Table of Contents

PART-A

PART-B

PART- A

ABSTRACT:

This document covers the TCP/IP layered architecture in-depth, providing detailed insights into the functioning of each layer. It also contrasts the TCP/IP and OSI models. Furthermore, the document delves into the design considerations and protocols unique to each TCP architecture layer.

INTRODUCTION:

The TCP model will have 4 layers; they are the Link, Internet, Transport and Application layer. These layers represent a structure that controls the internet and how it will be set up and function. There will be some differences if we compare it with the OSI model. This report will tell us about the detailed structure of the TCP, design issues and protocols for each layer of the TCP. The report also shows the SDN in the TCP architecture, describing its effects on every layer of the TCP.

TCP/IP LAYERED ARCHITECTURE:

The TCP model is a four-layer architecture that divides network communication into four categories. This model requires protocols for several tasks and creates a framework for data transmission between the devices.

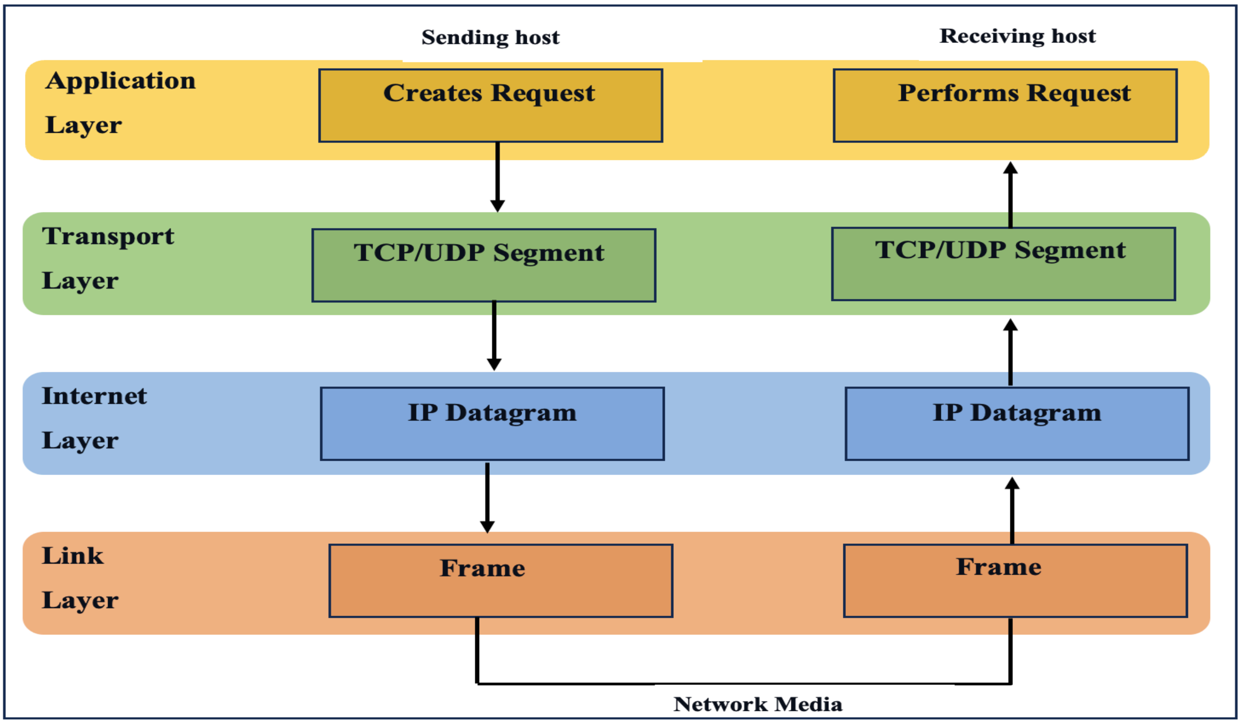


Fig 1: Data transmission through layers (Gicheha, 2023)

Application Layer

Description: The application layer is the topmost layer in the architecture; this layer is just above the transport layer. The application layer verifies that the application is compatible with other applications running on various networks and devices. **(Kirvan, 2022)**

Protocols: FTP, HTTP, Telnet, DNS, SMTP etc.

Functionality: As the applications give users the ability to create and receive data that can be transported on the network, An interface to that network is provided by the application layer. This layer serves as an interface for messages travelling over the underlying network to and from the applications we use for communication.

Transport Layer

Description: This is the third layer in the TCP model; it is in charge of checking that data packets between the sender and the recipient arrive correctly and consistently.

Protocols: TCP, UDP

Functionality:Transport layer establishes an Error-Free Data connection and splits the data into tiny packets, Moreover obtains acknowledgement of the reception of the packets.In simple words, this layer shows the service level and the status of the connection while transferring the data. (inflobox, 2024). Some protocols are depend on the connection, that means this layer can check the segments and transmits again those which fails; moreover, it provides acknowledgement for successful transmission.

Internet Layer:

Description: The second layer in this architecture which will be in between the Link and Transport. This layer is responsible for providing the internetworking. And moving the packets from sorce to destination.

Protocols: IP, ICMP(Internet Control Message Protocol).

Functionality: The functionalities of Internet layer includes sending the packets, checking that the packets are sent correctly as well as routes the data to the correct network. Provivions the logical addressing as well as routing of data packets using Internet protocol such as IPv4 are the additional functionalities of this layer.

Link Layer

Description: This layer Is the lowest in the TCP model; the primary responsibility of this layer is to show how the machine communicates to the network. This could use various network topologies for communication, such as Ethernet, FDDI etc,

Protocols: Ethernet, ARP(Address Resolution Protocol), PPP(Point to Point Protocol).

Functionality: This layer adds the destination Mac address, and send the data between applications over the network by handling the physical infrastructure.It works with physical media’s error detection, hardware addressing and access control.

COMPARISON AND KEY DIFFERENCE BETWEEN TCP/IP AND OSI MODEL:

OSI	TCP
Application Layer Details how application programs interface to the network and deliver services to them	**Application Layer** TCP network applications must handle the OSI presentation layer and some of its session layers themselves.
Presentation Layer Specify the data representation for the applications.	
Session Layer Create, manage and terminate network connections.	
Transport Layer Handles error handling and controlling the sequence of data moving through the network.	**Transport Layer** Manages all data routing and delivery aspects, including session, error handling and serialisation.
Network Layer Responsible for specifying, routing data and managing communications.	**Network Layer** Responsible for data processing, transmission and packet segmentation and reassembly.
Data Link Layer Defines access methods for the physical medium.	**Network Interface Layer** Defines the methods for sending data over the network, including access to the physical medium.
Physical Layer Defines the physical and procedural operational characteristics of a physical device.	

Fig 2: Comparison between TCP and OSI

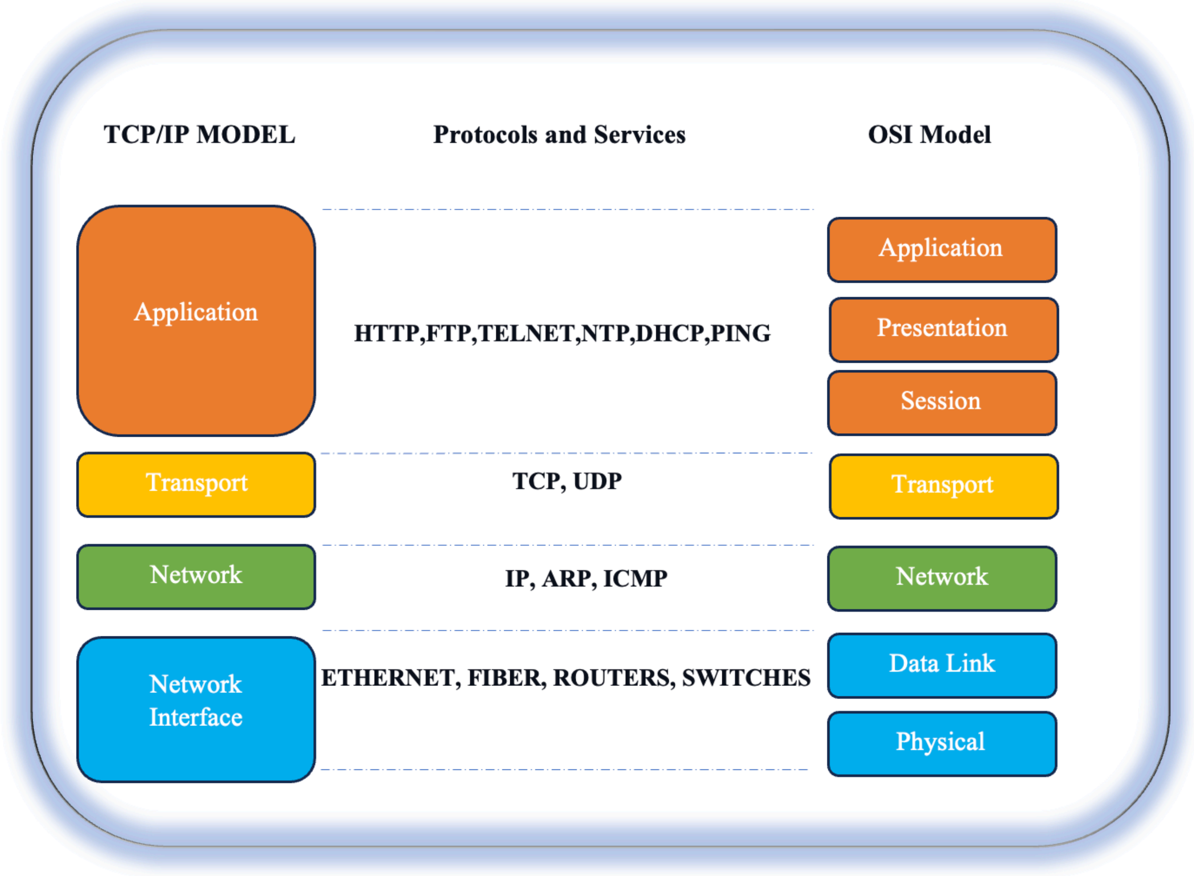


Fig 3: Difference of TCP and OSI

DESIGN ISSUES:

Application Layer:

Providing various application-specific services, ensuring secure data transmission and implementing network-specific protocols are essential considerations.

Transport Layer:

The main concerns are confirming reliable data transmission, congestion control, flow control and error control.

Internet Layer:

The main issues at this layer are routing, packet forwarding, IP communication and handling segmented messages.

Link Layer:

This layer is essential to address device-specific information, access control, and debugging.

DESIGN ISSUES FOR THE LAYERS OF COMPUTER NETWORKS:

• Addressing: IP addresses (IPv4, IPv6) are used for routing.
• Error Management: ICMP handles diagnostics and error reporting.
• Reliability: TCP offers dependable, error-checked and ordered byte stream communication.
• Efficient: UDP offers a faster, less dependable connectionless communication mechanism than TCP.
• Communication: Ethernet and similar link layer technologies are used to offer local area network communication.

PROTOCOLS

Application Layer:

1. **HTTP**: Hypertext Transfer Protocol is designed for transferring of information between the network devices and runs on top of the other layers of that stack of network protocols. **(Chari, 2003)**
2. **Telnet**: The Telnet Protocol is a standard technique for connecting terminal devices and terminal-oriented processes.
3. **FTP**: FTP stands for File transfer protocol. File transfers are done via the FTP, which has special features that enable communication in the digital world and allow communication across programs.

Transport layer:

1. **TCP:** Through the creation and maintenance of a virtual circuit between the sender and recipient, TCP supports reliable communication and guarantees error-free data transmission.
2. **UDP:** Although UDP does not confirm data integrity, it offers a straightforward connectionless connection that is proper for applications that desire low latency and light burden. These techniques dispense data across several networks.

Internet layer:

1. **IP:** The Internet Protocol is the major protocol of the Internet. It allows everyone to transmit information from all directions of the world at lightning speed. For instance, when we send data through email or browse a website, etc, our devices communicate with servers and devices across the world using this protocol.
2. **ICMP:** Internet control message protocol solves the reporting problem. However, IPv4 and IPv6 are the most extensively used address storage protocols. This is a network-level protocol that communicates information about network connection issues back to the source of the weakened transmission. ICMP is mainly used in routers to communicate with the source of a data packet for transmission issues. **(GeeksforGeeks, Internet Control Message Protocol (ICMP), 2023)**

Link layer:

1. **PPP:** A link layer communication technique called point to point establishes a direct connection between two network devices at that layer. WAN technology is usually utilised to establish connections between distant networks and the internet. Numerous

features, including encryption, error correction, and flexibility, are present in this protocol.

2. **Ethernet**: The common link layer technology used in wired networks is Ethernet. Ethernet protocol is a typical LAN technology. In local networks, these protocols guarantee error-free and effective data transmission as well as a secure transmission connection.

SOFTWARE-DEFINED NETWORKING (SDN)

SDN stands for Software Defined Network, which is an approach to networking architecture. It allows for monitoring and managing the network using software applications. There will be two planes in the architecture. They are

1. **Data plane:** This plane includes all functions that are linked and derived from data packages provided by the end user. **(GeeksforGeeks, Software defined Networking(SDN), 2023)** This comprises:
    - Data segmentation and aggregation.
    - Replication of packets for multicasts
    - Packet Forwarding

2. **Control plane:** This is also known as the brain of the network. All functions required to implement the data layer functions but not related to end-user data packets belongs to this plane. The control plane’s tasks consist of the following:
    - Making routing tables
    - Specifying packet handling policies.

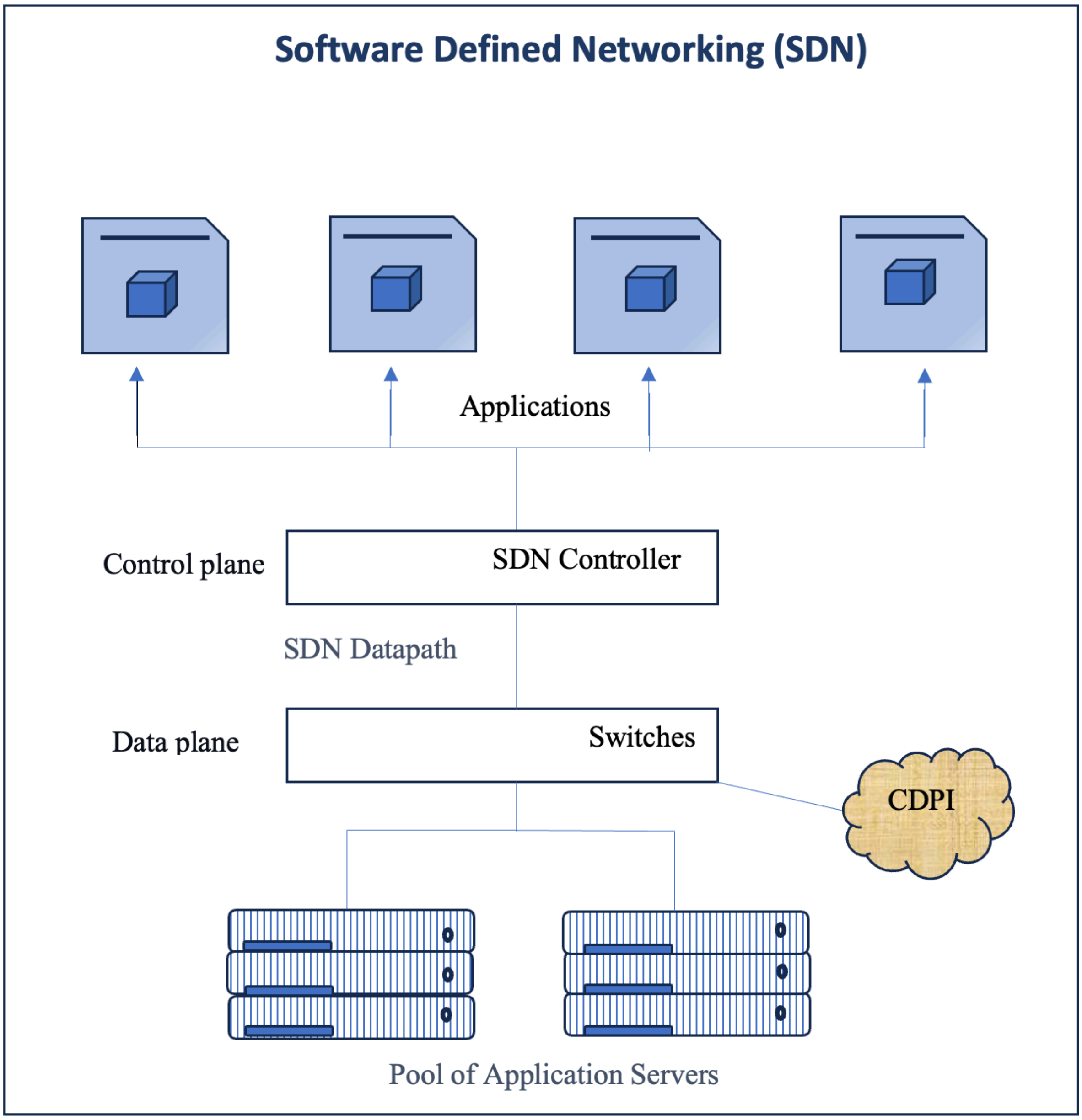


Fig 4: Software Defined Networking (GeeksforGeeks, Software defined Networking(SDN) , 2023)

The SDN architecture has 3 layers, they are

Application layer: This layer has typical network applications such as firewalls and load balancing.

Control layer: It has the SDN controller which acts as the brain of the network.
Infrastructure layer: Its hardware switches carry out the actual data packet movement and create the data plane. **(De, 2023)**

These layers communicate with the help of interfaces called north-bound APIs – a protocol that enables communication between lower level network, higher level network and southbound APIs- permits higher level components to send commands to lower level.

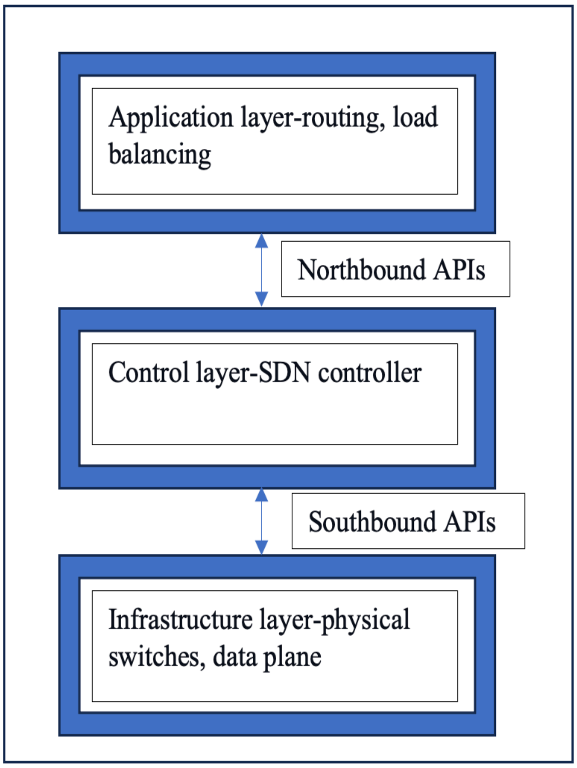

Application layer-routing, load balancing
Northbound APIs
Control layer-SDN controller
Southbound APIs
Infrastructure layer-physical switches, data plane

Fig 5: SDN architecture (drpankajdadhich, 2022)

SDN AND ITS IMPACT ON TCP/IP LAYERS :

Software-defined networking uses a programmable network management technique to replace various TCP layers.

- **Application layer:** Using programmable boundaries, SDN provides application designers with active control over network behaviour.
- **Transport layer:** SDN controllers can carry out blocking, develop traffic flow or execute network-wide policies.
- **Internet layer:** SDN can focus on routing decisions and make adjustments based on policies.
- **Link layer:** SDN technologies have the power to transform how the devices connect, configure and communicate within a physical network.

IMPLICATIONS ON NETWORK DESIGN AND MANAGEMENT:

Agility and Flexibility: By modifying network behaviours, SDN enables agile network management.

Centralised Control: SDN's centralised control streamlines network management and also enhances security by enforcing policies at all times.

Complexity: SDN implementation demands a departure from conventional network concepts and these adjustments are not without difficulty.

SDN first modifies the network topology and impacts TCP layer performance, boosting flexibility and enhancing injection control and design. Network architecture and performance both benefit from this.

SDN WITH TCP FRAMEWORK

The essential elements of today's network systems are TCP and SDN frameworks operating across several layers of network architecture. Following a careful analysis of these connections, the following connections are discovered:

SDN is an method for an architecture of networks that divides the planes like data and control. In simple terms an organised controller integrates control and programming ability and the abstract underlying hardware permits the network to be designed constantly.

SDN overview: SDN is a network architectural paradigm that divides the data and control planes. A conceptually centralised controller unifies programmability and control while abstracting the underlying hardware to enable dynamic network setup.

TCP framework: TCP serves as a dependable connection-oriented transport layer protocol in the TCP model. Its essential functions are ensuring data dependability and integrity, ordering delivery between devices, and managing complete connection and data transmission.

PART- B

Scenario:

As a junior network engineer, you have been assigned to create and subnet a network for the recently constructed UCB Camdon House building labs. The network will serve four labs, each varying sizes-four labs with 20, 24, 12, and 14 PCs, respectively. The PCs are connected to switches at each lab. For each lab to service the network as a whole, a router is needed. A virtualised PC running at least two operating systems (Windows, Active Directory, or Linux) is also required for each lab to facilitate the use of lab sessions for the construction and illustration of virtual networks.

1. Make the Design:

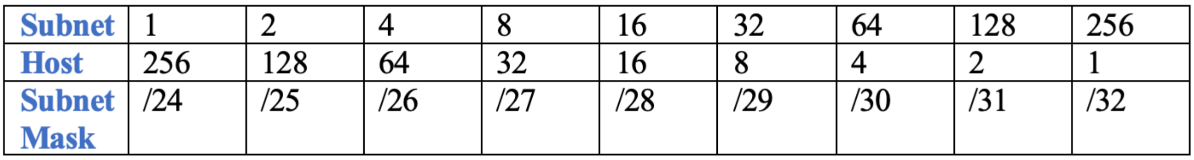
Subnetting:

- A subnet is the logical division of an IP network. Dividing a network into two or more networks is called subnetting.
- The main objectives of subnetting are to improve overall network performance and lessen network congestion. **(Hatim, n.d.)**

1.1 Computations on the number and type of subnets require:

According to our assignment, we require four subnets, which we can label Lab1 (20 PCs), Lab2 (24 PCs), Lab 3 (12 PCs), and Lab 4 (14 PCs). And we should be able to verify that they are all connected to the same network.

Subnetting Table:



Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

Fig 6: Subnetting Table

The table above illustrates subnetting; it indicates the number of hosts required for each subnet as well as the subnet mask needed for the subnet in use.

1.2 An estimate of the number of hosts per subnet that the network can provide :

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

According to the assignment, we also require four subnetworks, which are indicated in the table above by the highlighted areas. Each subnet will have 64 hosts, and its subnet mask will be /26.

I chose 193.168.1.0 as the Original network ID which belongs to Class-C, and the table that follows lists the host id ranges for each subnet along with the total number of viable hosts for each subnet. Furthermore, the last network id of that subnet, 193.168.1.63, can be used as the broadcast id and we cannot use that id for the component IP address. The initial network id, 193.168.1.0, will be considered as the network id of that subnet and cannot be used for the component IP address. Every subnet I chose will experience the same outcome. 62 hosts are so present in each subnet.

Network ID	Subnet Mask	Host ID Range	Number of Usable Host	Broadcast ID
193.168.1.0	**/26**	**193.168.1.1- 193.168.1.62**	**62**	**192.168.1.63**
193.168.1.64	**/26**	**193.168.1.65- 193.168.1.126**	**62**	**192.168.1.127**
193.168.1.128	**/26**	**193.168.1.129- 193.168.1.190**	**62**	**192.168.1.191**
193.168.1.192	**/26**	**193.168.1.193- 193.168.1.254**	**62**	**192.168.1.255**

1.3 Network device IP address assignment:

Since there are four subnets, I'm going to employ IP addresses ranging from 193.168.1.0 to 193.168.1.63, for the first subnet, as stated in the table. As previously stated, the first id will be the network id of that subnet, and the second IP address of that same series, 193.168.1.1, will be used as the router IP address and will be deemed the default gateway for that first subnet, Lab1. The third IP address in that series, 193.168.1.2, will be used as the IP address for the server in that subnet. Finally, the remaining IP addresses for the components will be assigned. The same will be done for the remaining subnets, which are Lab 2, Lab 3, and Lab 4.

Lab	Components start IP Address	Router IP	Server IP
Lab-1	193.168.1.3	193.168.1.1	193.168.1.2
Lab -2	193.168.1.67	193.168.1.65	193.168.1.66
Lab -3	193.168.1.131	193.168.1.129	193.168.1.130
Lab -4	193.168.1.195	193.168.1.193	193.168.1.194

I employed DHCP service in the current network design as it is a feasible solution. DHCP service assigns IP addresses to the end user devices which reduces human interaction to assign IP addresses manually. We can assign static IP addresses manually to the end users devices but it will become more complicate as the network grows and which will takes lot of time to assign manually. To overcome this issue i utilised DHCP.

Types of Interfaces or ports on networking devices:

In networking, the abbreviations "gig" and "se" are frequently used to refer to distinct types of ports on routers or other networking devices:

Gigabit Ethernet (Gig): Gig are network interfaces or ports that support Gigabit Ethernet speeds.
Fast Ethernet (SE): Fast Ethernet can achieve speeds of up to 100 Mbps, which is significantly quicker than standard Ethernet 10 Mbps.

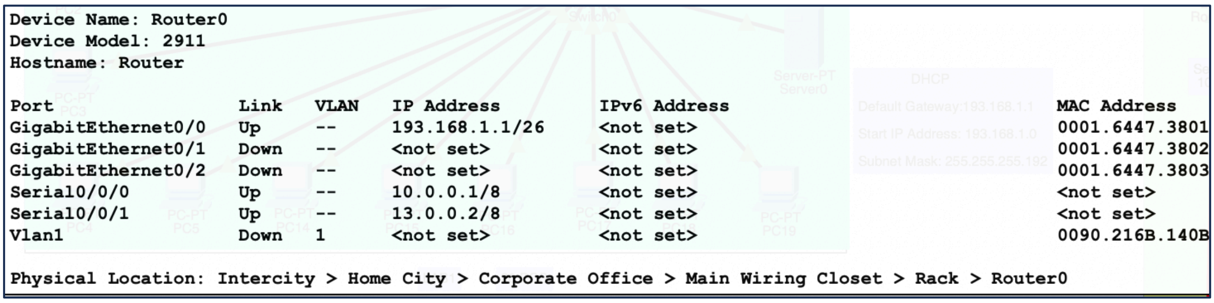
The interface configurations of Router-0, Router-1, Router-2,and Router-3 are :

For Router-0 :

Gig0/0: 193.168.1.1

Se0/0/0 : 10.0.0.1

Se0/0/1 : 13.0.0.2



```
Device Name: Router0
Device Model: 2911
Hostname: Router

Port                  Link   VLAN   IP Address        IPv6 Address                       MAC Address
GigabitEthernet0/0    Up     --     193.168.1.1/26    <not set>                          0001.6447.3801
GigabitEthernet0/1    Down   --     <not set>         <not set>                          0001.6447.3802
GigabitEthernet0/2    Down   --     <not set>         <not set>                          0001.6447.3803
Serial0/0/0           Up     --     10.0.0.1/8        <not set>                          <not set>
Serial0/0/1           Up     --     13.0.0.2/8        <not set>                          <not set>
Vlan1                 Down   1      <not set>         <not set>                          0090.216B.140B

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router0
```

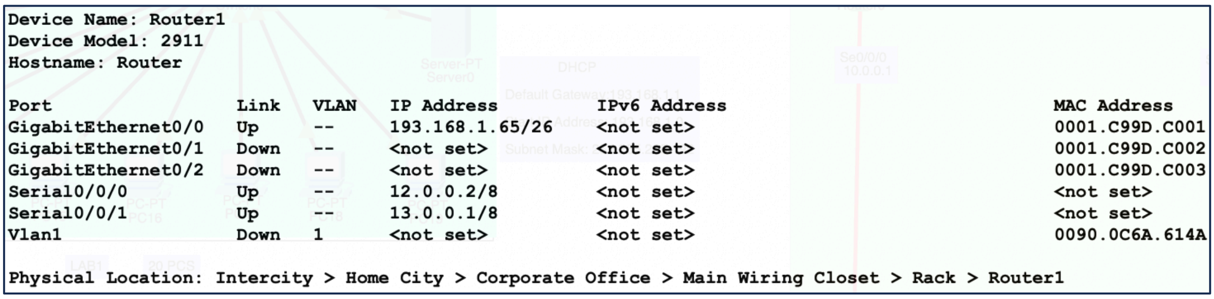
Fig 7

For Router-1 :

Gig0/0: 193.168.1.65

Se0/0/0 : 12.0.0.2

Se0/0/1 : 13.0.0.1



```
Device Name: Router1
Device Model: 2911
Hostname: Router

Port                  Link   VLAN   IP Address        IPv6 Address                       MAC Address
GigabitEthernet0/0    Up     --     193.168.1.65/26   <not set>                          0001.C99D.C001
GigabitEthernet0/1    Down   --     <not set>         <not set>                          0001.C99D.C002
GigabitEthernet0/2    Down   --     <not set>         <not set>                          0001.C99D.C003
Serial0/0/0           Up     --     12.0.0.2/8        <not set>                          <not set>
Serial0/0/1           Up     --     13.0.0.1/8        <not set>                          <not set>
Vlan1                 Down   1      <not set>         <not set>                          0090.0C6A.614A

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router1
```

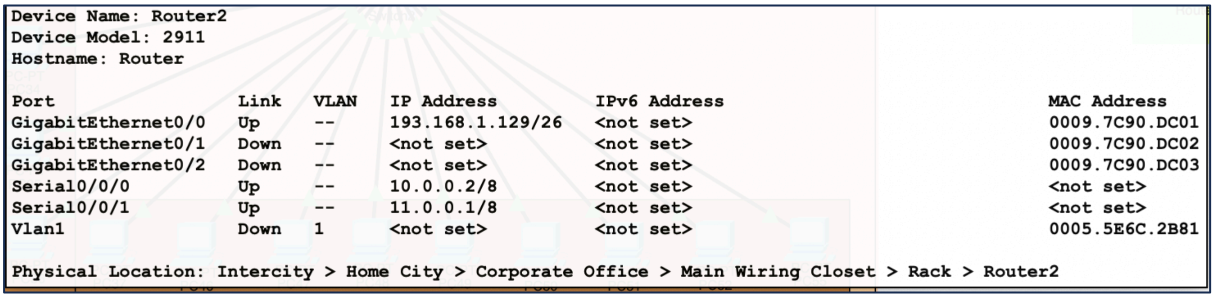
Fig 8

For Router-2 :

Gig0/0: 193.168.1.129

Se0/0/0 : 10.0.0.2

Se0/0/1 : 11.0.0.1



```
Device Name: Router2
Device Model: 2911
Hostname: Router

Port                  Link   VLAN   IP Address        IPv6 Address                       MAC Address
GigabitEthernet0/0    Up     --     193.168.1.129/26  <not set>                          0009.7C90.DC01
GigabitEthernet0/1    Down   --     <not set>         <not set>                          0009.7C90.DC02
GigabitEthernet0/2    Down   --     <not set>         <not set>                          0009.7C90.DC03
Serial0/0/0           Up     --     10.0.0.2/8        <not set>                          <not set>
Serial0/0/1           Up     --     11.0.0.1/8        <not set>                          <not set>
Vlan1                 Down   1      <not set>         <not set>                          0005.5E6C.2B81

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router2
```

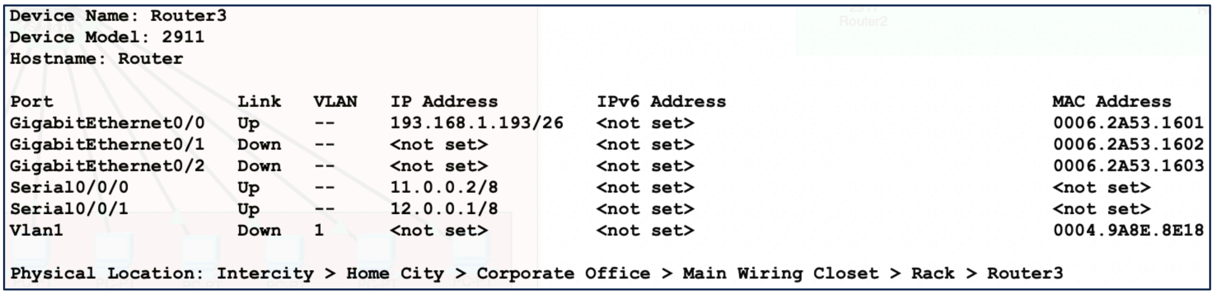
Fig 9

For Router-3 :

Gig0/0: 193.168.1.193

Se0/0/0 : 11.0.0.2

Se0/0/1 : 12.0.0.1



```
Device Name: Router3
Device Model: 2911
Hostname: Router

Port                Link   VLAN   IP Address        IPv6 Address                     MAC Address
GigabitEthernet0/0  Up     --     193.168.1.193/26  <not set>                        0006.2A53.1601
GigabitEthernet0/1  Down   --     <not set>         <not set>                        0006.2A53.1602
GigabitEthernet0/2  Down   --     <not set>         <not set>                        0006.2A53.1603
Serial0/0/0         Up     --     11.0.0.2/8        <not set>                        <not set>
Serial0/0/1         Up     --     12.0.0.1/8        <not set>                        <not set>
Vlan1               Down   1      <not set>         <not set>                        0004.9A8E.8E18

Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router3
```

Fig 10

1.4 A network diagram displaying the Network components, including devices and other equipment:

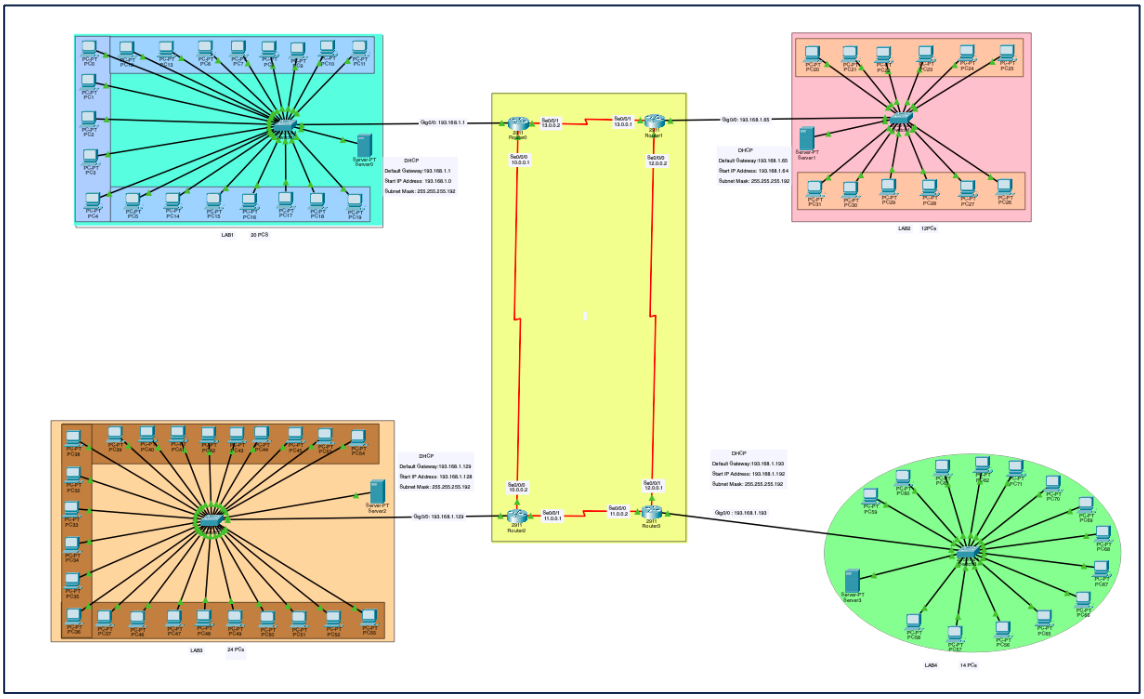


Fig 11:Network Structure

The above diagram depicts the overall network topology, which includes four subnets, as well as network devices such as routers, switches, and servers, as well as other network equipment such as PCs and laptops. These are linked utilising various cables such as copper straight, copper cross-over, and serial DTE. Let us watch how things turn out.

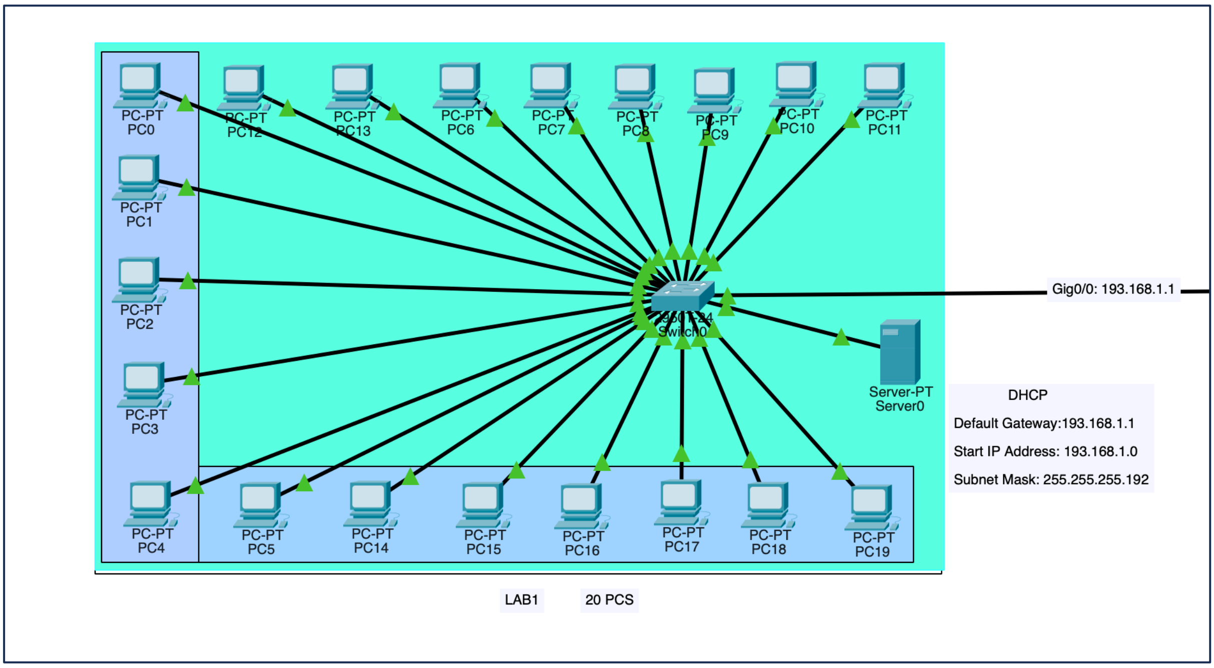


Fig 12: Lab-1

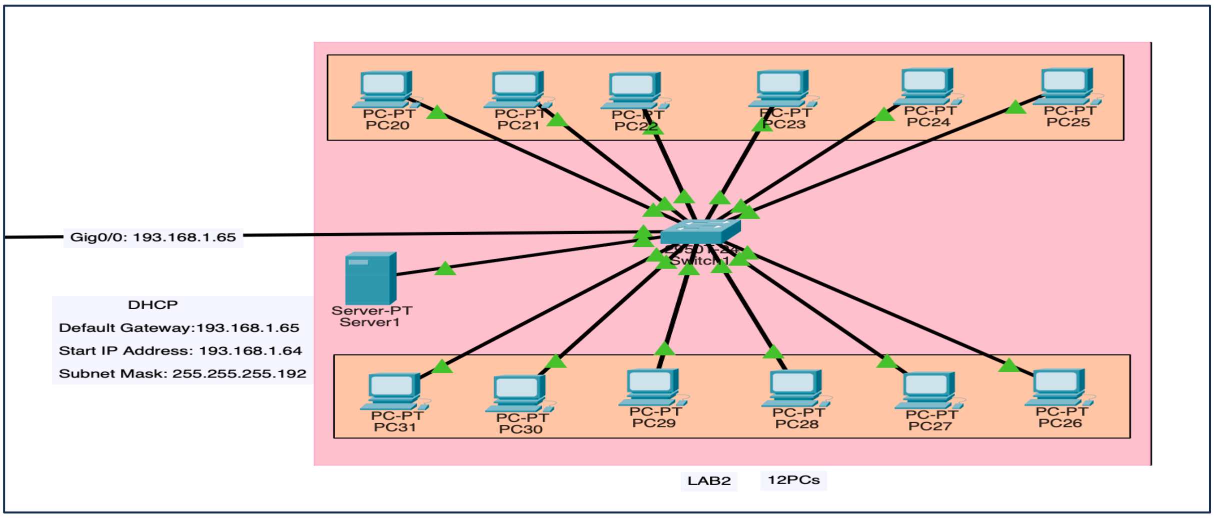


Fig 13: Lab-2

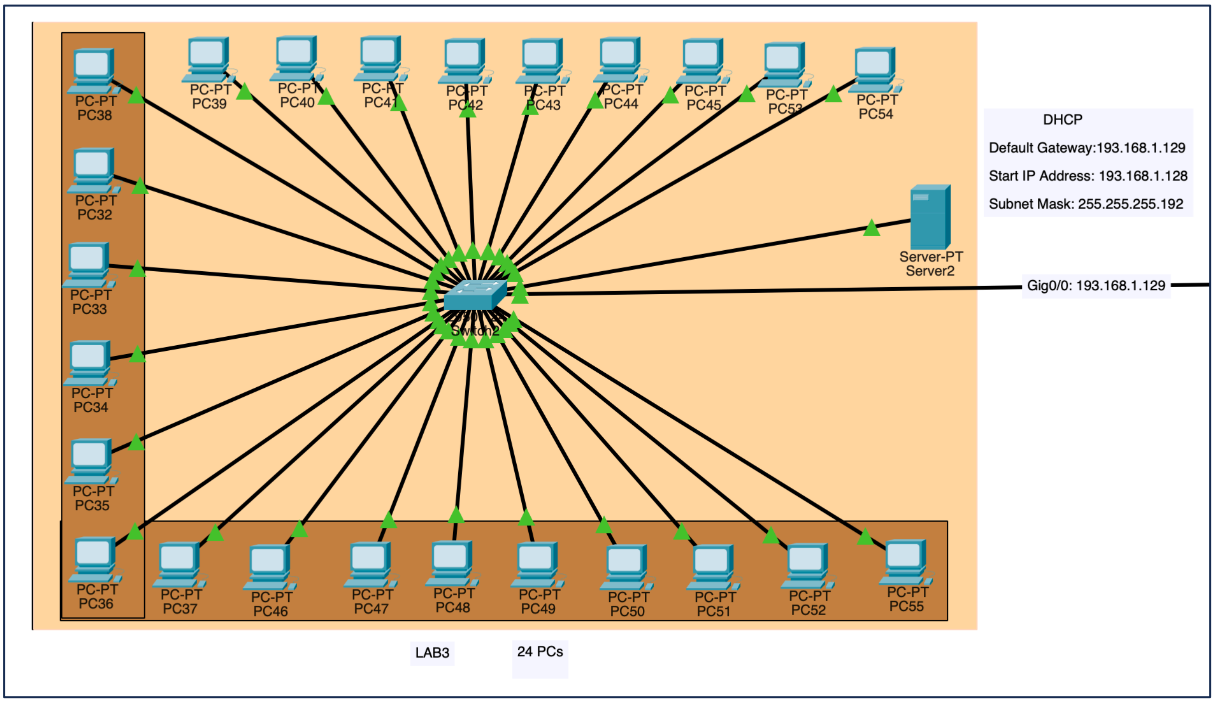


Fig 14: Lab-3

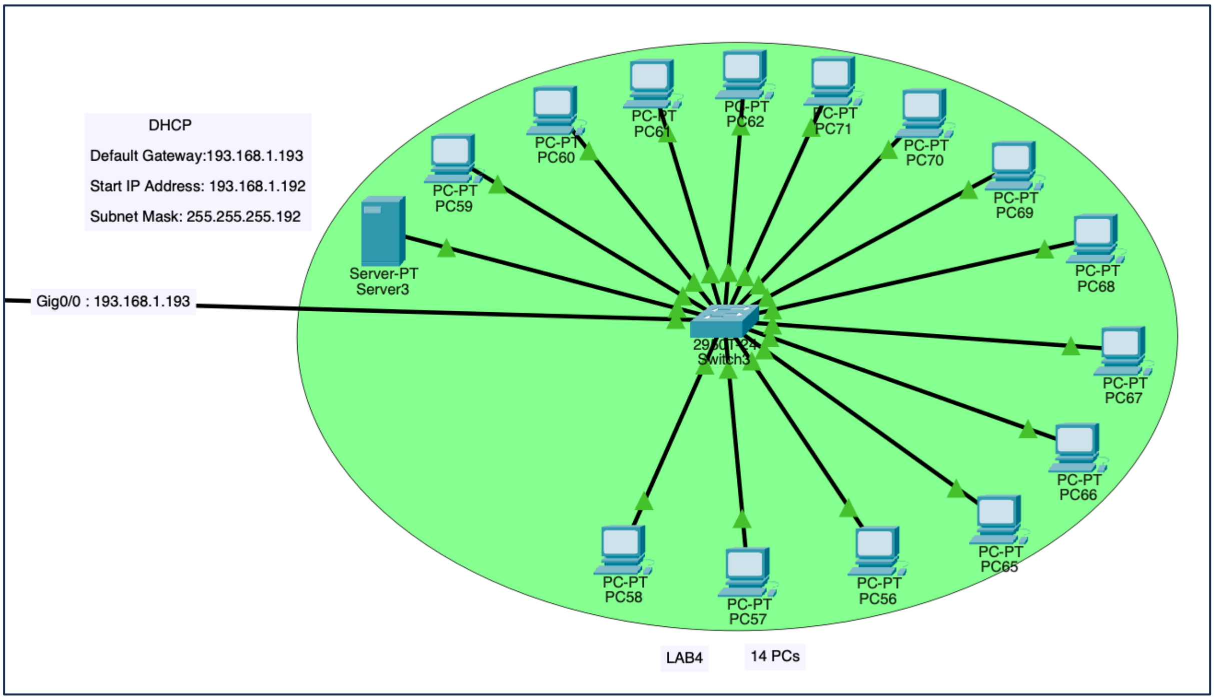


Fig 15: Lab-4

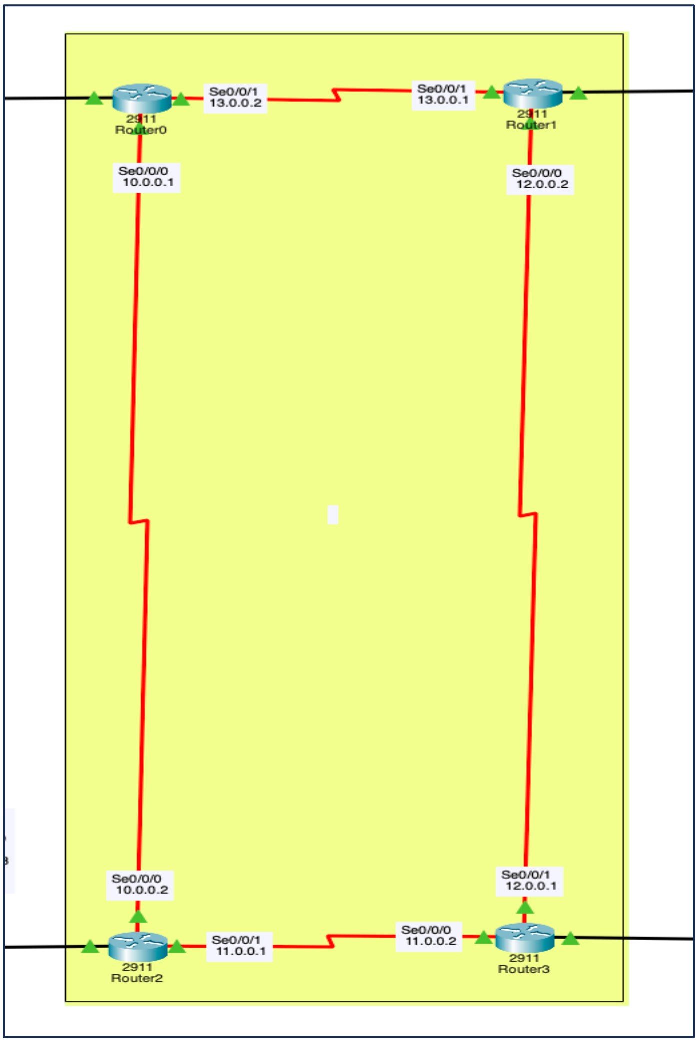


Fig 16: Server Room

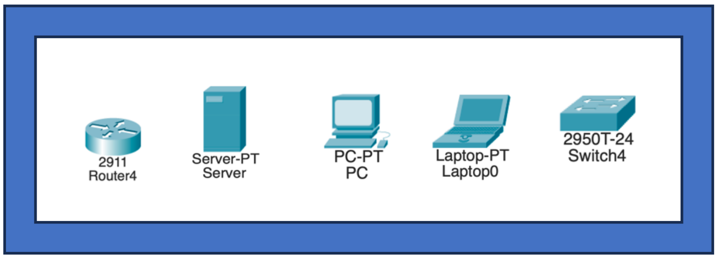


Fig 17: Devices used in this network

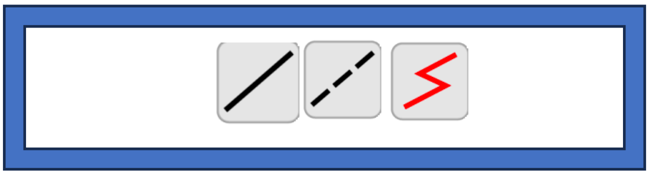


Fig 18: Cables used in this network

1.5 Justification of design decisions :

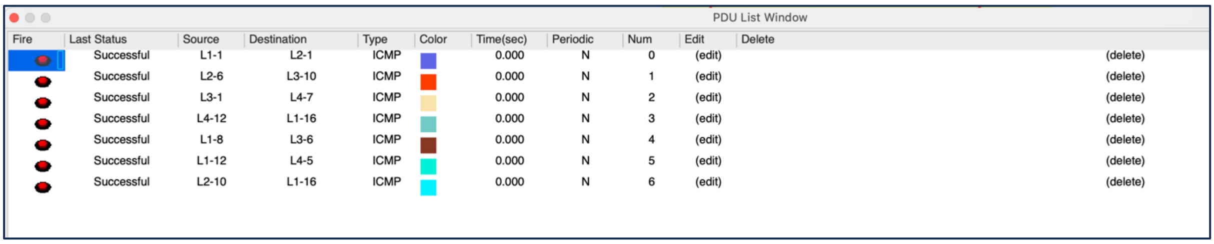
I used four subnetworks and the number of computers mentioned in the scenario and I utilised one router for each subnet because the network is a university and hence requires security. Using different routers increases network isolation and security between the two networks. This configuration can improve security by establishing distinct firewall rules, access control policies, and so forth.

Separate routers can provide redundancy and failover capabilities. If one router fails, the other network may continue to function.

Separate routers can improve scalability and performance optimisation in larger and more complicated networks.

2. Develop, Test and Evaluate the Network:

The network design was completed after assigning IP addresses to each device and connecting the devices with cables. Now we must test, assess, and validate the connections by transmitting messages from one computer to another over any subnetworks. We will learn about connection difficulties and IP configuration faults as a result of this. Using the PDU (protocol data unit), we can send messages from one computer to another. We can also test the procedure using simulation. And if the simulation goes well and the communication is favourable, we can observe the acknowledgement as successful, as shown in the graphic below.

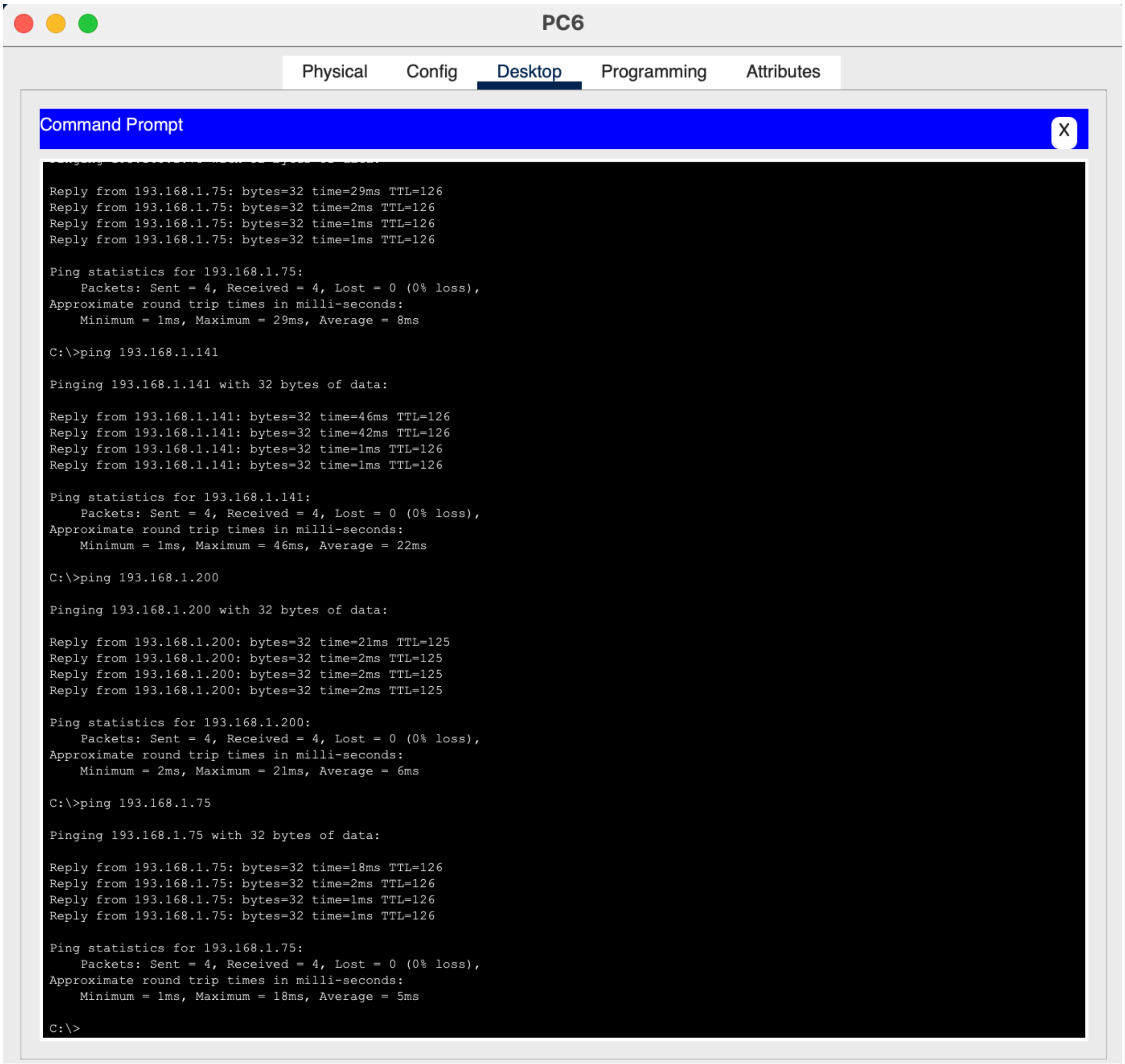


PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	L1-1	L2-1	ICMP	🟪	0.000	N	0	(edit)	(delete)
●	Successful	L2-6	L3-10	ICMP	🟥	0.000	N	1	(edit)	(delete)
●	Successful	L3-1	L4-7	ICMP	🟨	0.000	N	2	(edit)	(delete)
●	Successful	L4-12	L1-16	ICMP	🟩	0.000	N	3	(edit)	(delete)
●	Successful	L1-8	L3-6	ICMP	🟫	0.000	N	4	(edit)	(delete)
●	Successful	L1-12	L4-5	ICMP	🟦	0.000	N	5	(edit)	(delete)
●	Successful	L2-10	L1-16	ICMP	🟦	0.000	N	6	(edit)	(delete)

Fig 19: Acknowledgments

There is also a command prompt option for determining whether or not communication is working properly. Using the ping command, we can ping any computer using its IP address, for example ping 193.168.1.201



```
Reply from 193.168.1.75: bytes=32 time=29ms TTL=126
Reply from 193.168.1.75: bytes=32 time=2ms TTL=126
Reply from 193.168.1.75: bytes=32 time=1ms TTL=126
Reply from 193.168.1.75: bytes=32 time=1ms TTL=126

Ping statistics for 193.168.1.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 29ms, Average = 8ms

C:\>ping 193.168.1.141

Pinging 193.168.1.141 with 32 bytes of data:

Reply from 193.168.1.141: bytes=32 time=46ms TTL=126
Reply from 193.168.1.141: bytes=32 time=42ms TTL=126
Reply from 193.168.1.141: bytes=32 time=1ms TTL=126
Reply from 193.168.1.141: bytes=32 time=1ms TTL=126

Ping statistics for 193.168.1.141:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 46ms, Average = 22ms

C:\>ping 193.168.1.200

Pinging 193.168.1.200 with 32 bytes of data:

Reply from 193.168.1.200: bytes=32 time=21ms TTL=125
Reply from 193.168.1.200: bytes=32 time=2ms TTL=125
Reply from 193.168.1.200: bytes=32 time=2ms TTL=125
Reply from 193.168.1.200: bytes=32 time=2ms TTL=125

Ping statistics for 193.168.1.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 21ms, Average = 6ms

C:\>ping 193.168.1.75

Pinging 193.168.1.75 with 32 bytes of data:

Reply from 193.168.1.75: bytes=32 time=18ms TTL=126
Reply from 193.168.1.75: bytes=32 time=2ms TTL=126
Reply from 193.168.1.75: bytes=32 time=1ms TTL=126
Reply from 193.168.1.75: bytes=32 time=1ms TTL=126

Ping statistics for 193.168.1.75:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 18ms, Average = 5ms

C:\>
```

Fig 20: Command prompt

And after successful communication, it displays ping data for that specific IP address. The outcome displays transmitted, received, and loss statistics. The method is depicted in the diagram above.

2.1 Describing how the network design will meet the needs of the users:

We may presume that both staff and students are among the users. From the perspective of the student, the network I designed will satisfy the student's needs by facilitating error-free network communication. The student will be able to transfer data, browse data, and communicate with other systems using his or her own system. From the perspective of the staff, there are a few points to note as well. First, in addition to the ability to administer lab examinations in those systems, the staff will also need to be able to monitor the student data. Additionally, at least one computer in each lab has to be set up as a virtual machine that can run two or more operating systems at once. This configuration offers students practical teaching techniques that enable them to work with many operating systems, such as Windows, Ubuntu, MacOS, etc.

The network components and equipment are arranged in the UCB Camdon home to maximise lab operation. Given that there are four laboratories, each lab should have its own router, which aids in controlling network traffic and connectivity. Additionally, switches that facilitate data transfer and intra-lab communication should be placed between the routers and PCs.

The network has been precisely and effectively constructed to meet the aforementioned user demands without any connectivity problems or malfunctioning communications.

2.2 Three suggestions for further upgrading the network :

1. Using VLAN to divide the networks.

The network may broadcast traffic, increase network performance, and strengthen security by utilising VLAN. The physical network can be divided into several smaller virtual networks to achieve this. It is possible to divide this logically or virtually. There won't be any more resources needed for the procedure. **(Dach, 2023)**
Moreover, by doing this, we may have a high network performance and little traffic in the peak periods and also unneeded server overload..

2. Improve Availability and Redundancy Measures:

We are able to execute continuous operations and enhance network performance, stability, and downtime. Measuring the availability and redundancy of the primary devices, such as switches and routers, may do all of this. Implementing redundant connections, such as HSRP (Hot Standby Router Protocol) for switches, can assist with this. Educational institutions and learning environments that require constant access to materials might benefit from this procedure.

3. Prioritise Traffic using Quality of Service (QoS):

Quality of Service, or QoS, should be used to deliver the highest performance possible for certain needs, such as VoIP conversations, video conferencing, and educational courses. Through the use of QoS algorithms, traffic may be prioritised and managed extremely effectively **(Fortinet, 2022)**.Establishing these objectives enables the laboratories to run reliably and extremely responsively during periods of high demand.

3. Install and set up a Virtual Machine :

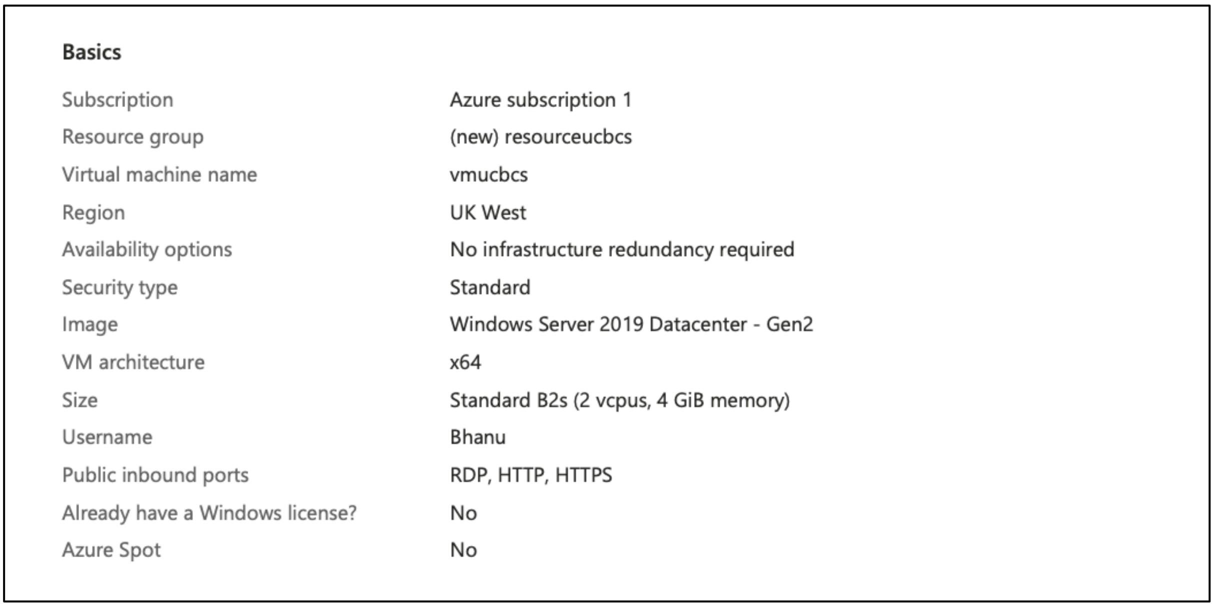
As a Junior Network Engineer, I am responsible for emulating the two operating systems to run on a virtual machine simultaneously. With the help of this setup, students may work with a variety of operating systems, including Windows, Ubuntu, MacOS, and others, while also learning useful teaching approaches.

Going to virtualise a PC from a lab by following the below steps:

I am setting up the virtual machine using Microsoft Azure.

User guide for installing and configuring virtual machines :

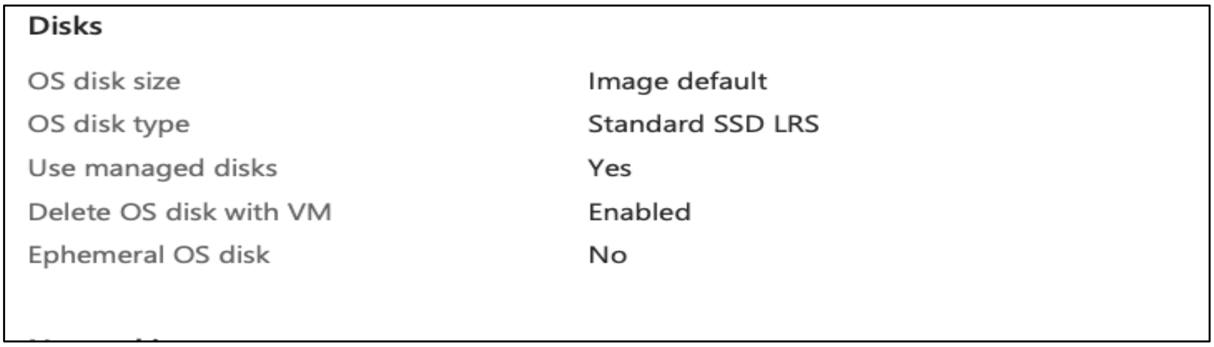
1. Log in to Microsoft Azure.
2. Select Virtual Machines from the Azure services menu.
3. Then click on Create, and from the drop-down menu, select the first option, Azure virtual machine. **(Azure, 2024)**From here, we must fill out certain information such as Basics, Discs, Networking, Management, and so on. The screenshots below demonstrate the information that we must enter in order to establish a virtual machine.



Basics

Subscription	Azure subscription 1
Resource group	(new) resourceucbcs
Virtual machine name	vmucbcs
Region	UK West
Availability options	No infrastructure redundancy required
Security type	Standard
Image	Windows Server 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard B2s (2 vcpus, 4 GiB memory)
Username	Bhanu
Public inbound ports	RDP, HTTP, HTTPS
Already have a Windows license?	No
Azure Spot	No

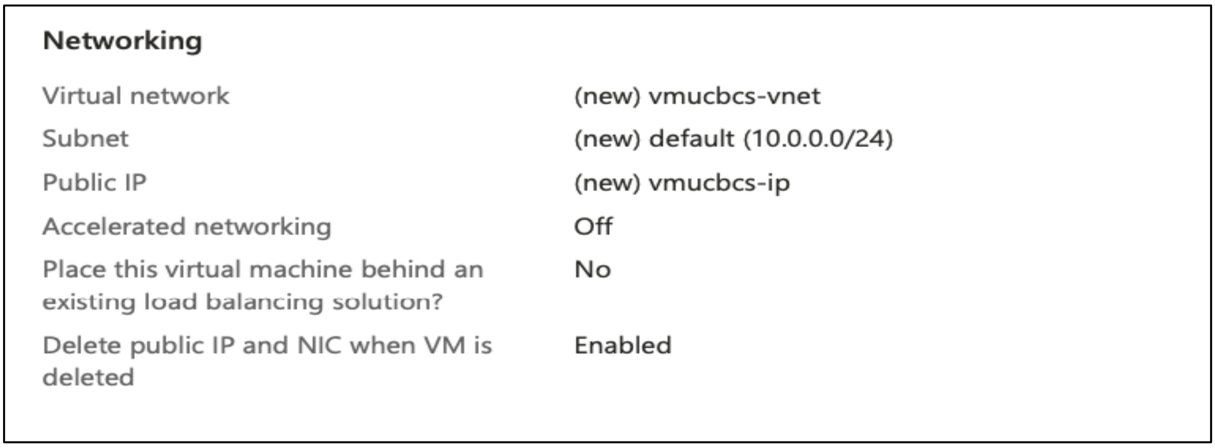
Fig 21: Basics



Disks

OS disk size	Image default
OS disk type	Standard SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

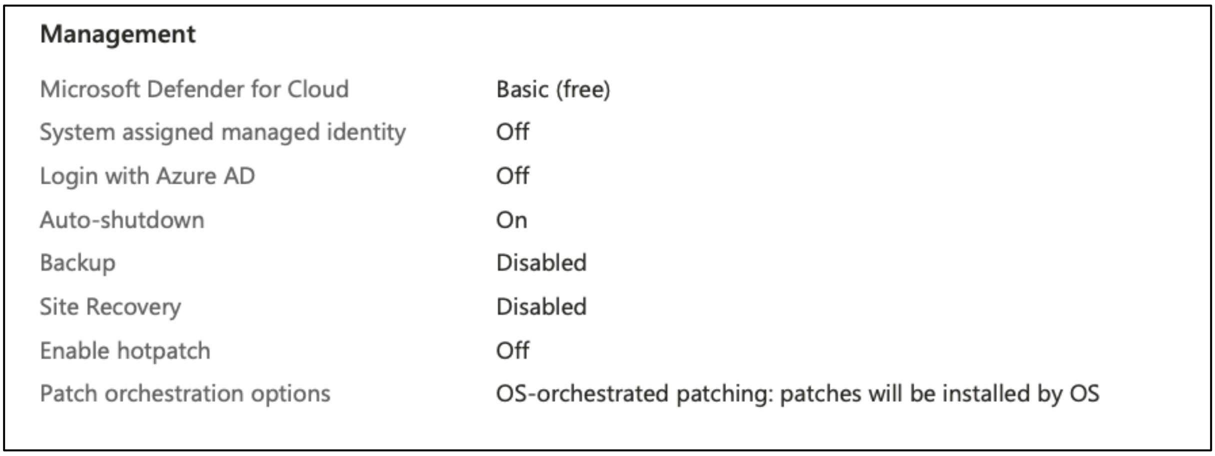
Fig 22: Disks



Networking

Virtual network	(new) vmucbcs-vnet
Subnet	(new) default (10.0.0.0/24)
Public IP	(new) vmucbcs-ip
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Enabled

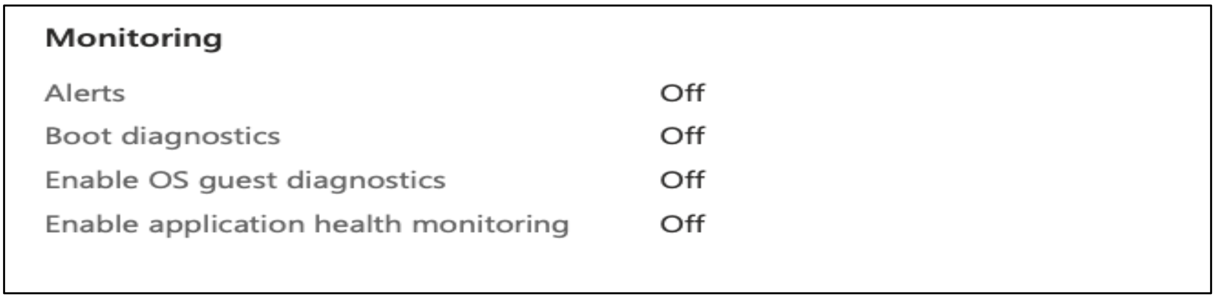
Fig 23: Networking



Management

Microsoft Defender for Cloud	Basic (free)
System assigned managed identity	Off
Login with Azure AD	Off
Auto-shutdown	On
Backup	Disabled
Site Recovery	Disabled
Enable hotpatch	Off
Patch orchestration options	OS-orchestrated patching: patches will be installed by OS

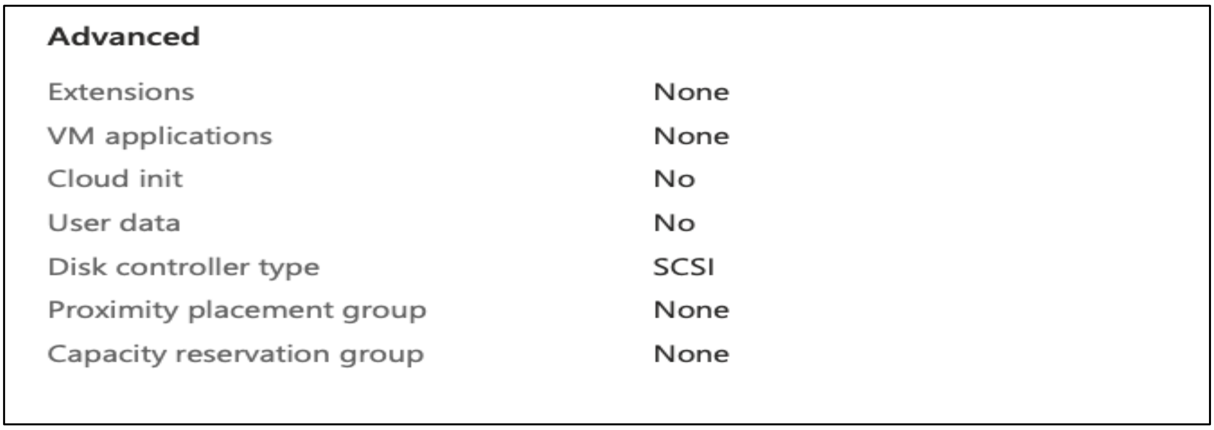
Fig 24: Management



Monitoring

Alerts	Off
Boot diagnostics	Off
Enable OS guest diagnostics	Off
Enable application health monitoring	Off

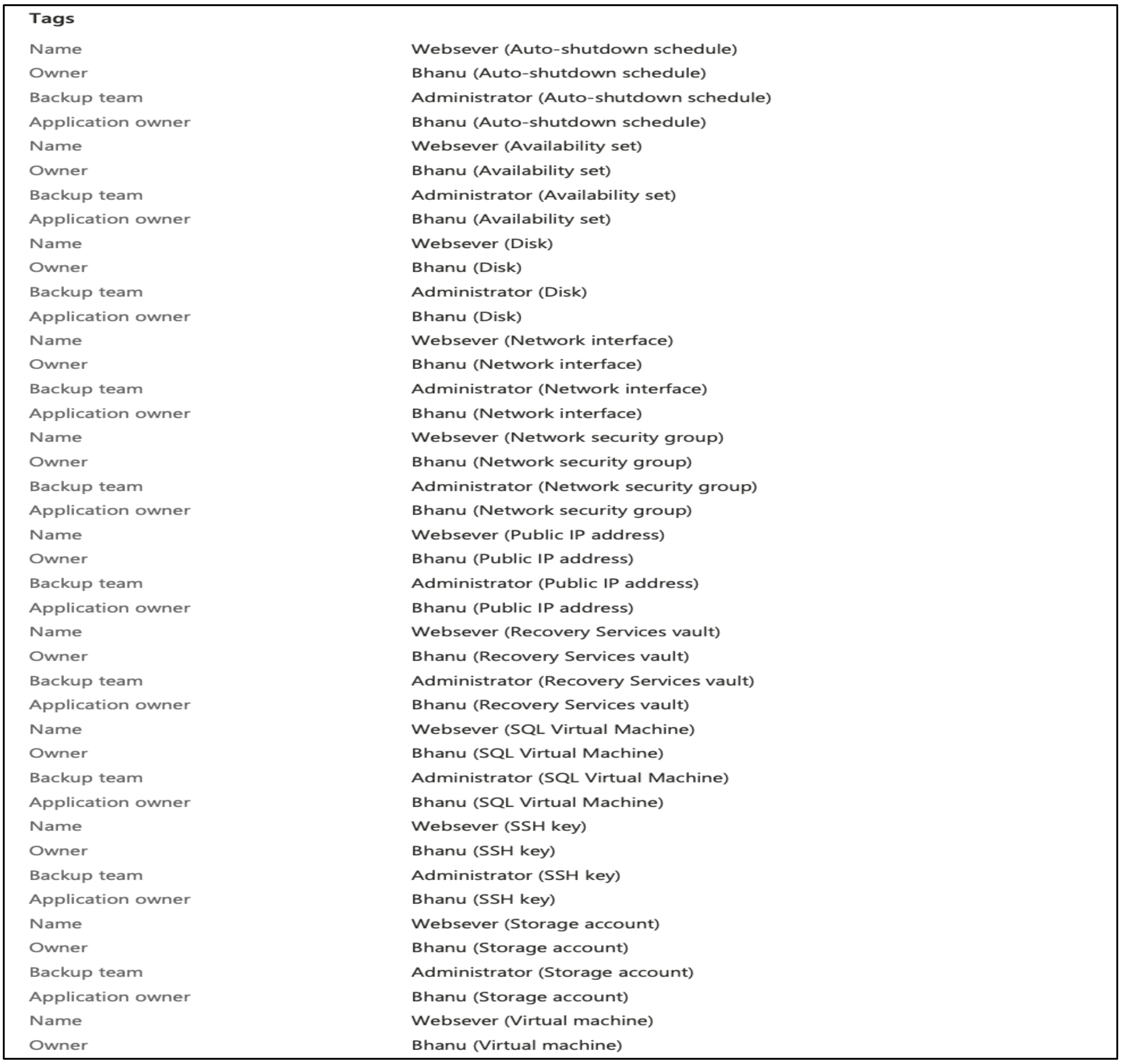
Fig 25: Monitoring



Advanced

Extensions	None
VM applications	None
Cloud init	No
User data	No
Disk controller type	SCSI
Proximity placement group	None
Capacity reservation group	None

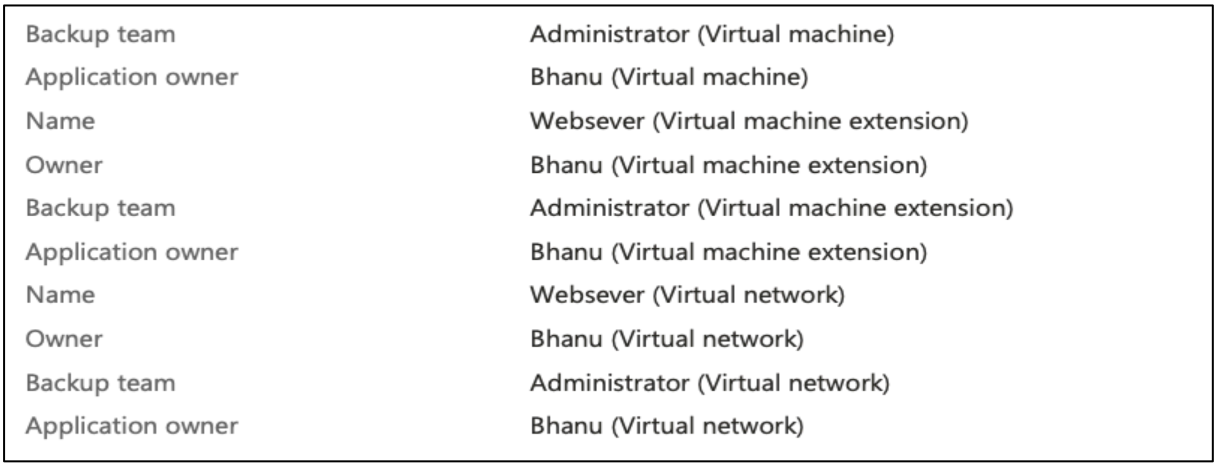
Fig 26: Advanced



Tags

Name	Websever (Auto-shutdown schedule)
Owner	Bhanu (Auto-shutdown schedule)
Backup team	Administrator (Auto-shutdown schedule)
Application owner	Bhanu (Auto-shutdown schedule)
Name	Websever (Availability set)
Owner	Bhanu (Availability set)
Backup team	Administrator (Availability set)
Application owner	Bhanu (Availability set)
Name	Websever (Disk)
Owner	Bhanu (Disk)
Backup team	Administrator (Disk)
Application owner	Bhanu (Disk)
Name	Websever (Network interface)
Owner	Bhanu (Network interface)
Backup team	Administrator (Network interface)
Application owner	Bhanu (Network interface)
Name	Websever (Network security group)
Owner	Bhanu (Network security group)
Backup team	Administrator (Network security group)
Application owner	Bhanu (Network security group)
Name	Websever (Public IP address)
Owner	Bhanu (Public IP address)
Backup team	Administrator (Public IP address)
Application owner	Bhanu (Public IP address)
Name	Websever (Recovery Services vault)
Owner	Bhanu (Recovery Services vault)
Backup team	Administrator (Recovery Services vault)
Application owner	Bhanu (Recovery Services vault)
Name	Websever (SQL Virtual Machine)
Owner	Bhanu (SQL Virtual Machine)
Backup team	Administrator (SQL Virtual Machine)
Application owner	Bhanu (SQL Virtual Machine)
Name	Websever (SSH key)
Owner	Bhanu (SSH key)
Backup team	Administrator (SSH key)
Application owner	Bhanu (SSH key)
Name	Websever (Storage account)
Owner	Bhanu (Storage account)
Backup team	Administrator (Storage account)
Application owner	Bhanu (Storage account)
Name	Websever (Virtual machine)
Owner	Bhanu (Virtual machine)

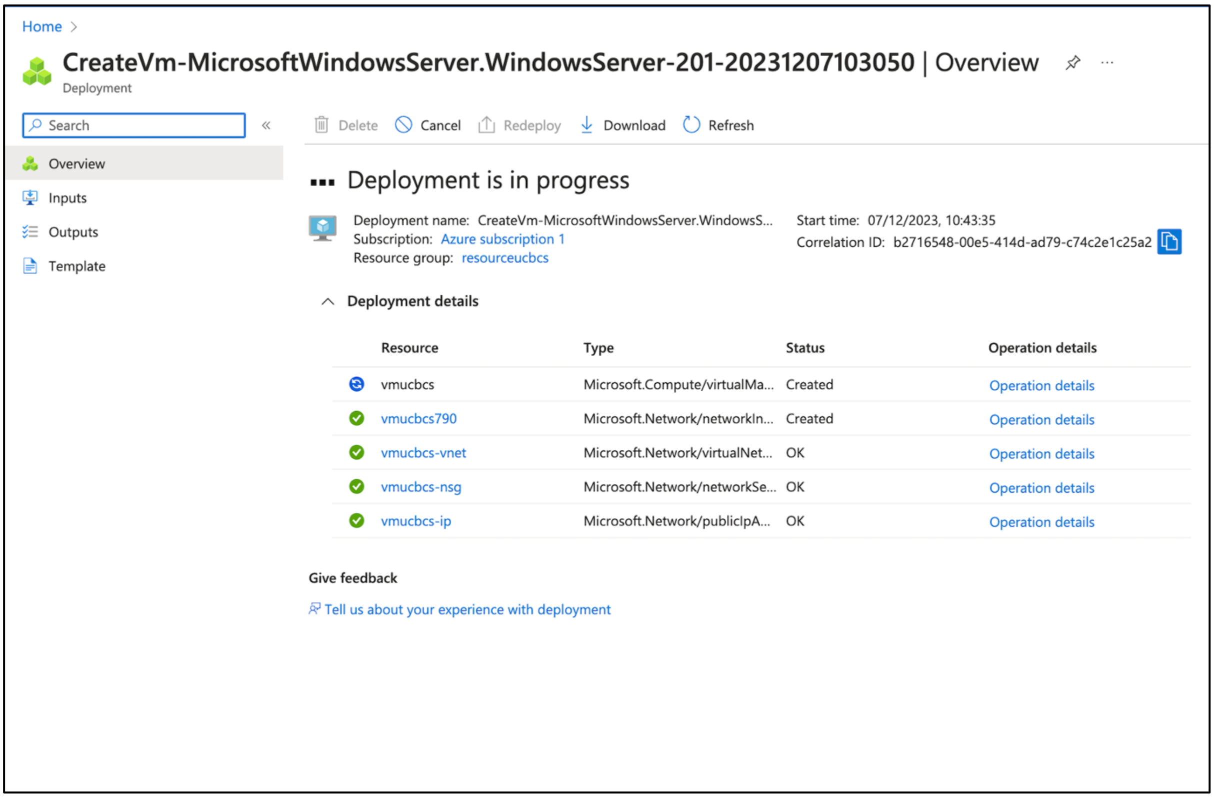
Fig 27 :Tags



Backup team	Administrator (Virtual machine)
Application owner	Bhanu (Virtual machine)
Name	Websever (Virtual machine extension)
Owner	Bhanu (Virtual machine extension)
Backup team	Administrator (Virtual machine extension)
Application owner	Bhanu (Virtual machine extension)
Name	Websever (Virtual network)
Owner	Bhanu (Virtual network)
Backup team	Administrator (Virtual network)
Application owner	Bhanu (Virtual network)

Fig 28: Tags

4. Finally, after entering these facts, we are given the opportunity to review and create. After that, we can click the 'review + create' button. The deployment will then begin (this will take some time). The deployment is seen in the screenshot below.



CreateVm-MicrosoftWindowsServer.WindowsServer-201-20231207103050 | Overview

Deployment

Deployment is in progress

Deployment name: CreateVm-MicrosoftWindowsServer.WindowsS...
Subscription: Azure subscription 1
Resource group: resourceucbcs

Start time: 07/12/2023, 10:43:35
Correlation ID: b2716548-00e5-414d-ad79-c74c2e1c25a2

Deployment details

Resource	Type	Status	Operation details
vmucbcs	Microsoft.Compute/virtualMa...	Created	Operation details
vmucbcs790	Microsoft.Network/networkIn...	Created	Operation details
vmucbcs-vnet	Microsoft.Network/virtualNet...	OK	Operation details
vmucbcs-nsg	Microsoft.Network/networkSe...	OK	Operation details
vmucbcs-ip	Microsoft.Network/publicIpA...	OK	Operation details

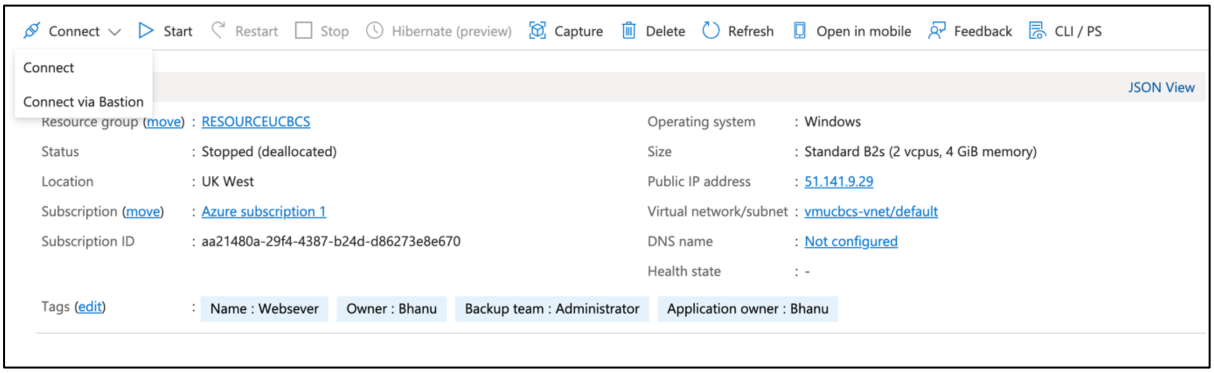
Fig 29: Deployment

After the deployment is complete, we can see that a virtual machine has been created. When we click on the virtual machine, it displays options such as connect, start, restart, and stop.

3.1 Connect to the virtual machine

Connect to the virtual computer via remote desktop. These instructions will show you how to connect to your virtual machine from a Windows computer. An RDP client, such as this Remote Desktop Client from the Mac App Store, is required on a Mac.

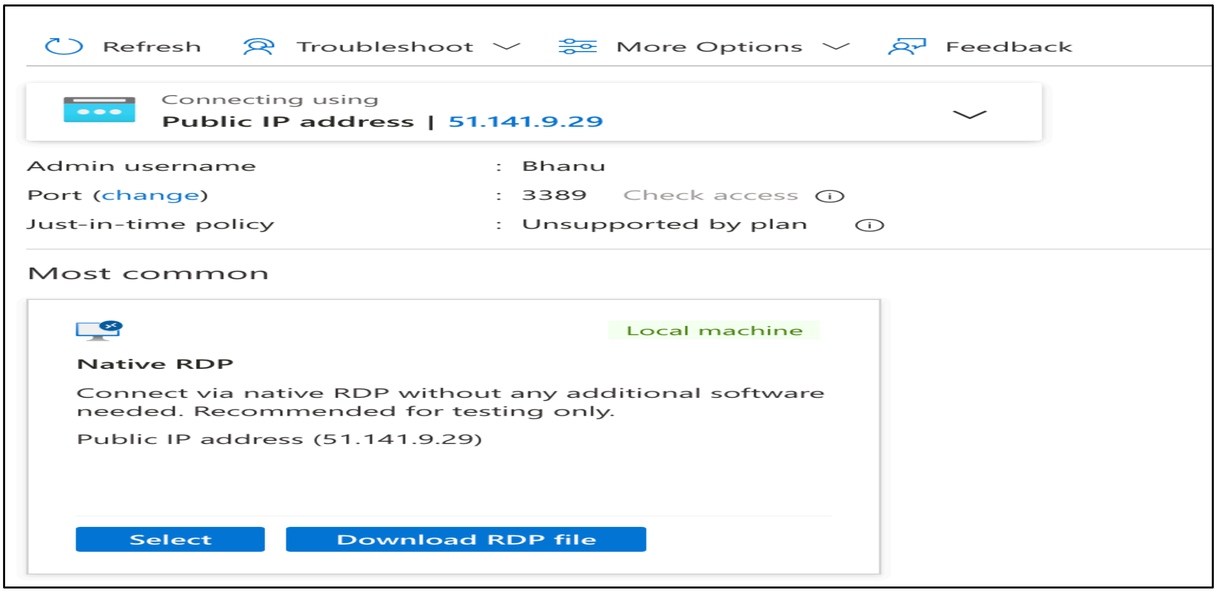
1. Select ‘Start’ from the overview page for your virtual machine. Then the virtual machine will be started.



Resource group (move) : RESOURCEUCBCS
Status : Stopped (deallocated)
Location : UK West
Subscription (move) : Azure subscription 1
Subscription ID : aa21480a-29f4-4387-b24d-d86273e8e670
Operating system : Windows
Size : Standard B2s (2 vcpus, 4 GiB memory)
Public IP address : 51.141.9.29
Virtual network/subnet : vmucbcs-vnet/default
DNS name : Not configured
Health state : -
Tags (edit) : Name : Websever Owner : Bhanu Backup team : Administrator Application owner : Bhanu

Fig 30: Virtual machine

2. And then click on connect, it shows an options to download RDP file. Download it and open the file.



Connecting using
Public IP address | 51.141.9.29
Admin username : Bhanu
Port (change) : 3389 Check access
Just-in-time policy : Unsupported by plan
Most common
Native RDP
Connect via native RDP without any additional software needed. Recommended for testing only.
Public IP address (51.141.9.29)

Fig 31: Virtual machine

3. During the sign-in procedure, you may receive a certificate warning. To establish the connection, select Yes or Continue.
4. After entering our name and password, the remote desktop connection will be established and our virtual machine will be launched.
5. Here, it requests your name and password. If the validation is successful, a remote desktop connection will be established, launching our virtual machine.

References

Gicheha, K. (2023, September 28). *TCP/IP Model*. Retrieved from Medium: medium.com/@gichehakevin/tcp-ip-model-d9209dff86db

inflobox. (2024). *WHAT IS LAYER 4 OF THE OSI MODEL: TRANSPORT LAYER?* Retrieved from inflobox: https://www.infoblox.com/glossary/layer-4-of-the-osi-model-transport-layer/#:~:text=Layer%204%20of%20the%20OSI%20Model%3A%20Transport%20Layer%20provides%20transparent,and%20desegmentation%2C%20and%20error%20control.

De, A. (2023, may 08). *Software defined Networking(SDN)*. Retrieved from Geeksforgeeks: geeksforgeeks.org/software-defined-networking/

elprocus. (2023). *TCP/IP Protocol Architecture and Its Layers* . Retrieved from elprocus: https://www.elprocus.com/tcp-ip-protocol-architecture-and-its-layers/

WHAT IS LAYER 4 OF THE OSI MODEL: TRANSPORT LAYER? (2024). Retrieved from infoblox: https://www.infoblox.com/glossary/layer-4-of-the-osi-model-transport-layer/#:~:text=Layer%204%20of%20the%20OSI%20Model%3A%20Transport%20Layer%20provides%20transparent,and%20desegmentation%2C%20and%20error%20control.

Kirvan, P. (2022, march). *application layer*. Retrieved from TechTarget: techtarget.com/searchnetworking/definition/Application-layer#:~:text=The%20application%20layer%20sits%20at,different%20computer%20systems%20and%20networks.

Chari, K. (2003). *Application Layer*. Retrieved from ScienceDirect: sciencedirect.com/topics/computer-science/application-layer-protocol#:~:text=HTTP%20is%20an%20application%20layer,a%20server%2C%20a%20web%20site.

GeeksforGeeks. (2023, april 27). *Internet Control Message Protocol (ICMP)*. Retrieved from GeeksforGeeks: geeksforgeeks.org/internet-control-message-protocol-icmp/

Hatim. (n.d.). *What is the purpose of subnetting in a network?* Retrieved from TutorChase: tutorchase.com/answers/a-level/computer-science/what-is-the-purpose-of-subnetting-in-a-network

GeeksforGeeks. (2023, may 08). *Software defined Networking(SDN)*. Retrieved from GeeksforGeeks: geeksforgeeks.org/software-defined-networking/

GeeksforGeeks. (2023, may 08). *Software defined Networking(SDN)* . Retrieved from GeeksforGeeks: geeksforgeeks.org/software-defined-networking/

drpankajdadhich. (2022, june 14). *SDN architecture*. Retrieved from drpankajdadhich: drpankajdadhich.com/2022/06/software-defined-networking-sdn.html

Dach, T. (2023, aug 09). *Network segmentation vs. VLAN explained*. Retrieved from algosec: algosec.com/blog/network-segmentation-vs-vlan/

Fortinet. (2022). *Guarantee Performance with QoS*. Retrieved from Fortinet: fortinet.com/uk/resources/cyberglossary/qos-quality-of-service#:~:text=QoS%20enables%20an%20organization%20to,of%20performance%20across%20their%20networks.

Azure. (2024, april 01). *Quickstart: Create a Windows virtual machine in the Azure portal*. Retrieved from Azure: learn.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal

CONCLUSION:

From Part A, In summary, while the TCP model has 4 layers and defines the Internet's basic architecture, the OSI has 7 layers. This provides an in-depth analysis of the TCP layer architecture, a thorough comparison with the OSI model and an explanation of the various functions of each layer. By looking at design issues and protocols at each level, we can better understand the practical issues of TCP. In addition, SDN is becoming a critical factor affecting several layers of the TCP architecture. The analysis and findings show how dynamic modern Internet infrastructures are and how important it is to adapt network designs and management techniques to the changing environment resulting from SDN integration.

From Part B, Finally, we have shown how to create a network according to the requirements. In task 1, the network was designed by allocating IP addresses to each network and figuring out subnetting for each lab. Task 2 involved installing both software and hardware components to complete the implementation. In-depth testing is also carried out to confirm whether or not the network is communicating effectively. To work with the various operating systems, a PC from each lab has been virtualized for task three.

Additionally, three recommendations have been made for the network's future growth that regulates traffic control and network performance. This paperwork demonstrates that the prescribed duties have been satisfactorily finished. Our designed network provides high-performance, scalable, and secure connectivity that meets current requirements and may be expanded and developed as needed in the future.