/qos-quality-of-service#:~:text=Quality%20of%20service%20(QoS)%20is)

[service#:~:text=Quality%20of%20service%20\(QoS\)%20is](https://www.fortinet.com/resources/cyberglossary/qos-quality-of-service#:~:text=Quality%20of%20service%20(QoS)%20is) [Accessed 30 Nov. 2023].

Gillis, A. (2021). *What is RAID?* [online] SearchStorage. Available at:

<https://www.techtarget.com/searchstorage/definition/RAID> [Accessed 30 Nov. 2023].

Health and Care Professions Council (2021). *What Is Reflection?* [online] [www.hcpc-uk.org](http://www.hcpc-uk.org).

Available at: [https://www.hcpc-uk.org/standards/meeting-our-standards/reflective-](https://www.hcpc-uk.org/standards/meeting-our-standards/reflective-practice/what-is-reflection/)

[practice/what-is-reflection/](https://www.hcpc-uk.org/standards/meeting-our-standards/reflective-practice/what-is-reflection/) [Accessed 1 Dec. 2023].

Serpanos, D., 2011. *Architecture of Network System*. Burlington: Elsevier.

Team, W. (2023). *Exploring Scalability in Networking for Business Growth*. [online] Blog

Wrike. Available at: [https://www.wrike.com/blog/exploring-scalability-in-](https://www.wrike.com/blog/exploring-scalability-in-networking/#:~:text=Scalability%20refers%20to%20the%20capability)

[networking/#:~:text=Scalability%20refers%20to%20the%20capability](https://www.wrike.com/blog/exploring-scalability-in-networking/#:~:text=Scalability%20refers%20to%20the%20capability) [Accessed 30 Nov. 2023].