Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

- **RFC**: Request for Comments
- **CIDR**: Classless Inter-Domain Routing
- **IPS**: Intrusion Prevention System
- **IDS**: Intrusion Detection System
- **OSI**: Open Systems Interconnection
- **IP**: Internet Protocol
- **TCP**: Transmission Control Protocol
- **IANA**: Internet Assigned Numbers Authority
- **NAT**: Network Address Translation
- **AFRINIC**: African Network Information Centre

QUESTION 1

Explain 192.168.20.0/26?

IP addresses are expressed using the dotted decimal notation. In this format, each of the four bytes is expressed in decimal form, ranging from 0 to 255.

In order to fully understand the value of CIDR, it is important to briefly discuss the design that came before it. Prior to 1993, IP addresses were categorised into five distinct groups as seen in Figure 1.1. This allocation is sometimes referred to as classful addressing.

Rekhter & Li (1993) in RFC 1518 (7) entitled "An Architecture for IP Address Allocation with CIDR" illustrated a scalable and efficient method for address allocation within the Internet by introducing the concept of Classless Inter-Domain Routing (CIDR). This approach mitigates the growth of routing tables and maximizes the utilization of available IP address space by allowing for variable-length subnet masking, which enables the division of IP addresses into groups that can be routed with a single network prefix.

Furthermore, the Internet Protocol specification RFC 791 defined three classes of addresses to define the relative size of these portions per class. These classes, denoted simply as classes A, B, and C, were identified by the initial bits of the 32-bit address as depicted in Figure 1.1

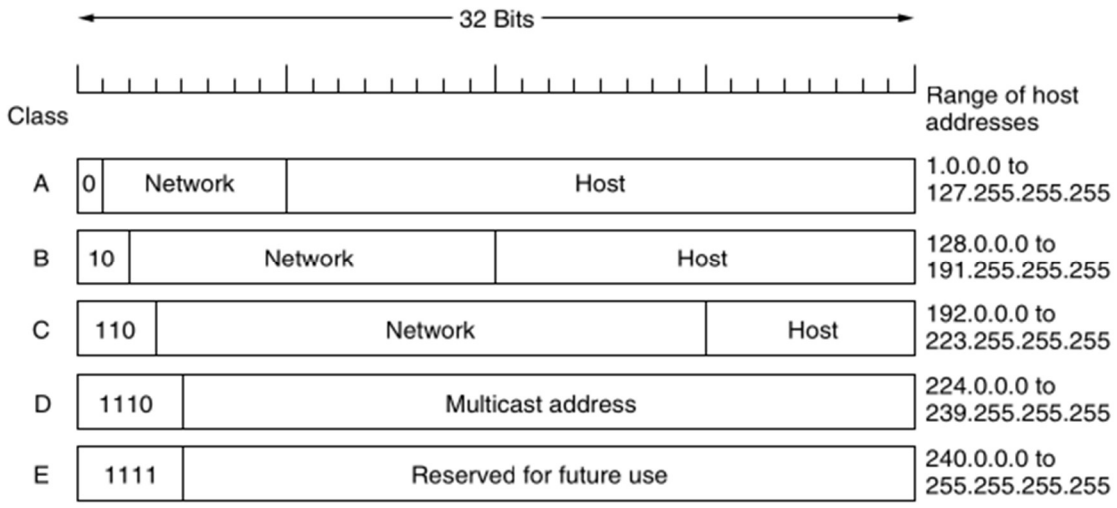

Figure 1.1: IP address formats (class-based IP addressing)

(Courtesy: Figure 5-53, Tanenbaum & Wetherall, 2010, p. 449)

Table 1.1: Class C Limits

(Courtesy: Table 3.31, Liu, D. (2009) *Cisco CCNA/CCENT Exam 640-802, 640-822, 640-816 Preparation Kit*. Syngress Publishing, p. 106.)

Table 3.31 Class C Limits

Class	C
Default network mask	255.255.255.0
Number of networks	2,097,152, which is 65,536 = 256 × 256 (for the second and third octet), times 32 = 223 – 192 + 1 (for the first octet)
Number of hosts per network	254, which is 256 (for the fourth octet); minus 2 (broadcast and network address)
First network address	192.0.0.0
First address assignable to a host	192.0.0.1 (one after the first network address)
First broadcast address	192.0.0.255 (last address of the first network)
Last network address	192.255.255.0
Last broadcast address	192.255.255.255
Last address assignable to a host	192.255.255.254 (one before the last broadcast address)

Table 1.2: Addresses Represented with the CIDR Notation

(Courtesy: Table 3.36, Liu, D. (2009) *Cisco CCNA/CCENT Exam 640-802, 640-822, 640-816 Preparation Kit*. Syngress Publishing, p. 117.)

Table 3.36 Addresses Represented with the CIDR Notation

IP Address	Subnet Mask	Subnet Mask in Binary	Number of 1s	CIDR
192.168.10.100	255.255.255.192	11111111.11111111.11111111.11000000	26	192.168.0.100/26
10.20.30.40	255.240.0.0	11111111.11110000.00000000.00000000	12	10.20.30.40/12
234.192.111.30	255.255.255.128	11111111.11111111.11111111.10000000	25	234.191.111.30/25
130.145.160.180	255.255.224.0	11111111.11111111.11100000.00000000	19	130.145.160.180/19

The IP address 192.168.20.0/26 is part of the IPv4 addressing scheme as per **Figure 1.1**

- 192.168.20.0 is the IP address itself.
- /26 is the subnet mask in CIDR (Classless Inter-Domain Routing) notation.

Type of Class

The IP address 192.168.20.0 originally falls within the Class C range when considering the traditional classful network scheme because its first octet is between 192 and 223 with respect to Table 1.1

Conversion to Dotted Decimal Notation

With respect to Table 1.2, the /26 in the CIDR notation indicates that the first 26 bits of the subnet mask are set to 1. Below are how to write this in binary and then in dotted decimal:

- A full octet of bits set to 1 is 11111111, which is 255 in decimal.
- The first three octets will be full, so they will all be 255.
- The fourth octet has 26 - 24 = 2 bits set to 1 (since the first three octets contain 24 bits in total), so it will start with 11000000 in binary, which is 192 in decimal.
- Thus, the subnet mask in dotted decimal notation is 255.255.255.192.

To summarise:

- The type of class, in traditional terms, would be Class C.
- The subnet mask /26 converts to a dotted decimal notation as 255.255.255.192.

CIDR Notation	Binary Subnet Mask	Dotted Decimal Notation
/26	11111111.11111111.11111111.11000000	255.255.255.192

What do you understand by the following terms?

1. Private IP address

2. Public or Global IP address

Both IPv4 and IPv6 are iterations of the Internet Protocol, a collection of regulations that govern the transmission and reception of data across the internet. The primary distinction among them pertains to the extent of the address space. The address space is limited to 4.29 billion with IPv4's 32-bit addresses, whereas IPv6's 128-bit addresses enable the addressing of a significantly greater number of devices.

A private IP address is an address that is not routable over the internet and is utilised exclusively within a private network. While lacking uniqueness on a global scale, it does possess exclusivity within its immediate local network. The Internet Assigned Numbers Authority (IANA) establishes these addresses, which are typical for enterprise local area networks (LANs), residential networks, and office networks. Devices possessing private IP addresses are able to connect to the internet via a network address translation (NAT) service implemented on a router. This service converts private IP addresses to their corresponding public addresses. These IPv4 addresses are derived from specific domains designated for private use and are defined in RFC 1918:

- 172.16.0.0 to 192.168.255.255 (192.168/16 prefix),
- 10.0.0.0.0 to 10.255.255.255 (10/8 prefix), and
- 192.168.0.0 to 172.31.255.255 (172.16/12 prefix).
- For IPv6, private addresses are known as Unique Local Addresses (ULA) and are defined in the RFC 4193. They typically start with fc00: :/7.

Figure 1.2: Ranges of Private IPv4 Addresses as Specified by RFC 1918

A public or global IP address is allocated to computational devices for the purpose of establishing a distinct identification for them on the internet. Each of these addresses must be distinct throughout the complete internet. Public IP addresses are accessible and routable over the global internet, barring any security settings or firewalls that may impede access. These addresses are assigned to end-users by Internet service providers (ISPs) and are utilised by remote servers, websites, and any other device or service that must be accessible from multiple locations on the internet. Public IP addresses, as opposed to private IP addresses, are restricted and must be allocated uniquely to avoid duplication. In response to the depletion of IPv4 addresses, IPv6 has been designed to offer an essentially infinite quantity of distinct IP addresses.

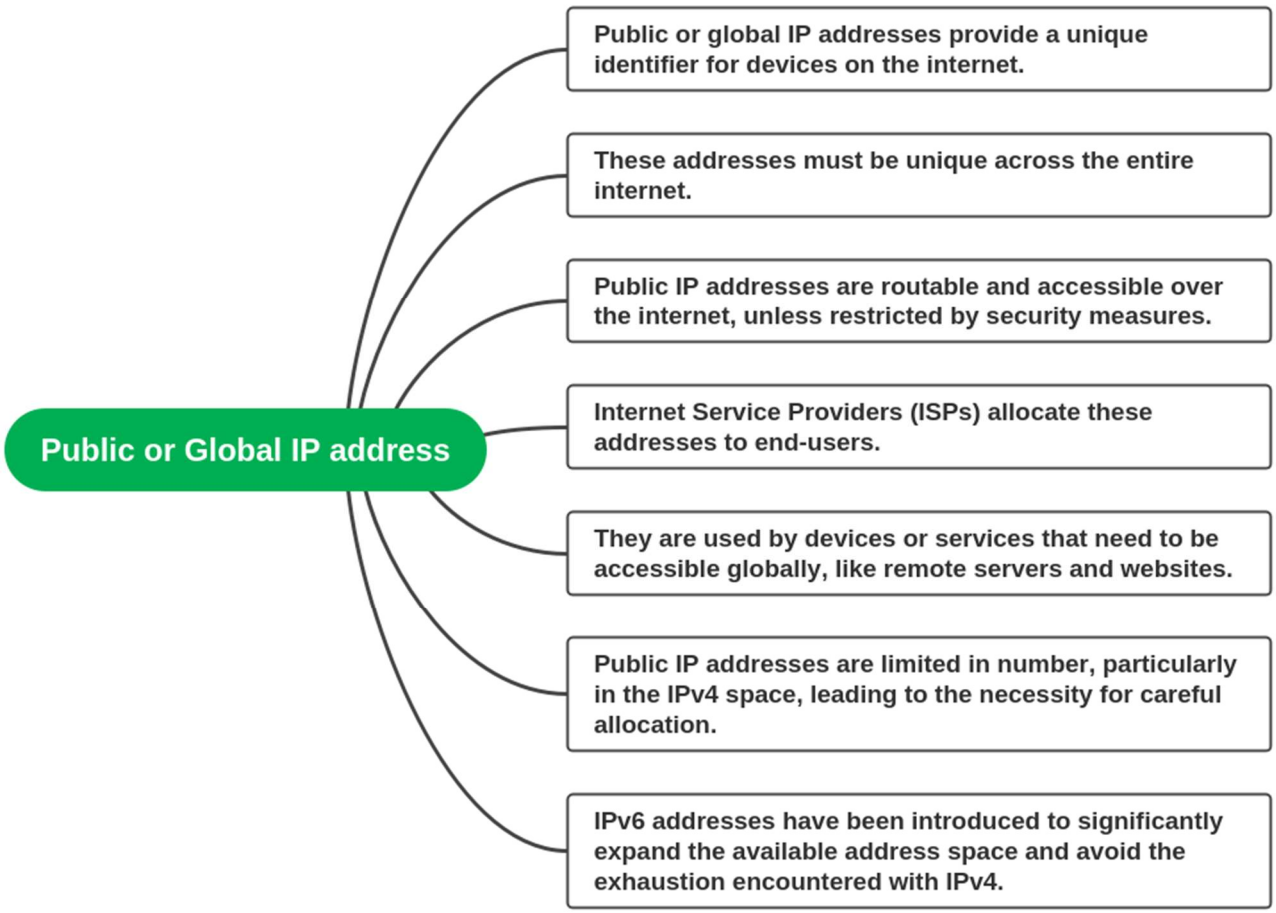

Figure 1.3: Characteristics and Allocation of Public or Global IP Addresses

Refer to question b). above, explain which IP address is being and why?

The IP address 192.168.20.0/26 is being used as a private IP address. Moskowitz et al. (1996) in RFC 1918 (5) entitled "Address Allocation for Private Internets" give clear indication in this regard. This designation is in accordance with the guidelines established by RFC 1918, which designates specific IP address ranges exclusively for private usage.

According to the Table 1.3, the address 192.168.20.0/26 falls within the 192.168.0.0/16 range. Specifically, the /26 subnet mask means that the first 26 bits of the IP address are the network part of the address, with the remaining 6 bits designated for host addresses within that network.

The IANA reserves the following IPv4 address ranges for private internets in accordance with the standards outlined in the Internet Engineering Task Force (IETF) document RFC-1918; these ranges are not publicly routable on the global internet.

- The 10.0.0.0/8 range covers all IP addresses from 10.0.0.0 to 10.255.255.255.
- The 172.16.0.0/12 range covers all IP addresses from 172.16.0.0 to 172.31.255.255.
- The 192.168.0.0/16 range covers all IP addresses from 192.168.0.0 to 192.168.255.255.

Table 1.3: CIDR and Dotted Binary Addresses

(Courtesy: Table 3.37, Liu, D. (2009) *Cisco CCNA/CCENT Exam 640-802, 640-822, 640-816 Preparation Kit*. Syngress Publishing, p. 118.)

Table 3.37 CIDR and Dotted Binary Addresses

Address in CIDR Format	IP Address in Dotted Binary
192.168.100.0/24	11000000.10101000.01100100.000000000
192.168.101.0/24	11000000.10101000.01100101.000000000
192.168.102.0/24	11000000.10101000.01100110.000000000
192.168.103.0/24	11000000.10101000.01100111.000000000

Table 1.4: Special Use IPV4 Addresses

(Courtesy: Table 2.1, Rooney, T. (2011). *Introduction to IP Address Management*. John Wiley & Sons. p.34)

TABLE 2-1: IPv4 Address Allocations (9–10)

Address Space	Special Use
0.0.0.0/8	"This" network; 0.0.0.0/32 denotes this host on this network
10.0.0.0/8	Private IP address space, not routable on the public Internet per RFC 1918
127.0.0.0/8	Assigned for use as the Internet host loopback address, i.e., 127.0.0.1/32
169.254.0.0/16	The "link local" block used for IPv4 auto-configuration for communications on a single link
172.16.0.0/12	Private IP address space, not routable on the public Internet per RFC 1918
192.0.0.0/24	Reserved for IETF protocol assignments
192.0.2.0/24	Assigned as "Test-Net-1" for use in documentation and sample code
192.88.99.0/24	Allocated for 6to4 relay anycast addresses (6to4 is an IPv4-IPv6 co-existence technology discussed in Chapter 8)
192.168.0.0/16	Private IP address space, not routable on the public Internet per RFC 1918
198.18.0.0/15	Allocated for use in benchmark tests of network interconnect devices
198.51.100.9/24	Assigned as "Test-Net-2" for use in documentation and sample code
203.0.113.0/24	Assigned as "Test-Net-3" for use in documentation and sample code
224.0.0.0/4	Allocated for IPv4 multicast address assignments (formerly Class D space)
240.0.0.0/4	Reserved for future use (formerly Class E space)
255.255.255.255/32	Limited broadcast on a link

Differentiate between Private and Public IP in our context.

When designing the network infrastructure for the medical store using the subnet 192.168.20.0/26, it is critical to comprehend the distinction between public and private IP addresses:

Private IP Addresses:

- **Application**: The subnet 192.168.20.0/26 is situated within the RFC 1918-specified private IP address space. This signifies that its utilisation is restricted to private networks and it cannot be routed on the worldwide internet. Internal communication within the medical store's network would occur over this spectrum using devices.
- **Characteristics**: The aforementioned addresses are network-local and shall be employed by every internal device within the medical store's network, including computers, point-of-sale systems, printers, and any other devices that require communication.
- In order to prevent unauthorised access from the outside internet, private IP addresses must be routed through a gateway utilising Network Address Translation (NAT).
- Private IP addresses do not incur any expenses due to the fact that they lack global uniqueness and are therefore accessible to all users within private networks.

Public IP Locations:

- The utilisation of a public IP address is mandatory for any device within the network that necessitates direct internet access. This includes a server that hosts the website for the medical store as well as a remote access VPN.
- The nature of public IP addresses is such that they are unique across the entire internet and are assigned by Internet Service Providers (ISPs) or African Network Information Centre (AFRINIC)
- **Accessibility**: Public IP addresses, in contrast to private IP addresses, are globally routable, meaning they are reachable from any location on the internet.
- ISPs generally impose a fee for public IP addresses, particularly static ones that remain constant over time.

Implementation within the medical store network:

Regarding internal networking, the medical store will allocate the private IP range 192.168.20.0/26 to various devices and computers.

Internet Access: By utilising a router or firewall that implements NAT, any of these devices will be able to connect to the internet. The ISP will provide the public IP address that is converted from the private IP address. This public IP address will serve as the online representation of the network.

In essence, private IP addresses will be utilised for local networking within the medical store, thereby separating internal traffic from that of the public internet. In the event that internal devices necessitate an internet connection, they will employ a public IP address that has been allocated by their ISP, generally via a NAT process implemented on the gateway.

Refer to the IP address given, calculate the following:

i) Subnet mask.

ii). the number of Subnet/s

iii). the number of Hosts per subnet

Part e (i)

1. **Understanding the CIDR Notation**:
    - CIDR notation /26 means that the first 26 bits of the IP address are reserved for the network portion.
    - This leaves the remaining bits (32 - 26 = 6 bits) for host addresses within the subnet.

2. **Calculating the Binary Subnet Mask**:
    - Writing out 26 '1's to represent the network portion of the address in binary.
    - Following this with 6 '0's to represent the host portion.
    - The resulting binary subnet mask is: 11111111.11111111.11111111.11000000

3. **Converting the Binary to Dotted Decimal Notation**:
    - Dividing the binary string into four octets (groups of 8 bits): 11111111, 11111111, 11111111, 11000000.
    - Converting each binary octet to decimal:
        - 11111111 in binary equals 255 in decimal.
        - 11000000 in binary equals 192 in decimal.
    - The other two octets are also 11111111, so they also convert to 255.

4. **Writing the Subnet Mask in Dotted Decimal**:
    - Combining the decimal values of the four octets separated by dots.
    - The final subnet mask in dotted decimal notation is: 255.255.255.192

5. **Verifying the Subnet Mask**:
    - Making sure there are 32 bits in total.
    - Ensuring the transition from '1's to '0's only happens once, as subnet masks must be contiguous.

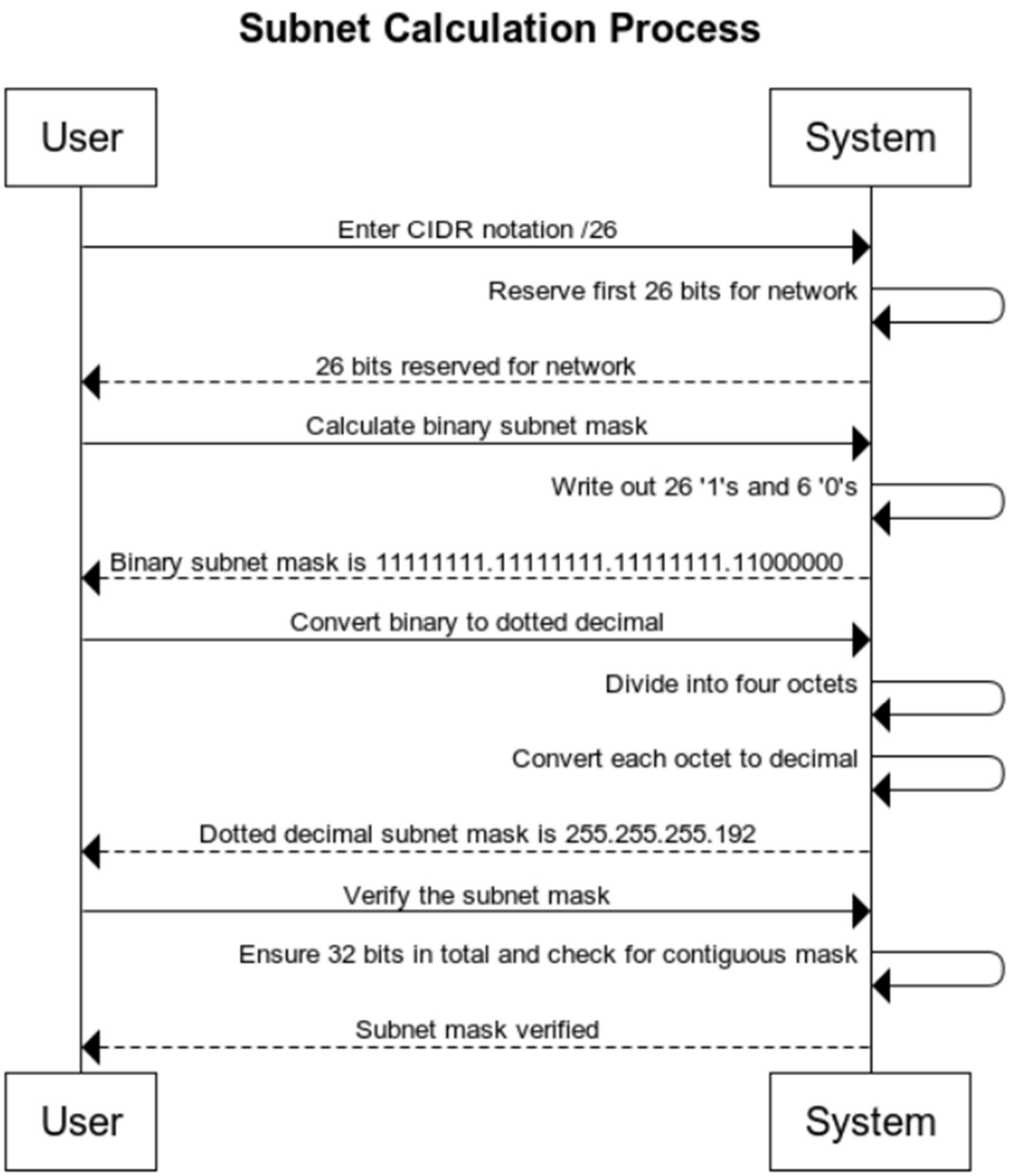

Figure 1.4: Sequence diagram for subnet calculation

Step Description	Binary Representation	Dotted Decimal Notation
Network portion for /26 (26 bits)	11111111.11111111.11111111.11000000	-
Split into octets	11111111	11111111
Convert each octet to decimal	11111111 (255)	11111111 (255)
Final subnet mask in dotted decimal	-	255.255.255.192

Each binary octet is converted into its decimal equivalent, which gives us the final subnet mask in the dotted decimal format used in IP addressing.

Part e (ii)

Table 1.5 shows how to calculate the number of /26 subnets within a /16 network.

Table 1.5: IPv4 Subnetting Calculation Steps for a /16 Network Block

Step	Description	Calculation	Result
1	Determine the size of the original network block	-	/16 (for 192.168.x.x)
2	Determine the size of the subnet	-	/26
3	Calculate the bit difference for subnet size	26 - 16	10 bits
4	Calculate the number of subnets	2^10	1024 subnets
5	Identify the starting subnet address	-	192.168.0.0/26
6	Increment to find subsequent subnet addresses	+64 addresses per subnet	Starts at 192.168.0.0, ends at 192.168.255.192

Table 1.6 outlines the steps referring to the subnets within the 192.168.20.0/24 range. Therefore, the number of /26 subnets would be:

Table 1.6: Subnet Division Steps for a /24 Network Block

Step	Description	Calculation	Result
1	Determine the size of the original network block	-	/24 (for 192.168.20.x)
2	Determine the size of the subnet	-	/26
3	Calculate the bit difference for subnet size	26 - 24	2 bits
4	Calculate the number of subnets	2^2	4 subnets
5	Identify the starting subnet address	-	192.168.20.0/26
6	Increment to find subsequent subnet addresses	+64 addresses per subnet	192.168.20.0, 192.168.20.64, 192.168.20.128, 192.168.20.192

This gives us the 4 subnets which fits within the single /24 network block of 192.168.20.0/24.

Part e (iii)

To determine the number of hosts per subnet, we can refer to the binary structure of IP addresses and subnet masks.

1. **Subnet Size**: A subnet with a /26 prefix means that 26 bits are used for the network part, and the remaining bits are used for hosts.
2. **Host Bits**: With a /26 prefix, there are 32 - 26 = 6 bits available for host addresses.
3. **Number of Addresses**: Each bit in the host portion can be either 0 or 1. So, with 6 bits for hosts, the total number of combinations (and therefore the total number of addresses) is 26.
4. **Total Addresses Calculation**: $2^6 = 64$ This means there are 64 addresses in total for each subnet.
5. **Usable Addresses**: Out of these 64 addresses, 1 is reserved for the network address (all host bits are 0) and 1 for the broadcast address (all host bits are 1). Therefore, the number of usable addresses for hosts is 64 - 2 = 62.

In conclusion, each /26 subnet contains 64 total addresses, of which 62 are usable for assigning to devices.

Table 1.7: Details of /26 Subnet Allocation within the 192.168.20.0/24 Network

Subnet ID	Network Address	Usable Host Range	Broadcast Address
1	192.168.20.0	192.168.20.1 - 192.168.20.62	192.168.20.63
2	192.168.20.64	192.168.20.65 - 192.168.20.126	192.168.20.127
3	192.168.20.128	192.168.20.129 - 192.168.20.190	192.168.20.191
4	192.168.20.192	192.168.20.193 - 192.168.20.254	192.168.20.255

Part f

Select a block of IP of your choice from your answer and provide the following:
1. Network ID
2. Broadcast ID
3. Valid Hosts

Using Subnet **ID#4** from Table 1.7,

1) To Find the Network ID:

1. **Identifying the Subnet**: Looking at the subnet address provided, in this case, 192.168.20.192/26.
2. **Understanding CIDR Notation**: The /26 indicates that the first 26 bits are the network portion of the address.
3. **Calculating the Network Address**: For the network 192.168.20.192/26, the network ID is the IP address with the last (32 - 26) bits set to 0. In this case, 192.168.20.192 is already the network address because the last 6 bits (of the fourth octet) are 0.

2) To Find the Broadcast ID:

1. **Identifying the Subnet and its Size**: Use the subnet's CIDR notation to understand the size. Here, it's /26.
2. **Determining the Range of the Subnet**: Calculate the range by noting that the /26 means 6 bits are used for hosts.
3. **Calculating the Broadcast Address**: Set all the host bits to 1 on the network address. For 192.168.20.192/26, the broadcast address is the IP with the last 6 bits set to 1, which gives 192.168.20.255

3) To Find the Valid Hosts:

1. **Starting with the Network ID**: From the previous step, it is known that the Network ID is 192.168.20.192.
2. **End with the Broadcast ID**: We also have the Broadcast ID as 192.168.20.255.
3. **Calculating the Usable Range**: The valid hosts are all the addresses between the network ID and the broadcast ID, exclusive. So, incrementing the network ID by 1 to get the first valid host (192.168.20.193) and decrementing the broadcast ID by 1 to get the last valid host (192.168.20.254).

4. **List the Range**: All addresses between 192.168.20.193 and 192.168.20.254 are valid hosts.

So, in summary for Subnet **ID#4**:

- **Network ID**: 192.168.20.192
- **Broadcast ID**: 192.168.20.255
- **Valid Hosts Range**: 192.168.20.193 - 192.168.20.254

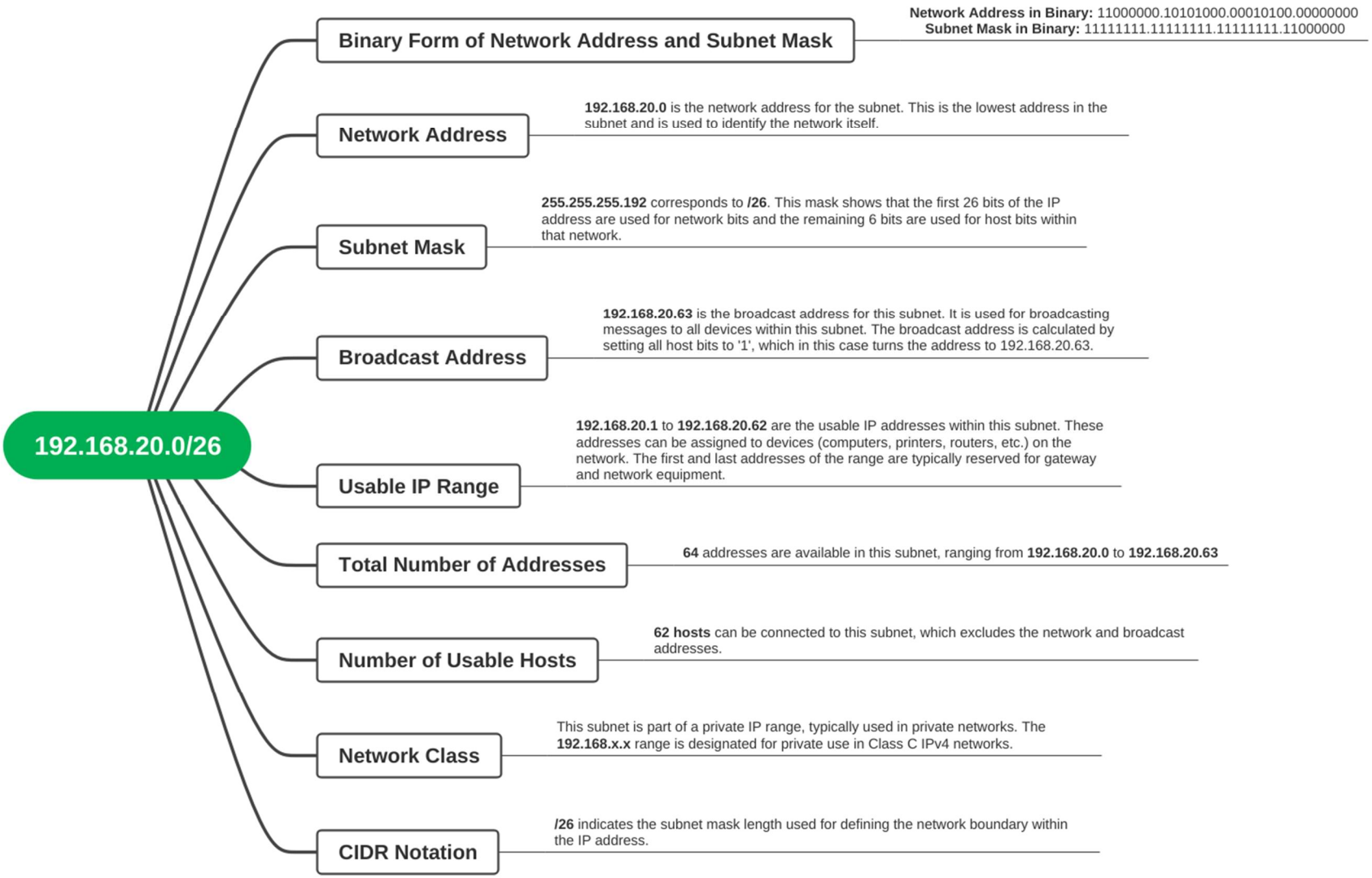

Figure 1.5: Subnetting Overview of 192.168.20.0/26 Address Space

QUESTION 2

Part a: Based on the above statement, provide two remote access methods which could be of support to the robber.

In their paper, Imamura et al. (2007) mentioned that common methods for remote access include Point-to-Point Tunnelling Protocol (PPTP), Layer 2 Tunnelling Protocol (L2TP), IPsec, and Secure Socket Layer (SSL).

Two remote access methods that could potentially be exploited by a cybercriminal for unauthorised access to a bank's network are:

- Secure Socket Layer (SSL) is a commonly used protocol that ensures the security of the connection between a client and a server by encrypting the sent data. This protocol is frequently employed for safe web browsing through HTTPS, which is the encrypted iteration of HTTP.

    - Potential for abuse: An SSL vulnerability can be exploited by a cybercriminal through the establishment of a man-in-the-middle attack. This attack involves the interception and decryption of SSL encryption between a client and a financial institution. By intercepting the communication, they were able to illicitly obtain confidential data, such as login passwords or transaction details, without the need to physically be at the bank

- IPsec, short for Internet Protocol Security, is a network protocol that provides security for Internet Protocol (IP) communications. IPsec is a collection of protocols that are utilised to protect Internet Protocol (IP) connections. It achieves this by verifying the authenticity and encrypting every IP packet within a data stream. It is commonly employed to establish VPNs (Virtual Private Networks), which securely link remote users to an organization's network.

    - Potential for abuse: IPsec could be exploited by cybercriminals to establish unauthorised VPN tunnels within a bank's network architecture. If individuals successfully acquire the required authentication credentials using techniques such as phishing, social

engineering, or brute-force attacks, they can get remote access to the bank's internal network and engage in harmful actions that appear to be legal communications.

Part b: Explain two differences between an IPS and an IDS.

Stalling (2016) explained that intrusion management involves the activities of detecting, preventing, and responding to intrusions. This service primarily focuses on deploying intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) at the entrance points to the cloud and on servers within the cloud. An Intrusion Detection System (IDS) is a collection of automated tools specifically created to identify and flag any unauthorised attempts to gain access to a host system. An Intrusion Prevention System (IPS) combines the features of an Intrusion Detection System (IDS) with additional mechanisms specifically designed to prevent unauthorised network traffic.

Kilic et al. (2019) mentioned that Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) serve as the initial barrier in safeguarding the cyber-environment. This technology is designed to capture and prevent breaches and attacks. Bypassing an Intrusion Prevention System/Intrusion Detection System (IPS/IDS) introduces a significant vulnerability in the field of cybersecurity.

Difference 1:
The purpose of an Intrusion Detection System (IDS) is to passively observe network traffic and produce alerts whenever it identifies potentially malicious behaviour. In contrast, an Intrusion Prevention System (IPS) is specifically designed to proactively block any potentially malicious network data from reaching its intended destination. This could entail completely obstructing the flow of traffic or restoring a link to its original state.

Difference 2:
An Intrusion Detection System (IDS) is a suitable option for systems that necessitate optimal accessibility, such as industrial control systems (ICS) and other essential infrastructure. An Intrusion Detection System (IDS) solely produces notifications without causing any interference to ongoing activities. An Intrusion Prevention System (IPS) is more appropriate for contexts where security is of utmost importance, even if it results in periodic interruptions. An Intrusion Prevention System (IPS) can effectively thwart harmfully network traffic by automatically blocking it, thereby mitigating the risk of possible harm.

Part c: Elaborate on how the two intrusion devises could be of help to the bank.

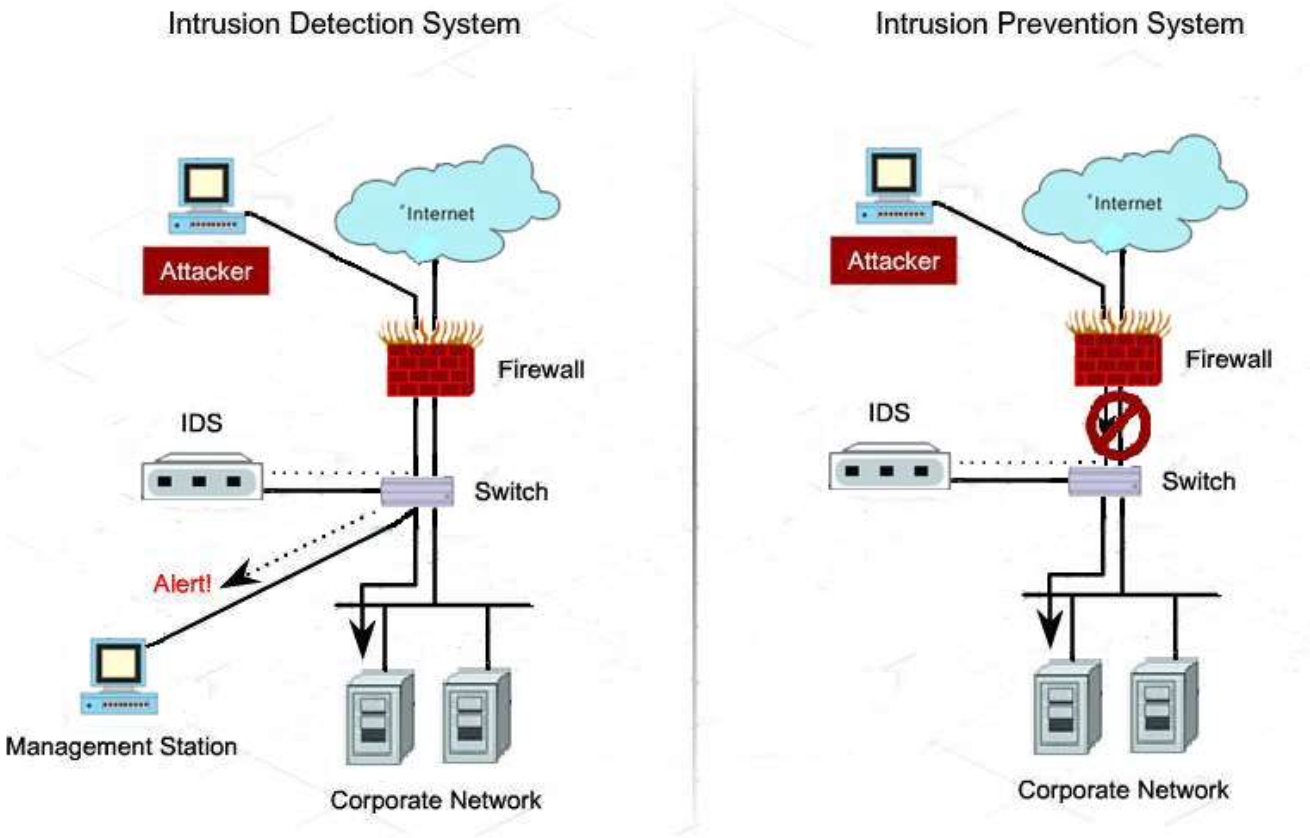

Figure 2.1: Comparison of Intrusion Prevention System and Intrusion Detection System (BoBeni, 2015)

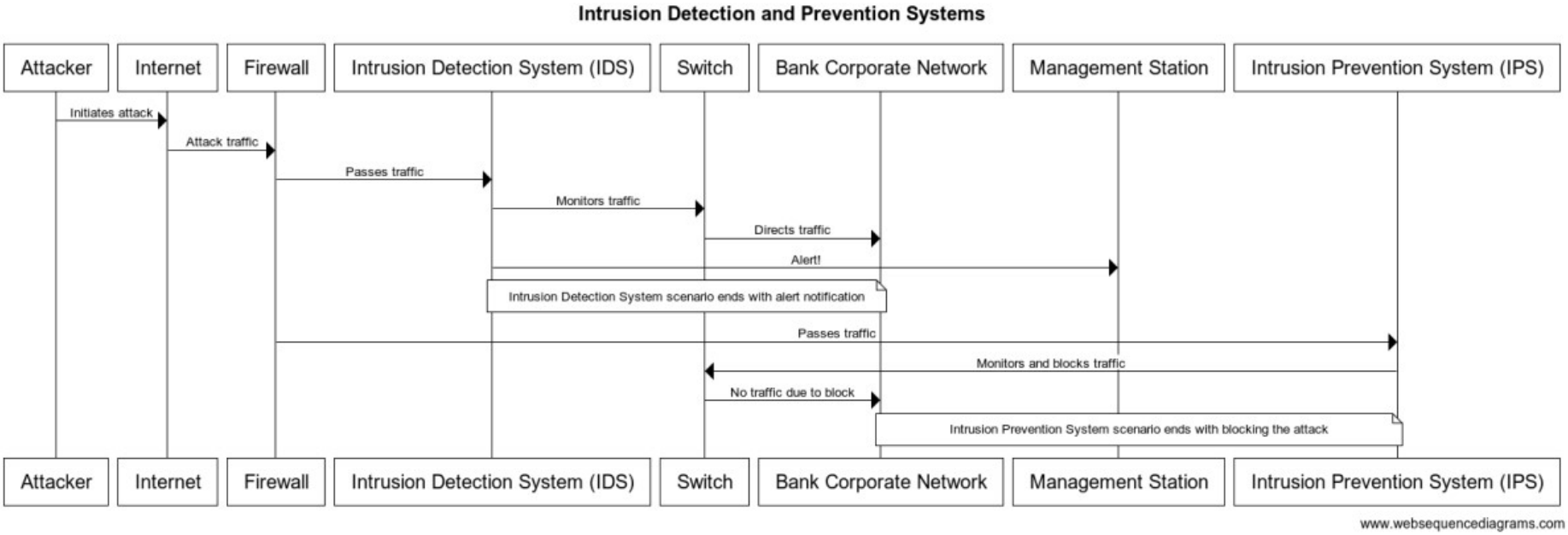

Figure 2.2: Workflow Diagram of Intrusion Detection and Prevention Systems in a Network Security Architecture

Intrusion Detection System (IDS):

- The **Attacker** initiates an attack from their computer, attempting to breach the bank corporate network.
- The attack traffic passes through the **Internet** to reach the target.
- A **Firewall** is the first line of defence, which inspects the incoming traffic.
- The traffic then reaches the **IDS**, which is designed to monitor and analyse the data.
- As the IDS detects malicious activity, it sends an **alert** signal to the **Management Station**.
- The **Switch** in the network infrastructure routes the traffic within the corporate network.
- The **Corporate Network** is the final destination of the internet traffic, potentially affected by the attack.

Intrusion Prevention System (IPS):

- The **Attacker** also initiates an attack in this scenario.
- The attack passes through the **Internet** as in the previous case.
- The **Firewall** again filters the traffic but is integrated with an **IPS**.
- The **IPS** is configured not just to detect but also to prevent the attack by blocking the malicious traffic.
- The **Switch** does not route the attack traffic to the corporate network due to the IPS's intervention.
- The **Corporate Network** remains secure without receiving the attack traffic.
- The **IPS** may send a notification or log the prevention action to the **Management Station**.

In summary, the key difference is that the IDS alerts the management station of an intrusion without actively intervening, whereas the IPS takes direct action to block the intrusion from reaching the corporate network.

Part d: Apart from an IDS and IPS, provide two basic network equipment required to prevent an intruder from attacking your network?

Sawant (2018) concluded after analysing the various IDS/IPS given in Table 2.1, it is evident that each IDS/IPS possesses its own distinct characteristics and limitations. Every IPS/IDS exhibits unique occurrences of false positives, contingent upon the specific network in which they are deployed.

Signature-based intrusion detection systems (IDS) and intrusion prevention systems (IPS) are unable to identify previously unknown vulnerabilities, often known as zero-day vulnerabilities. On the other hand, anomaly-based IPS/IDS systems have a significant number of false positives, meaning they often mistakenly identify normal behaviour as malicious.

IDS/IPS can be deployed in a system to enhance security, depending on its requirements. This can be done in conjunction with other security technologies to ensure optimal protection.

Two fundamental network technologies that are crucial for enhancing network security and preventing attacks, in addition to an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), are:

1. **Firewall**
2. **Router with Security Features**

When these devices are set and updated correctly, they play a crucial role in a layered security strategy to safeguard a network from unauthorised access.

Table 2.1: Comparison of Different IPS/IDS Systems, showing various parameters and their specifications across three different systems (Adapted from Sawant, 2018).

IPS/IDS / Parameters	Trend Micro DSM 10	OSSEC	Snort IDS
Type of IPS/IDS	Host Based	Host Based	Network based
Multiplatform/ Cross Platform	Both	Cross Platform	Multi-platform
Detection Method	Hybrid	Signature based	Signature Based
Additional Hardware Appliance	No	No	No
Integration Support	Yes	Yes	Yes
Max number if Machine supported	20000	~256	NA
Open Source/Proprietary	Proprietary	Open Source	Open Source
Compliance	PCI-DSS,HIPAA	PCI-DSS, HIPAA	PCI-DSS
VE Support	Yes	No	No

Part e: Refer to your answer of d.), provide one feature of each of the networking equipment.

1. **Firewall**
   - A firewall functions as a protective barrier that separates a secure internal network from potentially unsafe external networks. When these devices are set and updated correctly, they play a crucial role in a layered security strategy to safeguard a network from unauthorised access.
   - Manages the flow of network data by enforcing a set of predefined rules for both incoming and outgoing traffic.
   - Creates a defensive shield that oversees and screens network activity, preventing unauthorised entry while permitting authorised communication to proceed.

2. **Router with Security Features**
   - A router equipped with security features is capable of directing network traffic and implementing security protocols.
   - enhanced routers are equipped with built-in security capabilities such as VPN support, enhanced encryption, and traffic filtering.
   - Segmenting a network into multiple subnets allows for the division of important sections of the network, hence minimising the attack surface and enhancing security

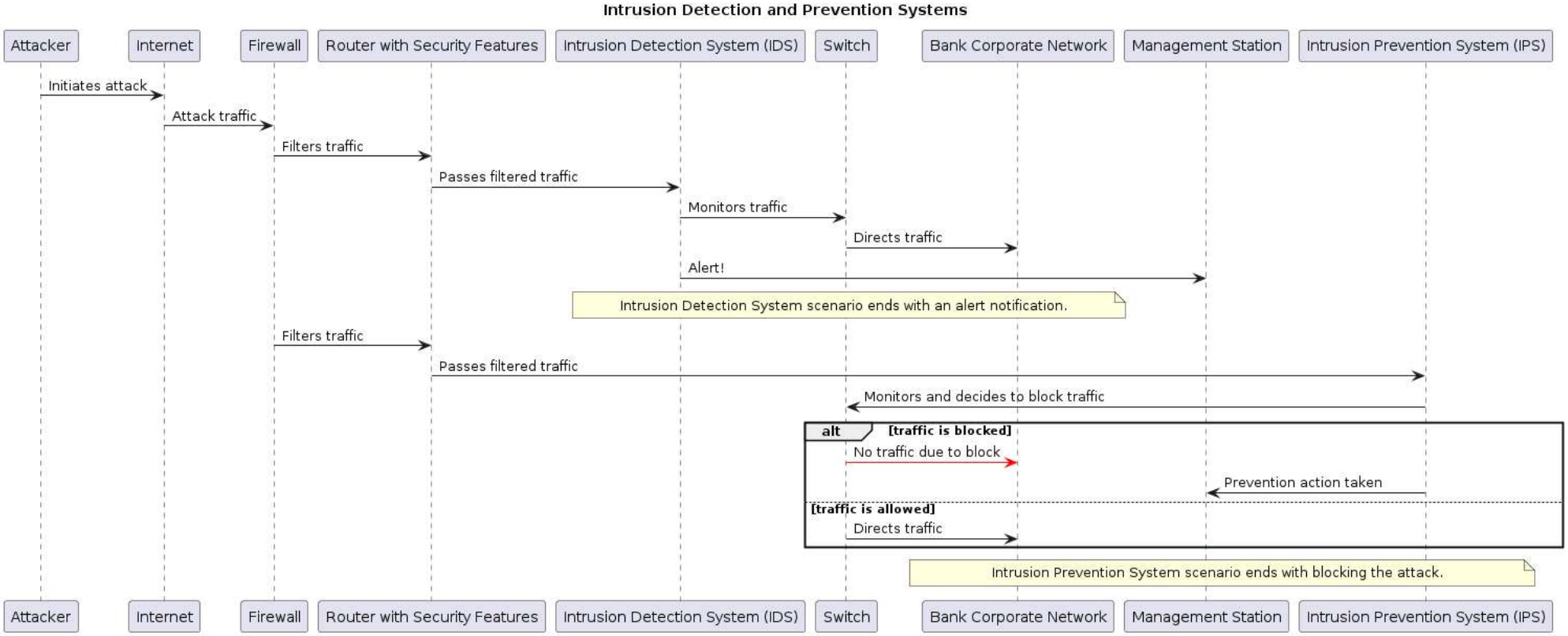

Figure 2.3: Enhanced Network Security Flow with Intrusion Detection and Prevention Systems Including Firewall and Router Security

In summary, within the sequence diagram of **Figure 2.3**, the firewall and the secure router work in tandem to protect the network: the firewall does the initial heavy lifting of filtering incoming traffic from the Internet, and the secure router further refines the security by applying additional policies and directing the traffic to the IDS/IPS for monitoring or blocking. This layered approach to security ensures multiple opportunities to detect and stop potential threats before they can reach the bank corporate network's internal resources.

Part f: Explain how redundancy could support the bank's network infrastructure.

Computer TCP/IP networks are becoming essential in every facet of existence. With the ongoing improvement of computer networks, the levels of redundancy are consistently rising. Contemporary network redundancy features can be intricate and costly. This results in the misconfiguration of the redundancy features. Constantly monitoring every aspect is not always feasible. (Phillips et al., 2020)

Network redundancy is a data loss prevention and dependability investment. When one system, link, or route fails, network redundancy ensures that another may take its place. To backup and fail-over during a network outage, the bank needs extra gear, software, or connections. Network redundancy reduces downtime, which may cost productivity, money, and, in particular businesses, legal issues. Redundant systems and links protect networks and infrastructure against single failures. Even amid network disruptions, network redundancy helps preserve continuity. To satisfy and retain customers, the bank must have redundancy to stay connected and accessible. Businesses may safeguard critical data using redundant networks. Redundant backup solutions may protect vital data against outages and legal and financial penalties (Inseego, 2024)

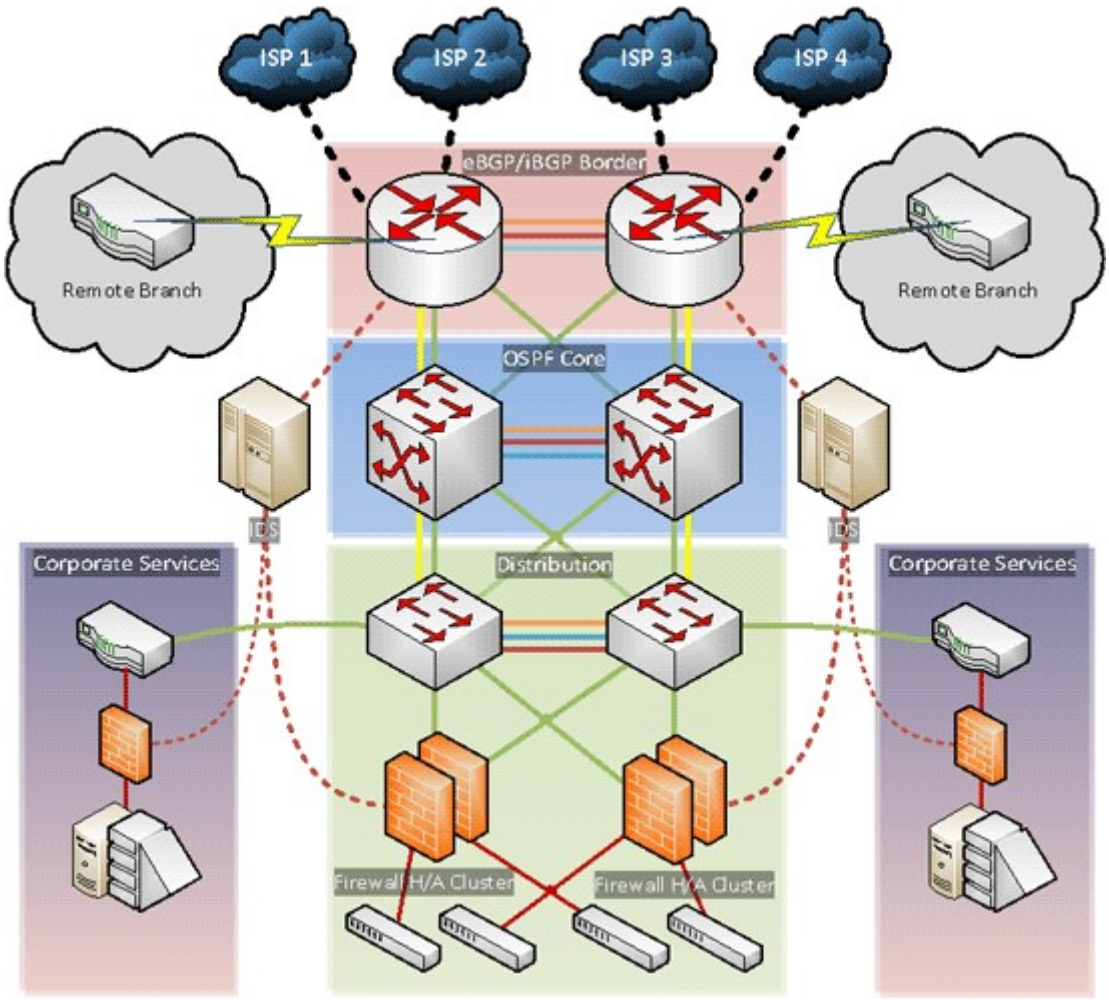

Figure 2.4: Redundant Network Design for network deployment map (Altexxa Group, 2024)

Based on Figure 2.4, it shows how redundancy can support a bank's network infrastructure:

1. Increased Uptime:

- Redundancy involves having multiple copies of critical network components, such as routers, firewalls, servers, and power supplies.
- If a single component fails, another one can take over its function seamlessly, minimizing downtime and ensuring continued network operation.
- This is especially important for critical systems like on-line banking platforms and transaction processing servers.

2. Improved Fault Tolerance:

- Network failures can occur due to hardware malfunctions, software bugs, power outages, or cyberattacks.
- Redundancy enables the network to withstand these failures without significant disruption.
- With redundant components, the network can automatically switch to a backup system in case of a failure, minimizing the impact on ongoing operations.

3. Enhanced Scalability:

- Redundant components can be used to scale the network's capacity to meet increased traffic demands.
- Banks often experience fluctuations in network traffic throughout the day, with peak periods requiring more processing power and bandwidth.
- By adding redundant components, the network can be easily scaled up to handle these surges in traffic volume without compromising performance.

4. Faster Disaster Recovery:

- In case of a major disaster, such as a fire, flood, or natural disaster, redundancy can help the bank recover its network operations quickly.
- By having backup systems located in a geographically separate location, the bank can minimize data loss and restore critical services faster.

5. Improved Security:

- Redundancy can also enhance a bank's security posture.
- By having redundant firewalls and intrusion detection systems, the network is less susceptible to cyberattacks.
- If one security layer is compromised, another redundant layer can still provide some protection and help mitigate the impact of an attack.

Examples of Redundancy in a Bank Network:

- **Dual Power Supplies:** Critical network devices can have redundant power supplies to ensure they continue to operate even if one power supply fails.
- **Redundant Routers and Switches:** Having multiple routers and switches allows traffic to be rerouted automatically in case of a failure on a single device.
- **Mirrored Servers:** Data and applications can be mirrored across multiple servers to ensure continuous service even if one server experiences an issue.
- **Backup Data Centres:** A bank might have a geographically separate backup data centre to ensure critical data and systems are available in case of a disaster at the primary location.

QUESTION 3

Part a: Differentiate between OSI Model and TCP/IP

According to Tanenbaum and Wetherall (2010), there are two significant network architectures that are widely recognised: the OSI reference model and the TCP/IP reference model. The OSI model is depicted in Figure 3.3, excluding the physical medium. This model is derived from a proposal created by the International Standards Organisation (ISO) as an initial effort to standardise the protocols used in different layers. The model is known as the ISO OSI (Open Systems Interconnection) Reference Model because it focuses on connecting open systems, which are systems that can communicate with other systems. According to Kurose and Ross (2013), the OSI reference model consists of seven layers, as depicted in Figure 3.2: application layer, presentation layer, session layer, transport layer, network layer, data link layer, and physical layer. Panek (2020) mentioned that the TCP/IP (or TCP) model bears resemblance to the OSI model. It is commonly utilised by software manufacturers who prioritise the transmission of information over physical media and the establishment of data links. There are only four layers in total.

The OSI model and TCP/IP are fundamental concepts in networking, each with its own distinct purpose:

- **The OSI Model:**
  - The conceptual framework explains the process of exchanging data between various systems, regardless of the technology used.
  - The focus is primarily on the functionality aspect, as it breaks down network communication into seven layers with distinct functions. This breakdown helps in better comprehending the process.
  - It is not a specific protocol suite and does not dictate how data is actually transmitted.
  - However, one advantage is that it is useful for teaching and troubleshooting network issues because of its clear separation of functionalities.

- **TCP/IP:**
  - The functional model describes the protocols utilised in real internet communication.

- It emphasises practical implementation and is structured into four layers that correspond to actual protocols such as TCP and IP.
- A widely used standard is the underlying protocol suite for the internet.
- One advantage of this approach is its practicality and ability to promote seamless communication between various networks.

Below is a table that outlines the main distinctions between the OSI reference model and the TCP/IP reference model.

Table 3.1: Comparison of OSI and TCP/IP Networking Models

Feature	**OSI Model**	**TCP/IP Model**
Type	Conceptual framework	Functional model
Focus	Functionality	Implementation
Number of Layers	7	4
Usage in real world	Not directly used	Widely used standard

To put it more simply, OSI is like a plan for how to communicate over a network, and TCP/IP is the real building that was made from that plan. OSI gives us a way to think about things, and TCP/IP makes that thinking real.

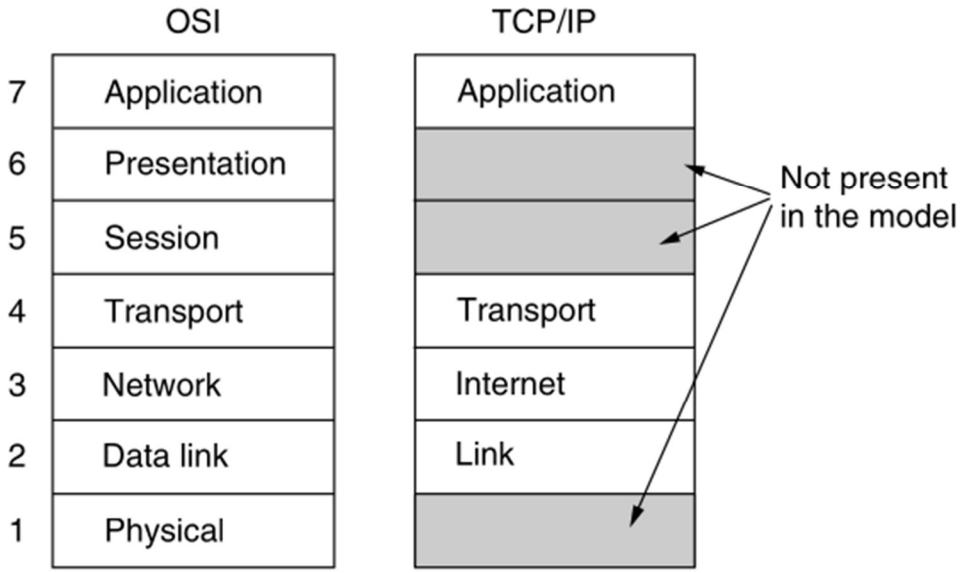

Figure 3.1: The TCP/IP reference model

(Courtesy: Tanenbaum and Wetherall, 2010, p. 46)

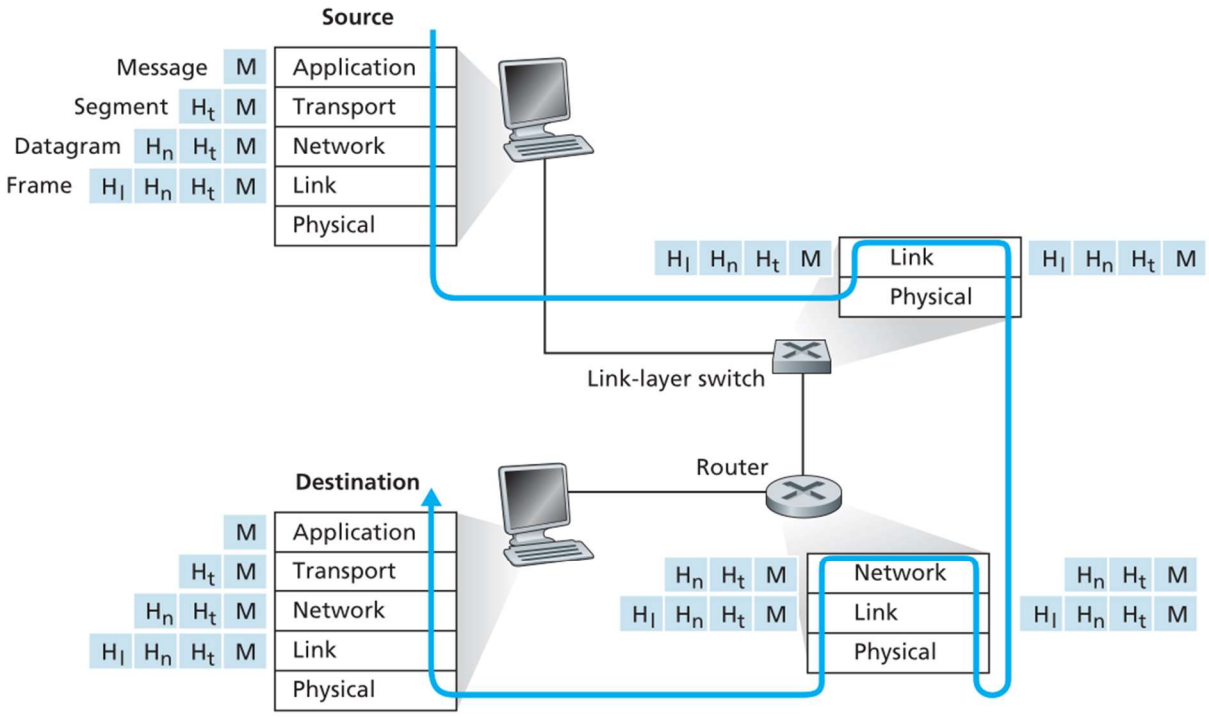

Figure 1.24 ♦ Hosts, routers, and link-layer switches; each contains a different set of layers, reflecting their differences in functionality

Figure 3.2: Encapsulation and De-encapsulation in Network Communication (adapted from Kurose and Ross, 2013, p. 54).

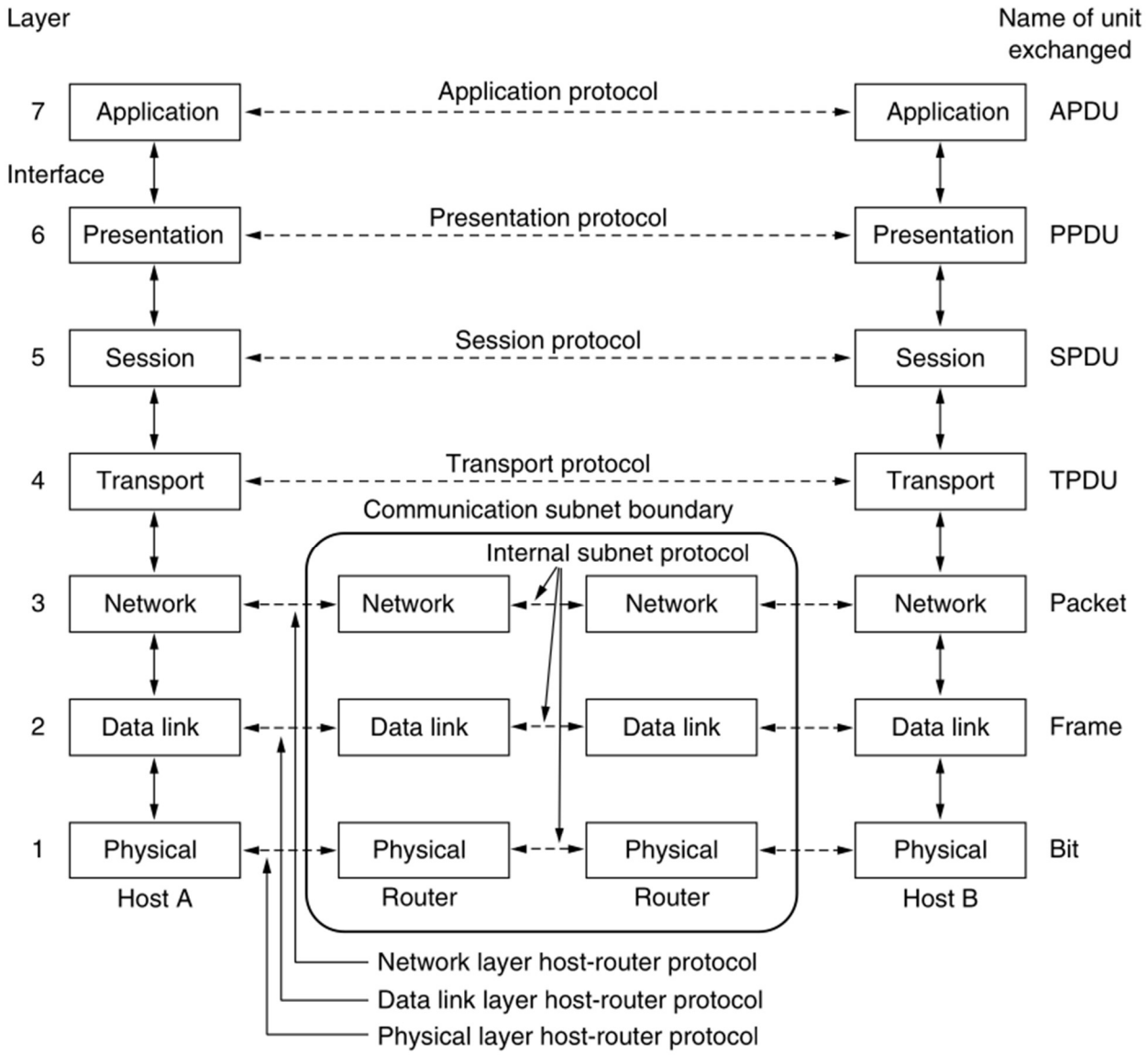

Figure 1-20. The OSI reference model.

Figure 3.3: The OSI Reference Model (adapted from Tanenbaum and Wetherall, 2010, p. 42).

Part b: List down different layers of the OSI Model in their respective orders

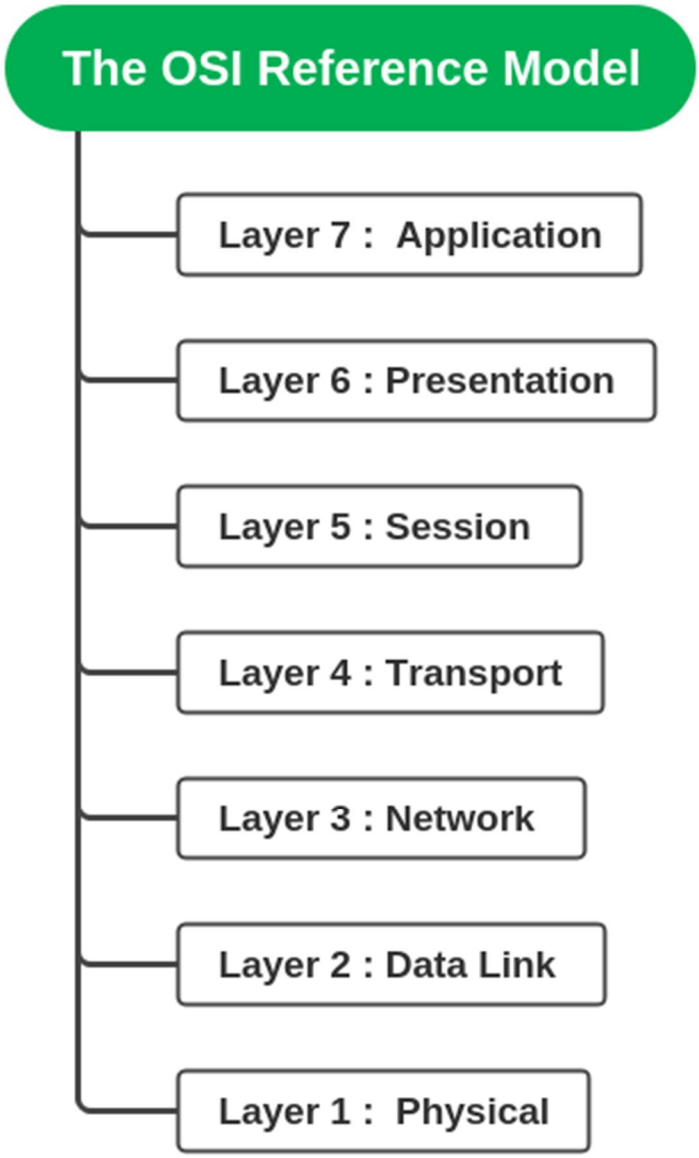

Figure 3.4: The OSI Reference Model

Part c: Explain TCP/IP and provide all layers of the model

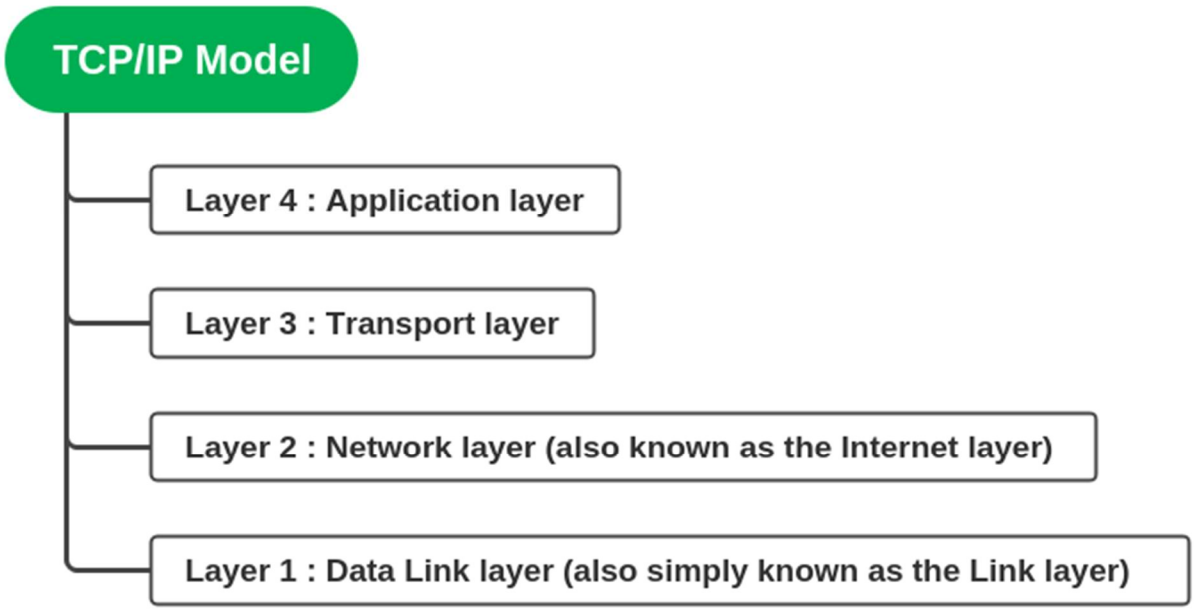

Figure 3.5: TCP/IP model

Panek (2020) stated that the OSI model is a reference model, while the TCP/IP model (also known as the DoD model or Internet model) is more descriptive. It defines principles such as end-to-end and robustness, which emphasise strong endpoint connections and conservative transmission of data. The Internet Engineering Task Force (IETF) is responsible for maintaining it.

TCP/IP is the suite of protocols that govern the transmission of data over the internet. It is the fundamental language that enables countless devices to communicate effortlessly. The TCP/IP model consists of four layers as shown in Figure X, each responsible for a different aspect of data communication:

1. Application Layer:
The top layer of the system directly interacts with the applications we use, such as web browsers, email clients, or online games. Offers network services using protocols such as HTTP for web browsing, FTP for file transfer, SMTP for email, and DNS for domain name resolution. Users typically do not directly engage with this layer, instead they depend on applications that utilise these protocols.

2. Transport Layer:

- Ensuring the dependable transfer of data across various devices and applications. There are two primary protocols:
  - The TCP (Transmission Control Protocol) ensures that data packets are delivered in the correct order by breaking them down, sending acknowledgments, and retransmitting any lost packets.
  - The UDP (User Datagram Protocol) provides a faster and connectionless method of transferring data. It is particularly useful for real-time applications such as video streaming, where maintaining a specific order of data is not crucial.

3. Network Layer:

- Manages the process of directing and transmitting data packets between different networks. The fundamental protocol in this context is IP (Internet Protocol):
  - Assigning unique IP addresses to devices on the network, determining the optimal path for data packets to reach their destination network, and
  - encapsulating data from the transport layer into packets with header information for routing.

4. Network Interface Layer (sometimes merged with Physical Layer):

- The first layer handles the actual transmission of data packets across the network medium, such as cables or WIFI.
- Focuses on the physical aspects of the network, such as cable types, signal encoding, and MAC addresses used to identify devices on the network.
- Network protocols such as Ethernet or Wi-Fi function at this particular layer.

Through collaboration, these layers ensure the reliable packaging, addressing, routing, and delivery of data across networks, establishing the fundamental basis for internet communication.

Part d: Network troubleshooting is a complex task. Describe any three of the following utilities and explain how they may be useful for first level troubleshooting.

1) ipconfig

This handy tool provides with all the essential details about a network setup. It reveals important information like the computer's IP address, subnet mask, default gateway, and DNS server addresses.

Practicality:

- Understanding an IP address is essential for a range of network-related tasks, such as accessing shared drives or adjusting network configurations.
- It is important to check the subnet mask and default gateway to ensure proper configuration for communication with other devices on your local network.
- Understanding DNS server addresses is crucial for converting website names into IP addresses. Having incorrect DNS settings can cause problems with accessing websites.

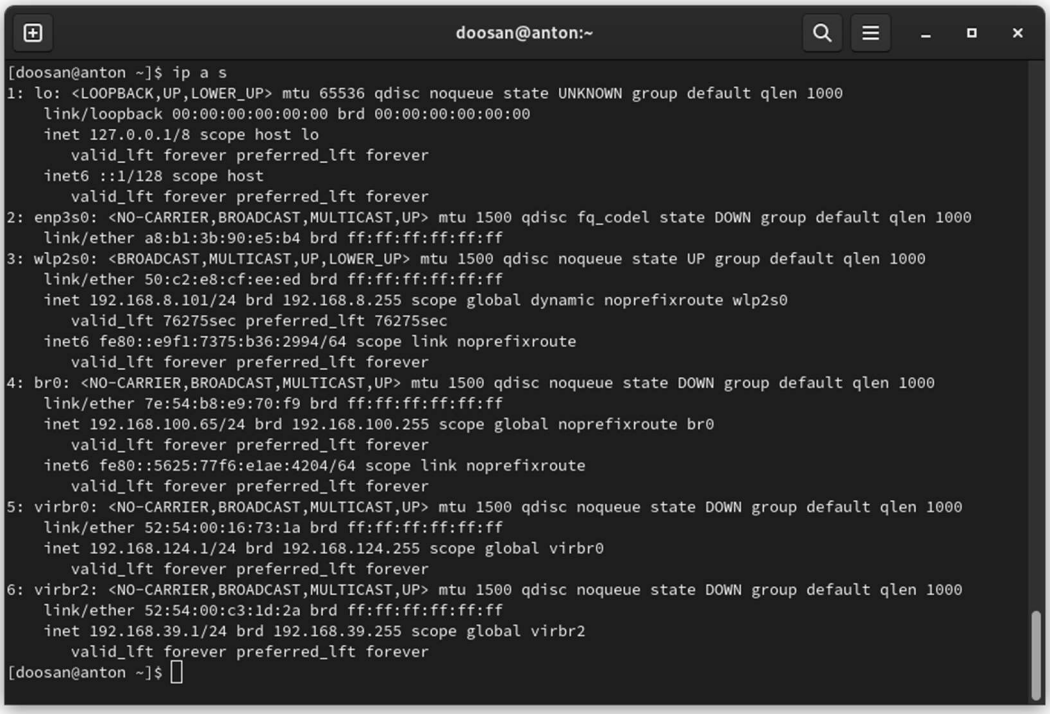

Figure 3.6: Terminal Output of Network Interface Configuration Command

2) PING

This tool is commonly used to check the basic connectivity between a computer and another device on the network, such as a website or another computer. It is an essential tool for network troubleshooting.

Practicality:

- It sends echo request packets to the target device and patiently waits for a response.
- If a ping is successful, it means that the device is reachable and responding. However, if there is no response, it could indicate a connectivity issue along the path.
- Additionally, Ping has the capability to measure the round-trip time (RTT) for packets, which can be useful in identifying possible slowdowns or latency problems.

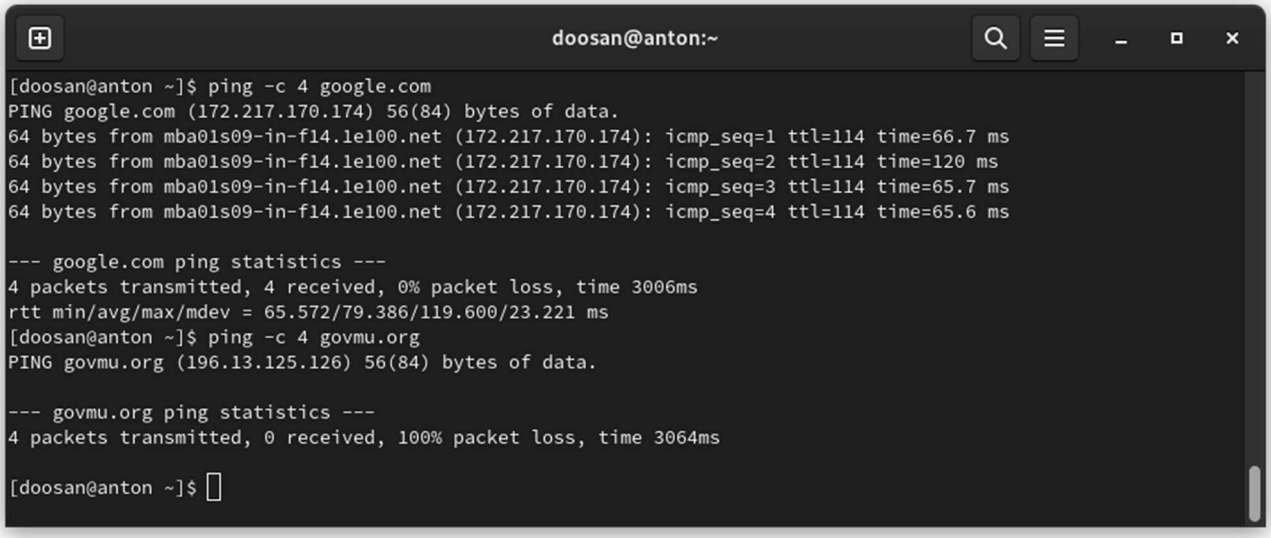

Figure 3.7: Terminal Output Showing Ping Command Results for Connectivity Test

3) traceroute (or tracert on Windows)

This tool is designed to provide a visual representation of the route that data packets follow in order to reach a particular destination on the internet.

Practicality:

- Traceroute provides a comprehensive overview of the network path that packets take to reach their destination.
- Through the identification of communication breakdowns, such as a lack of response from a specific hop, it becomes possible to determine the potential location of a network issue. This could be within your local network, your ISP, or further along the internet backbone.
- This is a useful tool for troubleshooting connectivity issues that extend beyond an immediate network.

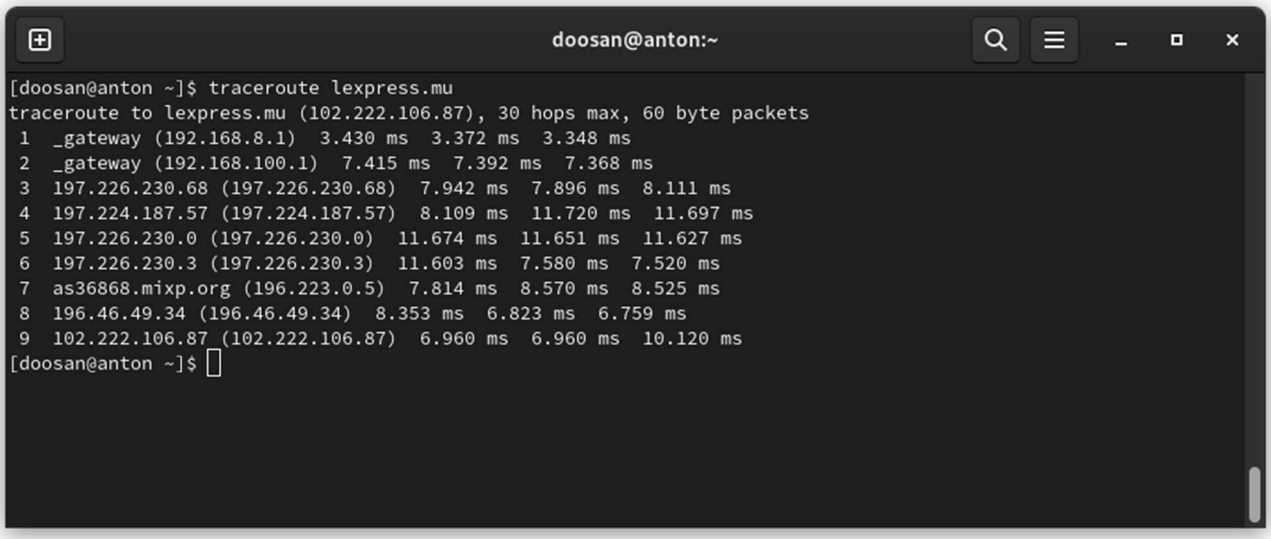

Figure 3.8: Network Path and Latency Analysis Using Traceroute Command

4) netstat

Netstat is a handy command-line tool that provides valuable information about a network connection. It gives details such as:

- Current TCP and UDP connections, both listening and established
- Details of the connection include both local and foreign IP addresses and ports.
- The status of the connection (e.g., established, listening, waiting)
- Occasionally, the connection requires additional flags to associate it with the process ID (PID)

Practicality:

Netstat is a useful tool for identifying the active connections that someone's computer has established with other devices or servers.

It is possible to identify the programmes that are utilising your network and the specific ports they are using for communication.

This information may prove beneficial for:

- Identifying and investigating potentially suspicious activity or malware that could be causing abnormal connections.
- Identifying programmes that may be using up a lot of bandwidth.
- Investigating connection problems with certain services by verifying the establishment of the connection and confirming the correct port.

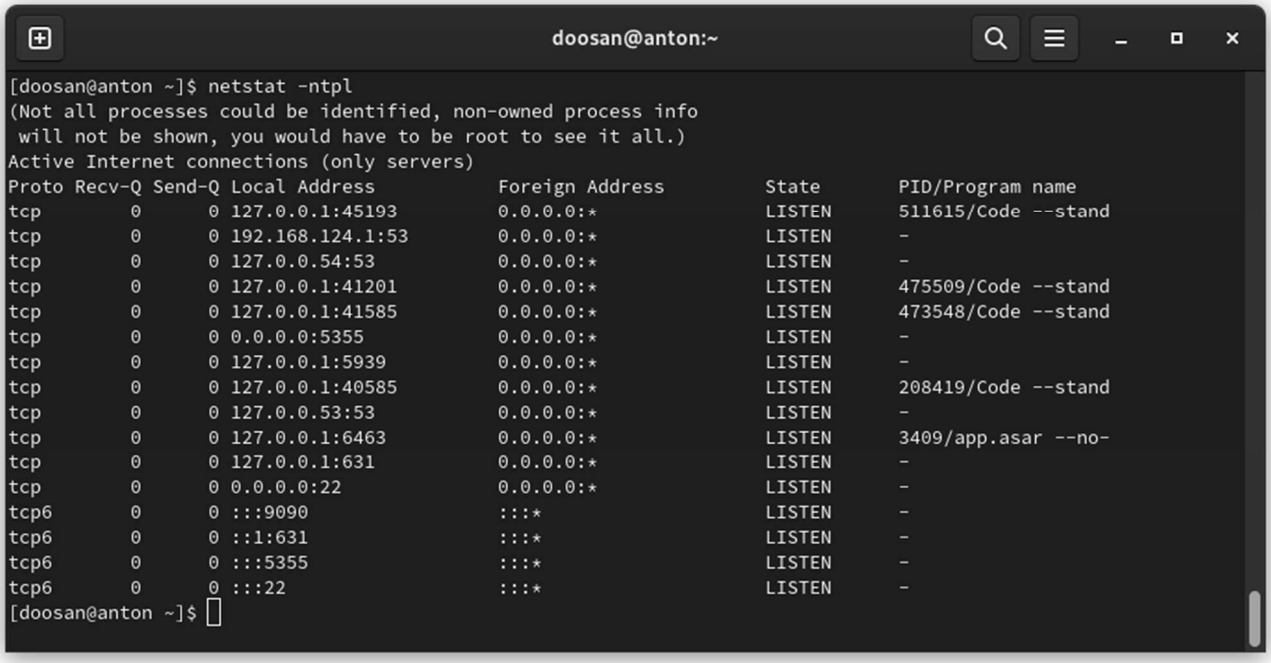

Figure 3.9: Output of the Netstat Command Showing Active TCP Connections

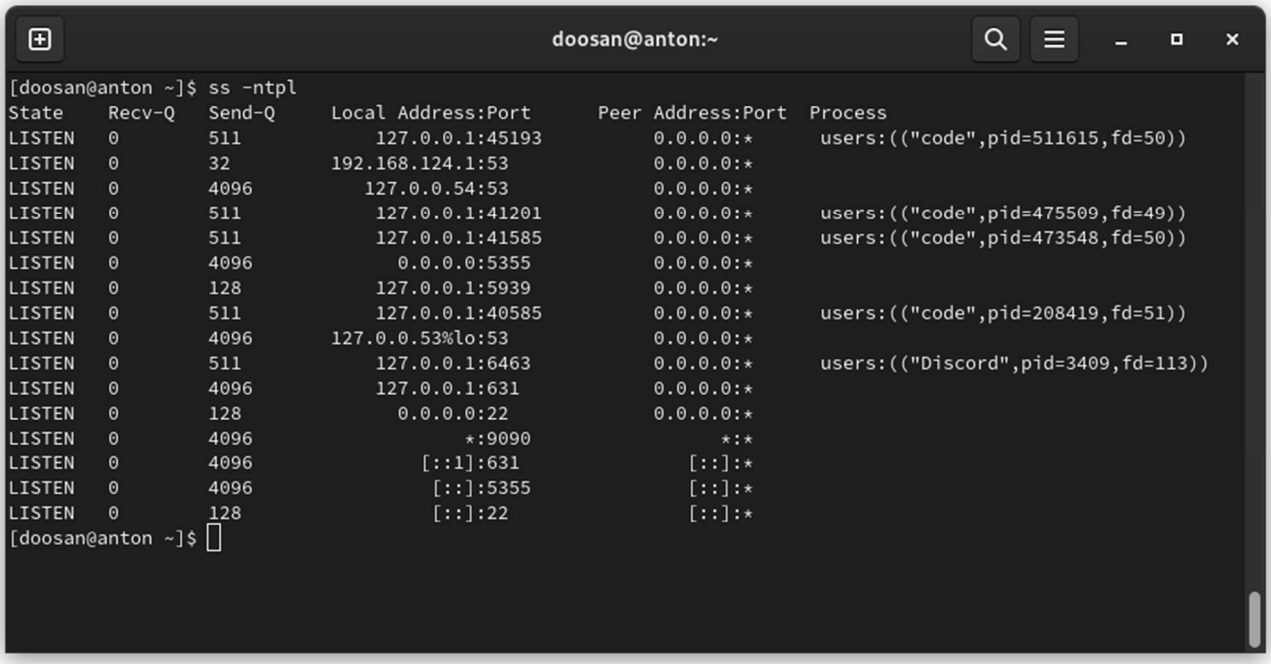

Figure 3.10: Detailed Netstat Command Output with Process Identification Information

REFERENCES

1) Altexxa Group. (2024) *Redundant Network Design*. [Online image]. Available at: https://altexxa.com/networks/redundant/ (Accessed: 18 April 2024).

2) BoBeni. (2015) *Ips vs ids*. [Online image]. Available at: https://commons.wikimedia.org/wiki/File:Ips-vs-ids.png (Accessed: 18 April 2024).

3) Crystal Panek, "Defining Networks with the OSI Model," in *Networking Fundamentals,* Wiley, 2020, pp.43-73, doi: 10.1002/9781119650768.ch2.

4) Imamura, K., Suzuki, H. and Watanabe, A. (2007) 'A proposal for a remote access method using GSCIP and IPsec', *TENCON 2007 - 2007 IEEE Region 10 Conference* [Preprint]. doi:10.1109/tencon.2007.4428854.

5) Inseego (2024) *Maximize business continuity with network redundancy*, *Inseego*. Available at: https://inseego.com/resources/blog/network-redundancy-is-crucial-to-business-success/ (Accessed: 18 April 2024).

6) Kilic, H., Katal, N.S. and Selcuk, A.A. (2019) 'Evasion techniques efficiency over the IPS/IDS Technology', *2019 4th International Conference on Computer Science and Engineering (UBMK)* [Preprint]. doi:10.1109/ubmk.2019.8907177.

7) Kurose, J.F. and Ross, K.W. (2013) *Computer networking: A top-down approach*. Boston: Pearson.

8) Liu, D. (2009). *Cisco CCNA/CCENT exam 640-802, 640-822, 640-816 preparation kit*. Burlington, Mass.: Syngress Pub.

9) Moskowitz, R. *et al.* (1996) *RFC 1918: Address allocation for private internets*, *IETF Datatracker*. Available at: https://datatracker.ietf.org/doc/html/rfc1918 (Accessed: 14 April 2024).

10) Phillips, R., Jenab, K. and Moslehpour, S. (2020) 'A practical approach to monitoring network redundancy', *International Journal of Data and Network Science*, pp. 255–262. doi:10.5267/j.ijdns.2019.9.004.

11) Rekhter, Y. and Li, T. (1993) *RFC 1518: An architecture for IP address allocation with CIDR*, *IETF Datatracker*. Available at: https://datatracker.ietf.org/doc/html/rfc1518 (Accessed: 14 April 2024).

12) Rooney, T. (2011). *Introduction to IP Address Management*. John Wiley & Sons.

13) Sawant, A. (2018) 'A comparative study of different Intrusion Prevention Systems', *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)* [Preprint]. doi:10.1109/iccubea.2018.8697500.

14) Stallings, W. (2011). *Cryptography and network security: principles and practice*. Boston; Montreal: Prentice Hall.

15) Tanenbaum, A.S. and Wetherall, D. (2010). *Computer Networks, Fifth Edition*. Prentice Hall.