

ASSIGNMENT1

Research, Build, and deploy a virtualized Enterprise Network

Module: **Network Operating System Services**

Module Code: **ACCA5023**

Student Name: **Beda Clement NDEPO**

Student No: **2411399**

Lecturer: **MD Sadeque Imam Shaikh**



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

UNIVERSITY OF WALES TRINITY ST DAVID

Table of Contents

INTRODUCTION	2
TASK 1	3
1- Research on Hypervisor	3
1.1 Hypervisor type 1 and type 2	3
1.2 Advantages & Disadvantages.....	4
1.3 Features of Type 1 and Type 2	4
1.4 Research on IP Addressing	4
1.4.1 What is IP address	4
1.4.2 IP Address Contributions.....	5
1.4.3 IP Address function	5
1.4.4 Difference between IPV4 and IPV6	5
Practical Example.....	6
1.4.5 How it works.....	6
1.5 Research on Routing.....	6
1.5.1 Difference between Static and Dynamic Routing.....	6
1.6 Research on Network Services.....	7
1.6.1 Virtual Private Networks (VPNs).....	7
1.6.2 Dynamic Host Configuration Protocol (DHCP).....	8
1.6.3 Active Directory Domain Services (AD DS).....	8
1.6.4 Certificate Authorities (CAs) & PKI	8
TASK 2	9
2.1 Evidence of Download and installation	9
2.1.1 Creation of Virtual machine Windows1 and 2	9
2.1.2 Creation of Virtual machine Linux Debian1 and 2	9
2.1.3 Installation of Windows and Linux OS.....	10
as you can see on the virtual box the 4 operations systems windows and Linux are installed and are running well.....	10
2.2 Deploy your network as per the given topology	10
2.2.1 Creation of Network with NAT Network 1 for windows	11
2.2.2 Creation of Network with NAT Network 2 for Linux	11
2.3 IP addressing	12
2.3.1 Windows Server and Windows Client	12
2.3.2 Debian Server and Debian Client.....	12

2.3.3 Successful connectivity within Windows network. (Ping 192.168.1.1 and Ping 192.168.1.10)	13
2.3.4 Successful connectivity within Linux network. (Ping 192.168.2.1 and Ping 192.168.2.10)	13
2.3.5 Unsuccessful connectivity between Linux and windows network	14
TASK 3	14
3- Technical Reflection covering network deployment and testing	14
3.1 Personal reflection	15
CONCLUSION	15
References	16

INTRODUCTION

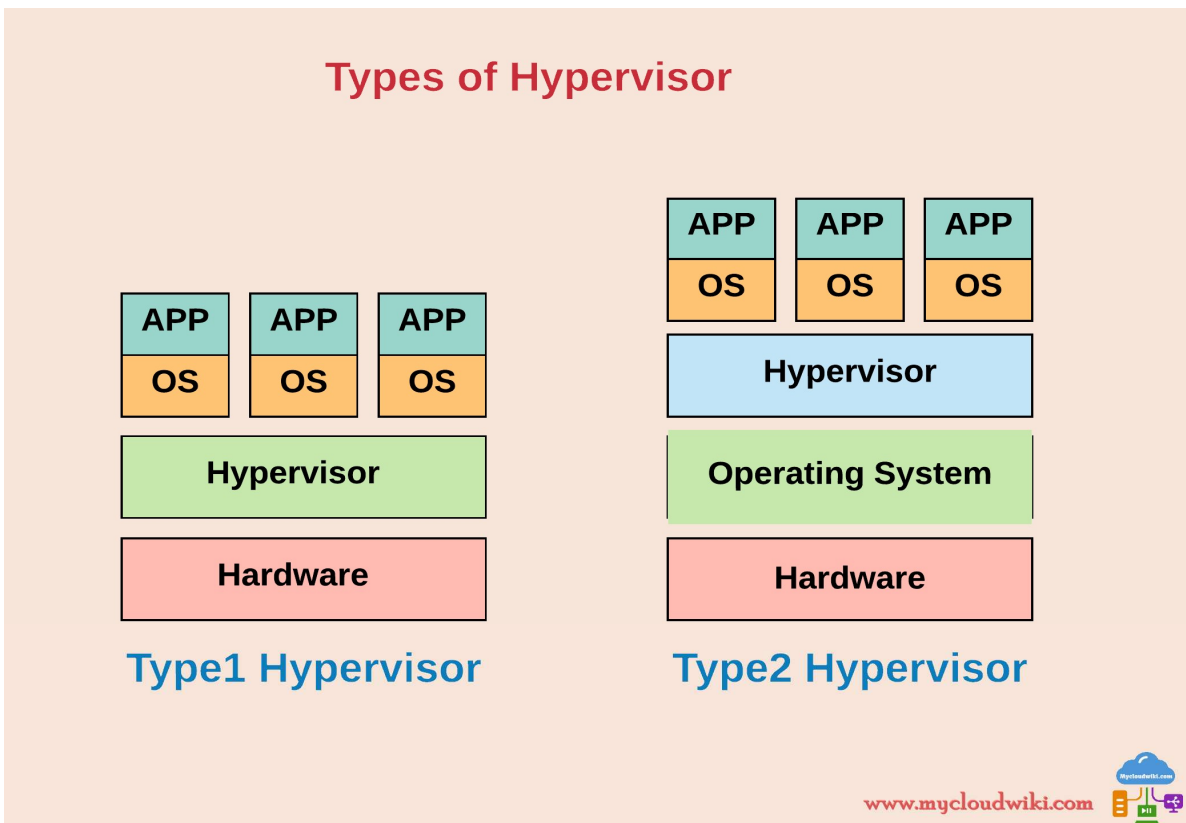
Network operations systems and services comprise the tools, processes, and architectures used to monitor, manage, and maintain network infrastructures for optimal performance. They play a vital role in tracking network behaviour, regulating traffic, ensuring quality of service, and detecting anomalies, functions that are crucial for effective network management and informed decision-making. Through this study, we will define the appropriate hypervisor type, how IP addressing is important, and some research on routing and Network services.

TASK 1

1- Research on Hypervisor

1.1 Hypervisor type 1 and type 2

A hypervisor is software that enables multiple operating systems to run at once on a single



physical machine by controlling hardware resources. [1]

Type 1 Hypervisors (Bare-Metal):

Run directly on hardware, no host OS. Provide strong isolation, security, and performance. Common in servers, less desktop support.

Type 2 Hypervisors (Hosted):

Operates on a host OS, easy to deploy, best for testing/dev, less isolation. Examples: VMware Player, Parallels Desktop, Windows Virtual PC.

1.2 Advantages & Disadvantages

Hypervisors are a fundamental element of virtualization technology, serving as an abstraction layer that allows Multiple virtual machines can run at the same time on a single physical system. By decoupling VMs from the underlying hardware, hypervisors enhance resource efficiency and enable diverse operating systems to coexist on the same platform. This separation also strengthens security by isolating each VM, thereby minimizing the risk of direct hardware-based attacks. [2]

1.3 Features of Type 1 and 2

Type 1 (Bare-metal Hypervisors)

Runs directly on hardware without a host operating system.

Performance & Stability: Offers better resource utilization and lower overhead.

Features: Live migration, high availability, snapshots, clustering, enterprise-grade scalability.

Type 2 (Hosted Hypervisors)

Runs on top of a host OS (e.g., Windows or Linux).

Ease of Use: Simple to install and manage, good for labs or small setups.

Features: Snapshots, portability, but less efficient than Type 1.

Considering the environment (**SWANSEA ACCA**) the most suitable hypervisor for this topology is the type2 because:

Oracle VirtualBox is free, cross-platform, supports Windows and Debian.

VMware Workstation is a robust desktop virtualization, good for testing

1.4 Research on IP Addressing

1.4.1 What is IP address

An IP address is the core system that directs data across the internet, like a digital postal service. Routers act as mail carriers, moving packets between devices until they reach their destination. Unique addresses and routing protocols ensure data arrives at the right place efficiently. [3]

IP addresses are the backbone of digital communication, making networks functional, effective, and capable of supporting everything from personal devices to global enterprises.

Data is split into **packets**, routed through networks, and reassembled at the destination, with IP addresses guiding each packet to ensure reliable communication. **Switches** link devices within a local network, while **routers** guide data between networks across the internet.

An IP address contributes by uniquely identifies devices, enabling efficient routing for reliable, scalable, and secure communication

1.4.2 IP Address Contributions

Contributions	Descriptions
Unique Identification	Each device is assigned a distinct IP address, preventing confusion and ensuring accurate delivery of data packets.
Location Addressing	IP addresses act like digital coordinates, guiding routers to deliver information to the correct destination.
Efficient Data Transmission	By combining identification and location, IP addresses enable seamless communication among billions of devices.
Routing and Delivery	Routers use IP addresses to choose the best path for data, ensuring speed, reliability, and scalability.
Scalability and Growth	IPv4 and IPv6 systems allow networks to expand; IPv6 supports nearly limitless unique addresses.
Security and Tracking	IP addresses enforce security policies, detect suspicious activity, and aid troubleshooting.

1.4.3 IP Address function

An IP address is a vital identifier that enables device communication across networks. As cloud computing and the Internet of Things expand, the surge in connected devices demands careful IP management to prevent conflicts and maintain efficient network operations [4]

1.4.4 Difference between IPV4 and IPV6

The key difference between IPv4 and IPv6 is address space. IPv4’s 32-bit system supports about 4.3 billion addresses, which ran out around 2010 due to rapid internet growth. IPv6, with its 128-bit design, offers 2^128 possible addresses, ensuring ample capacity for future expansion [5]

Feature	IPv4	IPv6
Address Size	32-bit (≈4.3 billion addresses)	128-bit (≈340 undecillion addresses)
Header Complexity	Larger, more complex	
Address Format	Decimal, dotted (e.g., 192.168.0.1)	Hexadecimal, colon-separated (e.g., 2001:0db8:85a3::8a2e:0370:7334)

Configuration	Manual or DHCP	Auto-configuration supported
Security	No built-in security (requires IPSec as add-on)	IPSec is mandatory, providing stronger security
Efficiency	Less efficient	More efficient, reduces routing table size
Quality of Service	Limited support	Better traffic prioritization for voice/video

Practical Example

Imagine you're setting up a small office:

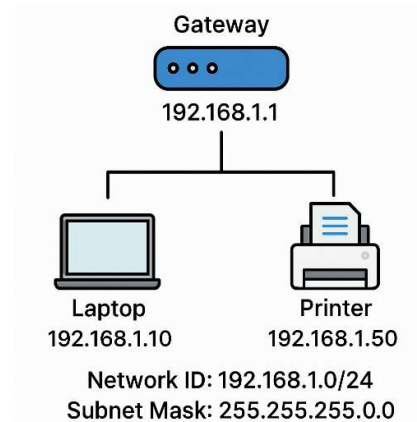
Network ID: 192.168.1.10/24

Subnet Mask: 225.225.225.0

Gateway: 192.168.1.1 (router)

Devices:

- Laptop: 192.168.1.10
- Printer: 192.168.1.50



1.4.5 How it works

When the laptop (192.168.1.10) wants to print, it sends data directly to the printer (192.168.1.50) because they're on the same subnet.

When the laptop wants to browse the web, it sends traffic to the gateway (192.168.1.1), which forwards it to the internet.

1.5 Research on Routing

Routing protocols are systems that define how data travels from a source node to its destination within a network. They are vital for directing data packets efficiently and reliably across different types of networks. By continuously managing routes, these protocols overcome challenges such as shifting network topologies, restricted bandwidth, energy limitations, and significant propagation delays. Their importance is particularly evident in specialized environments, including underwater wireless sensor networks (UWSNs) and opportunistic networks, where conditions are highly dynamic and resource constrained. [6]

Routing protocols play a crucial role in guiding data across networks by identifying the most efficient paths for transmission. They function by allowing routers to share network information, evaluate possible routes, and dynamically adjust to changes in the network to maintain smooth and reliable communication.

1.5.1 Difference between Static and Dynamic Routing

A **Static Routing** is: Manually configured routes by an administrator.

- **Operation:** Fixed paths in the routing table; no automatic updates.
- **Advantages:** Simple for small networks; predictable and secure.

- **Disadvantages:** Not scalable; requires manual changes if topology shifts.

Example: Small office router with preset route to the internet.

Dynamic Routing: Routes learned and updated automatically via routing protocols.

- **Operation:** Routers exchange information and adjust paths as the network changes.
- **Advantages:** Scalable, adaptive, and resilient to failures.
- **Disadvantages:** More complex; consumes bandwidth and processing resources.
- **Example:** Enterprise network using OSPF to reroute traffic when a link goes down.

If you have a single router connecting the Debian relay and the Windows server: Use static routes. Keep the route from client subnets to the Windows server and back clear and tested. DHCP relay will work if the relay can reach the Windows server's DHCP service and return traffic is routed correctly. [7]

If you have multiple routers or redundant links between client subnets and the Windows server: Use a dynamic IGP like OSPF so the relay and clients maintain reachability during failures without manual intervention.

According to the topology setup with one route, the best routing approach will be the **static Routing**

1.6 Research on Network Services

VPNs are commonly deployed to securely link remote offices, research sites, and mobile users, serving as a cost-effective alternative or supplement to dedicated network lines. By encrypting data traffic, they enable safe remote access and ensure that information remains confidential even when transmitted across public networks. [8]

VPNs safeguard remote connections, DHCP streamlines IP address allocation, AD DS centralizes identity and policy management, and certificate authorities (CAs) establish trust through digital certificates. Effective use of these technologies relies on strong security, precise configuration, and scalable practices.

1.6.1 Virtual Private Networks (VPNs)

VPNs provide secure remote access by encrypting data traffic, protecting confidentiality across public networks. [9]

Features: Confidential data exchange, remote access, IPSec/SSL/TLS

Best Practices: Strong encryption, MFA, regular patching, log monitoring

1.6.2 Dynamic Host Configuration Protocol (DHCP)

DHCP automates IP configuration by dynamically assigning addresses and network settings, reducing errors and simplifying administration.

Features: Dynamic IP assignment, subnet/gateway/DNS configuration, lease management

Best Practices: Reservations for critical devices, VLAN segmentation, failover setup, log auditing

1.6.3 Active Directory Domain Services (AD DS)

AD DS consolidates identity, access control, and policy administration for enterprise environments. [10]

Features: Centralized user/group management, Kerberos authentication, Group Policy enforcement, domain trust relationships

Best Practices: Apply least privilege, structure OUs logically, clean up stale accounts, enable auditing

1.6.4 Certificate Authorities (CAs) & PKI

Certificate authorities establish digital trust by issuing and managing secure cryptographic certificates. [11]

Features: Certificate issuance for authentication, encryption, and signatures; supports SSL/TLS, S/MIME, code signing; integrates with AD CS

Best Practices: Secure root CA, protect keys with HSMs, renew/revoke certificates regularly, enforce strong cryptography, document PKI policies

TASK 2

2.1 Evidence of Download and installation

A Type 2 hypervisor is best when you need a simple, flexible way to run multiple operating systems on a personal computer. It allows easy software testing and exploration of new environments without rebooting or investing in extra hardware.

Would you like me to make this even more concise like a one-line tagline you could use in slides or notes?

2.1.1 Creation of Virtual machine Windows1 and 2

1. Download and Install VirtualBox

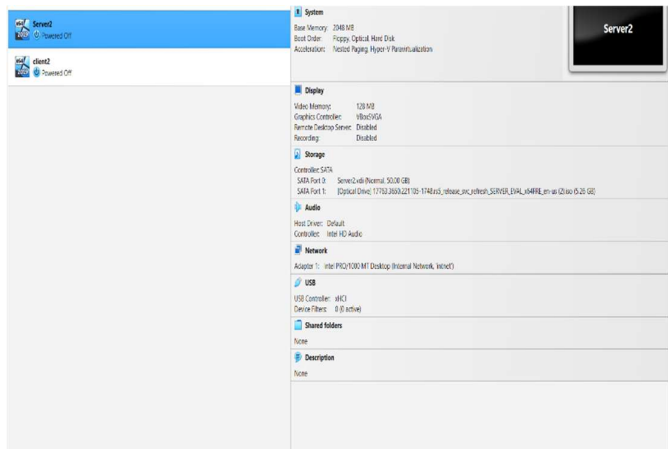
- Go to the [Oracle VirtualBox official site](#).
- Download the latest Windows installer.
- Run the setup file and follow the wizard.

2. Install Extension Pack (Optional but Recommended)

- Download the **VirtualBox Extension Pack** from the same site.
- Double-click the file to install it.

3. Create a New Virtual Machine

- Launch **VirtualBox Manager**.
- Click **New**, then enter a name (Windows 11).
- Choose the appropriate **operating system type** and **version** (Windows).



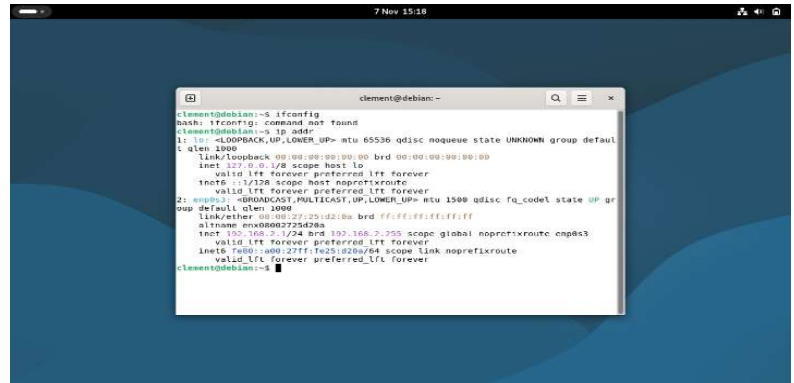
2.1.2 Creation of Virtual machine Linux Debian1 and 2

1 Install VirtualBox

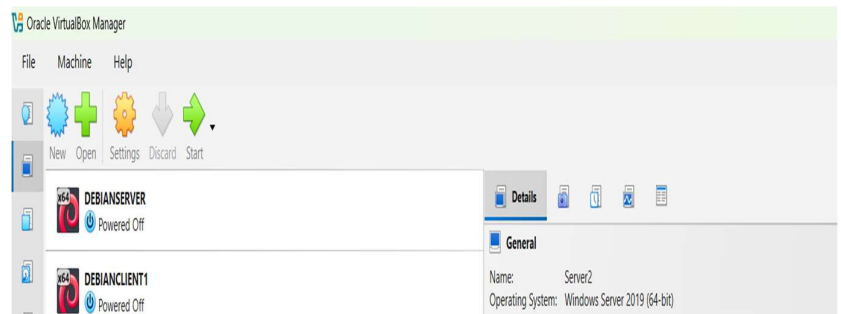
- Download VirtualBox from Oracle's official site.
- Install it on your system (Linux Debian server and Client).

Create a New Virtual Machine

1. Open VirtualBox and click New.
 2. Enter the following details:
- Name: Debian Server or Debian Client
 - Type: Linux

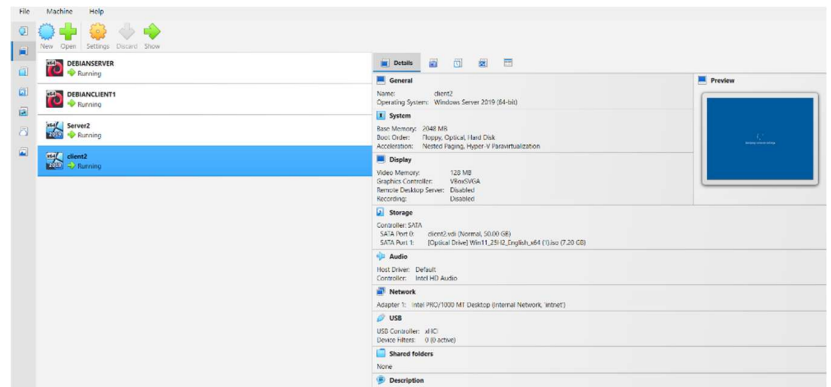


```
clement@debian:~$ ifconfig
bash: ifconfig: command not found
clement@debian:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP br
    default clem 1000
    link/ether 08:00:27:25:d2:0a brd ff:ff:ff:ff:ff:ff
    altname enx08002725d20a
    inet 192.168.2.1/24 brd 192.168.2.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::c000:27ff:fe25:d20a/64 scope Link noprefixroute
        valid_lft forever preferred_lft forever
```



2.1.3 Installation of Windows and Linux OS

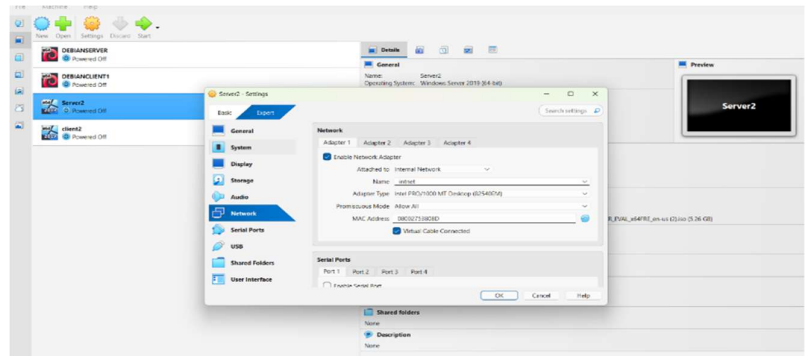
as you can see on the virtual box the 4 operations systems windows and Linux are installed and are running well



2.2 Deploy your network as per the given topology

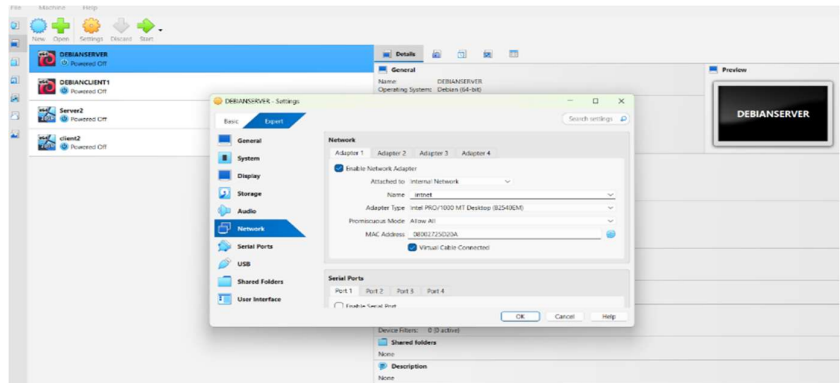
2.2.1 Creation of Network with NAT Network 1 for windows

Go to setting and click on Network
enable Network Adapter choose
Name: intnet promiscuous mode
Allow all



2.2,2 Creation of Network with NAT Network 2 for Linux

Setting-Network- enable Network
Adapter-Name intnet-
promiscuous mode allow all



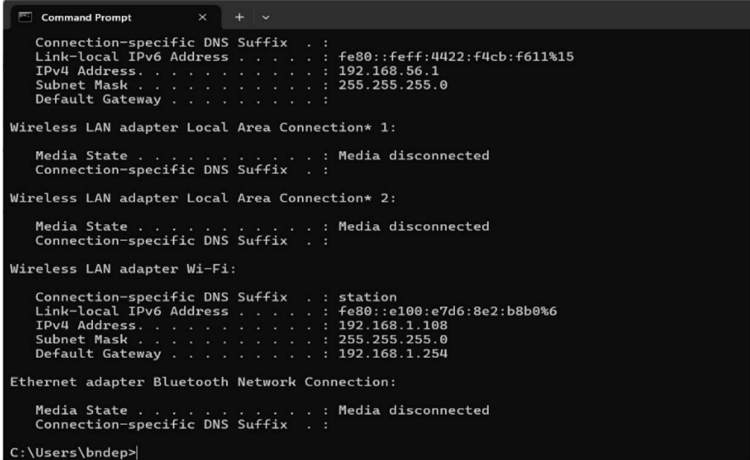
2.3 IP addressing

2.3.1 Windows Server and Windows Client

Windows Server IP address

192.168.1.1

Write in command prompt ipconfig then enter



```
Command Prompt
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::feff:4422:f4cb:f611%15
IPv4 Address. . . . . : 192.168.56.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 

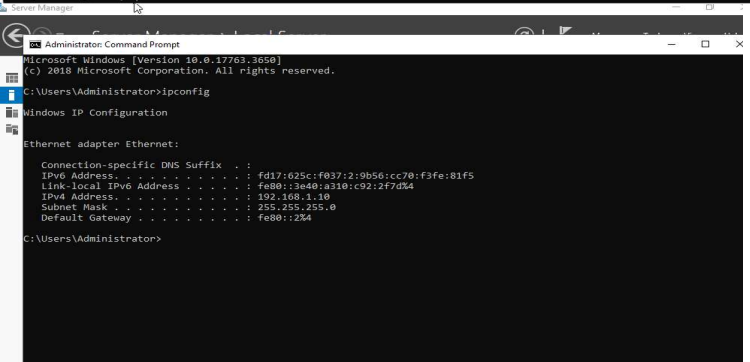
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : station
Link-local IPv6 Address . . . . . : fe80::e100:e7d6:8e2:b8b0%6
IPv4 Address. . . . . : 192.168.1.108
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.254

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 

C:\Users\bndep>
```



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : 
IPv6 Address. . . . . : fd17:025c:f037:2:0b56:cc70:f3fe:81f5
Link-local IPv6 Address . . . . . : fe80::3e40:a310:c92:2f7d%4
IPv4 Address. . . . . : 192.168.1.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::254

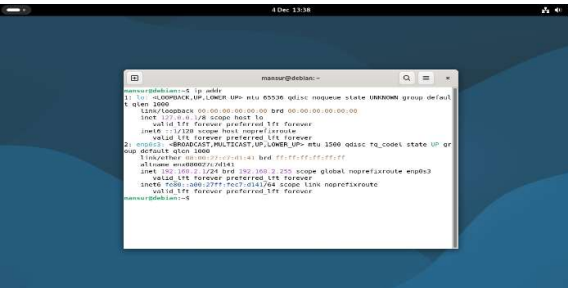
C:\Users\Administrator>
```

Windows Client IP address

192.168.1.1.10

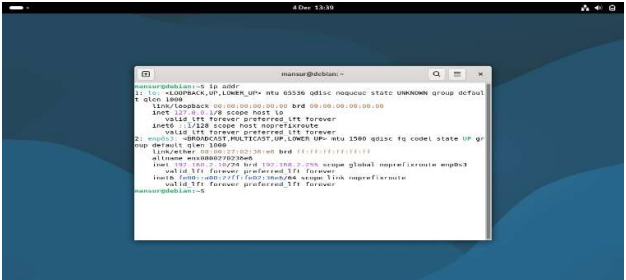
Write Ipconfig in command prompt then enter

2.3.2 Debian Server & Client



```
mamoo@debian:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link 0:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
    link/ether 08:00:27:00:00:00 brd ff:ff:ff:ff:ff:ff
    altname enx800270000
    inet 192.168.2.1/24 brd 192.168.2.255 scope global noprefixroute enp6b3
        valid_lft forever preferred_lft forever
    inet6 fe80::4002:7fff:fe00:0000 scope link noprefixroute
        valid_lft forever preferred_lft forever
mamoo@debian:~$
```

Debian Server 192.168.2.1

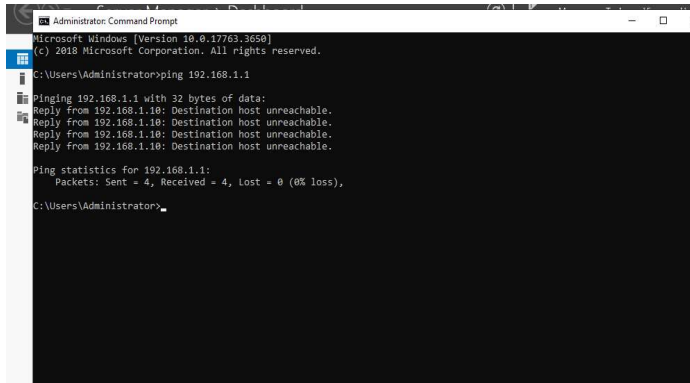


```
mamoo@debian:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link 0:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
    link/ether 08:00:27:00:00:00 brd ff:ff:ff:ff:ff:ff
    altname enx800270000
    inet 192.168.2.10/24 brd 192.168.2.255 scope global noprefixroute enp6b3
        valid_lft forever preferred_lft forever
    inet6 fe80::4002:7fff:fe00:0000 scope link noprefixroute
        valid_lft forever preferred_lft forever
mamoo@debian:~$
```

Debian Client 192.168.2,10

To find the IP address of Debian you should type Ip addr in command prompt

2.3.3 Successful connectivity within Windows network. (Ping 192.168.1.1 and Ping 192.168.1.10)



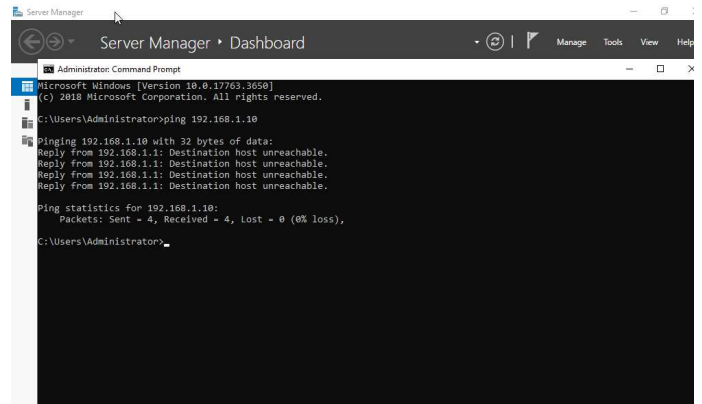
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Ping Windows sever 192.168.1,1 to Windows Client



```
Server Manager
Server Manager - Dashboard
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.1.10

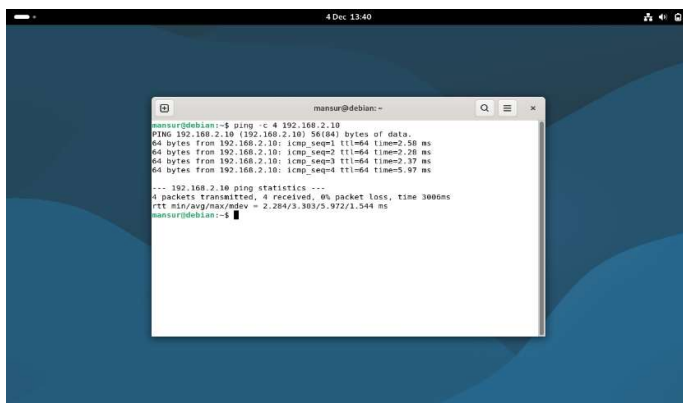
Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

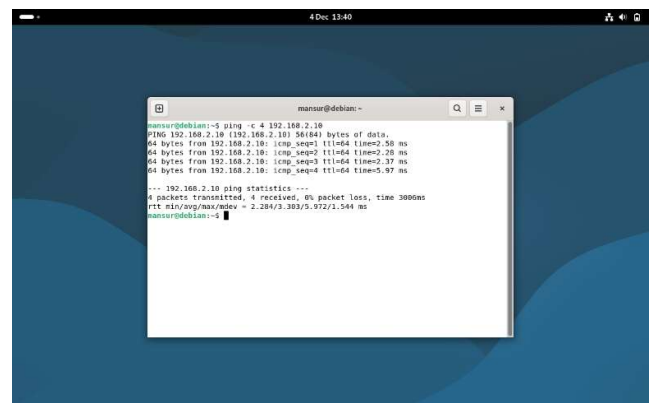
Ping Windows Client 192.168.1.10 to windows Server

Windows networks achieve seamless connectivity because all systems rely on common protocols, default firewall rules, unified authentication methods, and built-in discovery features, making communication nearly effortless.

2.3.4 Successful connectivity within Linux network. (Ping 192.168.2.1 and Ping 192.168.2.10)



```
mansur@debian:~$ ping -c 4 192.168.2.10
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data:
64 bytes from 192.168.2.10: icmp_seq=1 ttl=64 time=2.58 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=64 time=2.28 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=64 time=2.37 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=64 time=5.97 ms
--- 192.168.2.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 2.284/3.303/5.972/1.544 ms
mansur@debian:~$
```

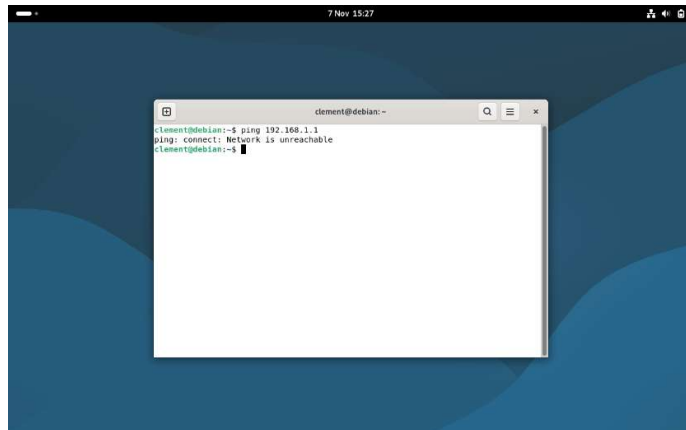


```
mansur@debian:~$ ping -c 4 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data:
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=2.58 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=2.28 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=2.37 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=64 time=5.97 ms
--- 192.168.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 2.284/3.303/5.972/1.544 ms
mansur@debian:~$
```

Linux systems connect successfully because they rely on open protocols, standardized tools, flexible configurations, and a unified kernel networking stack, ensuring reliable and predictable communication.

2.3.5 Unsuccessful connectivity between Linux and windows network

Connectivity issues between Linux and Windows often arise from firewall restrictions, protocol or service incompatibilities, incorrect IP or subnet configurations, authentication errors, or problems with virtualization and network adapters.



TASK 3

3- Technical Reflection covering network deployment and testing

Network deployment and testing often expose hidden complexities. IP conflicts highlight the need for structured address management, DNS issues emphasize the importance of reliable name resolution, and firewall misconfigurations remind us that security must balance accessibility. The reflection here underscores that resilient networks are built not only on strong design but also on careful validation, documentation, and continuous monitoring.

1 IP Address Conflicts

Issue: Duplicate IPs from poor static management or DHCP misconfiguration.

Impact: Connectivity loss, unstable ARP tables, time-consuming troubleshooting.

Resolution: Use DHCP scopes/reservations, maintain IPAM, and monitor conflicts proactively.

2 DNS Resolution Problems

Issue: Misconfigured servers, stale records, or delays in propagation.

Impact: Service access failures, broken dependencies (e.g., email, authentication).

Resolution: Validate DNS hierarchy, refresh caches, monitor with tools, and apply split-horizon DNS.

3 Firewall Configuration Challenges

Issue: Rules too restrictive block traffic; too permissive expose vulnerabilities.

Impact: Application communication failures weakened security posture.

Resolution: Apply least-privilege principles, document/test rules, monitor traffic, and automate deployments.

The deployment and testing phases must prioritize DNS resolution optimization, automated firewall configuration, and validation of stateful network functions to proactively address common issues that could undermine network performance and security. [12]

3.1 Personal reflection

Networking is a system of interdependencies where hypervisors enable virtualization, routing manages traffic, services provide functionality, connections ensure communication, deployment supports scalability, and IP addressing unifies it all. My experience across these areas highlighted the need for precision, planning, and adaptability to build reliable networks.

CONCLUSION

In conclusion, this assignment allowed us to explore and address questions related to hypervisors, routing, network services and connections, IP addressing, and deployment. However, certain practical challenges remain unresolved, such as establishing reliable connectivity between Debian and Windows systems

References

- [1] b. Jon, "bare-metal desktop hypervisor: A primer," Southborough Foundry, london, 2010.
- [2] P. M and Z. S. H. R. ichael, "Virtualisation: Issues, Security Threats and solution," *ACM computing Surveys*, vol. 45, pp. 1-39, 2013.
- [3] M. K. Tiwari, R. Pal, R. Singh, A. K. Singh, V. Kumar, S. Sharma and N. Zaib, "The Comprehensive Review: Internet Protocol (IP) Address a Primer for Digital Connectivity," *Asian Journal of Research in Computer Science*, vol. 17, no. 8, pp. .34-45, 2024.
- [4] N. Sahana and U. R. K R, "Design of Intelligent IP Address Management System for Communication Networks," in *11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, london, 2020.
- [5] M. Jothilakshmi, M. K. Pavithra and S. Yuvabarathi, "Performance Comparison between IPV4 AND IPV6," *International Journal of Science, Engineering and Computer Technology.*, vol. 4, no. 12, pp. 384-384, 2014.
- [6] A. S. Ismail, X. Wang, A. Hawbani, S. Alsamhi and S. Abdel Aziz, "Routing protocols classification for underwater wireless sensor networks based on localization and mobility," *Wireless networks*, vol. 28, no. 2, pp. 797-826, 2022.
- [7] Debian, "Debian Manpage".
- [8] A. Maulidi, M. Abdullah and D. Handani, "Virtual private network (VPN) model for AIS real time monitoring," *IOP conference series. Earth and environmental science*, vol. 1081, no. 1, p. 12028, 2022.
- [9] V. A. B. Scott and S. A. Giancarlo, "Designing the VPN with Top-Down to Improve Information Security," *Science and Information (SAI) Organization Limited; International journal of advanced computer science & applications*, vol. 15, no. 6, 2024.
- [10] N. Weinberg, "DHCP defined and how it works," *Network World*, 2022.
- [11] P. A. Kadam, S. Bhushan, V. Rishiwal, M. Yadav, P. Yadav and U. Agarwal, "ValidCertify: an effective blockchain-based domain certificate authentication and verification scheme," *Peer-to-peer networking and applications*, vol. 18, no. 4, p. 177, 2025.
- [12] D. Ranathunga, M. Roughan, H. Nguyen, P. Kernick and N. Falkner, "Case Studies of SCADA Firewall Configurations and the Implications for Best Practices," *IEEE; IEEE eTransactions on network and service management*, vol. 13, no. 4, pp. 871-884, 2016.

