



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

Assessment Title:

Research, build, and deploy a Virtualised Enterprise network.

Applied Computing.

Network Operating Systems and Services.
ACCA5023.

Dr. Sadeque Imam Shaikh (Lecturer)

University of Wales Trinity Saint David

(London Campus)

Student Name: Mauricio Honorato Acordi

Student Number: 2429788

Group: 01

Team: 01

Date: 25/03/2026

Table of Contents

Task 1	1
Introduction	1
Research on Hypervisor.....	1
Research on IP Addressing:.....	2
1.1.1 Diagram: IP Addressing & VLSM Example for Topology	2
Research on Routing	2
Research on Network Services:	3
Task 2	3
2.1. Choose your Hypervisor:.....	3
2.2. Download and Setup:.....	4
2.2.1 Evidence of Download and installation.	4
1.1.2 Creation of virtual machine Windows 1 e 2.....	4
2.2.2 Deploy your network as per the given topology:	7
2.2.3 IP addressing :.....	10
2.3. Configure IP Addressing	10
2.3.1. Use appropriate IP addresses to configure your network.	10
2.3.2. The above topology gives network address for the networks	11
2.4. Test and Troubleshoot.....	13
Task 3	14
3.1.1. Technical Reflection	14
3.1.2. Personal Reflection	14
References	15

Task 1

Introduction

The rapid evolution of enterprise IT infrastructure has made virtualisation one of the most essential technologies in modern network design [1]. By allowing multiple operating systems and services to run efficiently on shared hardware, virtualisation provides organisations with improved resource utilisation, scalability, flexibility, and cost-effectiveness. This coursework represents the first stage of a multi-site enterprise network project, simulating the connection between the Birmingham and London offices of the organisation used as the case study for this assessment.

This report begins by examining key theoretical concepts underpinning the solution, including different types of hypervisors and their architectural characteristics, IPv4 addressing and subnetting techniques, routing principles (with emphasis on static versus dynamic approaches), and essential network services such as DHCP, Active Directory Domain Services, VPNs, and Certificate Authorities. These elements are critically analysed in relation to their suitability for the proposed topology.

The second part of the report provides detailed technical documentation of the practical implementation. Using Oracle VirtualBox as the chosen hypervisor, four virtual machines were created and configured to replicate the required network segments: the Birmingham LAN, the London LAN, and the simulated WAN link. Finally, a reflection section evaluates both the technical challenges encountered and the personal learning outcomes gained throughout the project.

Research on Hypervisor

Virtualisation is a key component of modern IT infrastructure, allowing multiple operating systems to run on a single physical machine by abstracting hardware resources. This is made possible by a hypervisor, which manages virtual machines (VMs) and distributes system resources [2].

Type 1 hypervisors, also known as bare-metal hypervisors, run directly on the physical hardware without a host operating system. This direct interaction results in better performance, lower latency, and stronger security between VMs [3]. They are commonly used in enterprise environments and data centres. For a complex production setup that includes a Windows Server 2022 Domain Controller with multiple roles and a Debian server, a Type 1 hypervisor (like VMware ESXi or Microsoft Hyper-V) would provide a stable and efficient production environment.

In contrast, Type 2 hypervisors run on top of an existing operating system as applications. Although they introduce some performance overhead, they are easier to install and more suitable for personal, testing, or educational use [4]. For this specific topology and hardware constraints, Oracle VirtualBox (Type 2) is the most appropriate choice. It allows multiple VMs to run on standard student hardware, supports both Windows and Linux systems, and provides flexible networking options (such as NAT Networks and Internal Networks) to simulate different subnets and routing securely [5].

Research on IP Addressing:

IP addressing is the core system that allows devices to communicate across networks by providing each device with a unique logical address [6]. IPv4 uses a 32-bit address format written in dotted-decimal notation, allowing around 4.3 billion unique addresses. Each address is divided into a network and host portion, defined by a subnet mask.

Subnetting is used to divide larger networks into smaller segments, improving performance and security by reducing broadcast traffic. Variable Length Subnet Masking (VLSM) allows networks to use different subnet sizes within the same address range, making more efficient use of available IP addresses [7].

IPv6 was introduced to overcome the limitations of IPv4, using a 128-bit address written in hexadecimal format, providing an extremely large number of unique addresses alongside built-in IPsec security [8]. Routers facilitate the flow of data between these different IP networks by reading the destination IP and determining the best path.

1.1.1 Diagram: IP Addressing & VLSM Example for Topology

Machine	OS	Ipaddress	Network
Server01	Windows Server2019	192.168.100.10/24	Birmingham
Client01	Windows 10 Pro	192.168.100.20/24	Birmingham
DebianServer	Debian 13	192.168.200.10/24	London
DebianClient	Debian 13	192.168.200.20/24	London

Table 1: Topology

IPv6 was introduced to overcome the limitations of IPv4, using a 128-bit address written in hexadecimal format, providing an extremely large number of unique addresses alongside built-in IPsec security (Tanenbaum & Wetherall, 2011). Routers facilitate the flow of data between these different IP networks by reading the destination IP and determining the best path.

Research on Routing

Routing is the process by which network devices determine the best path for data to travel between different networks [9]. Routing protocols share information about network structure and update routing tables. These are generally divided into Interior Gateway Protocols (IGPs), like OSPF and RIP, which operate within a single autonomous system, and Exterior Gateway Protocols (EGPs), like BGP.

Routing can be configured statically or dynamically. Static routing involves manually adding routes to a routing table, giving the administrator full control with low processing overhead, making it ideal for small, stable networks [10]. Dynamic routing automatically updates routes based on network changes, which is useful in larger environments.

In this topology, featuring only two local subnets (Birmingham and London) and a single point-to-point connection between sites, static routing is the most suitable approach. It avoids the unnecessary complexity and broadcast overhead of dynamic protocols. To support the Debian Server's future role as a DHCP Relay, routing must be accurately configured so unicast DHCP requests can traverse the 10.0.0.0/30 network to reach the Windows Domain Controller.

Research on Network Services:

DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses and network settings (gateways, DNS) to clients, preventing IP conflicts and administrative overhead. In advanced configurations, a DHCP Relay Agent is required to forward broadcast DHCPDISCOVER packets across router boundaries to a central DHCP server [11].

Active Directory Domain Services (AD DS) provides a hierarchical directory service for managing users, computers, and security policies centrally. Integrating tightly with DNS, AD DS is critical for structural organisation and authentication in the Birmingham network [12].

VPNs (Virtual Private Networks)) create secure, encrypted tunnels over public networks (like the simulated internet in this topology), ensuring data confidentiality and integrity for site-to-site communication [13].

Certificate Authorities (CAs) issue digital certificates within a Public Key Infrastructure (PKI). They authenticate the identity of servers and devices, enabling secure protocols like HTTPS and encrypted VPN tunnels to function securely across the enterprise [13].

Task 2

2.1. Choose your Hypervisor:

Based on the research conducted, Oracle VirtualBox 7.x was selected as the hypervisor [14]. This choice is supported by its compatibility with both Windows Server 2019 and Debian 13 without requiring enterprise-grade physical hardware. Furthermore, VirtualBox provides flexible isolated networking features (NAT Network and Internal Network adapters) necessary to accurately simulate the Birmingham and London subnets and the intermediary WAN link for Coursework 2.

2.2. Download and Setup:

2.2.1 Evidence of Download and installation.

1.1.2 Creation of virtual machine Windows 1 e 2

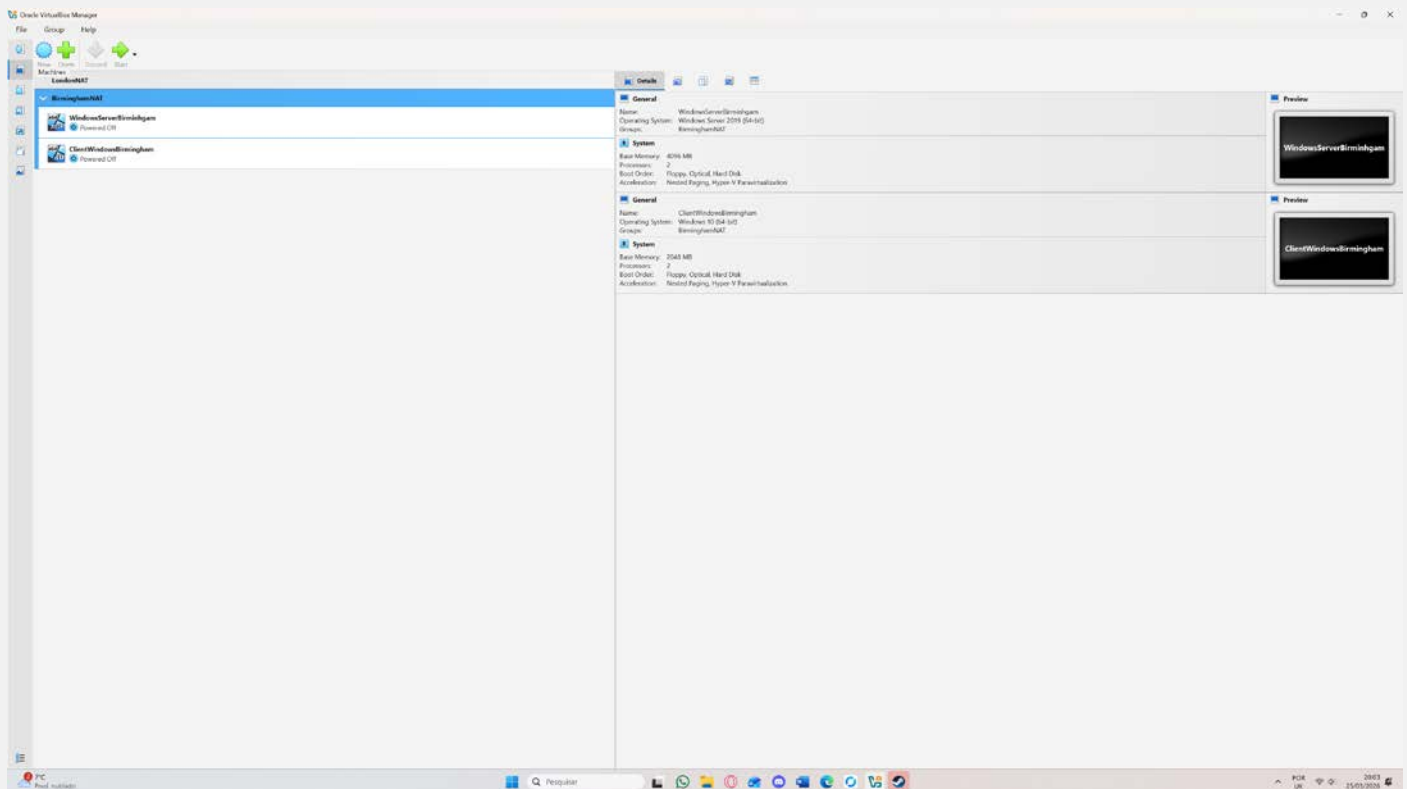


Figure 1: For Birmingham Windowsserver2019 & windows10 Client Virtualmachines are created.

1. Creation of Virtual machine Linux Debian 1 and 2(1 screenshot)

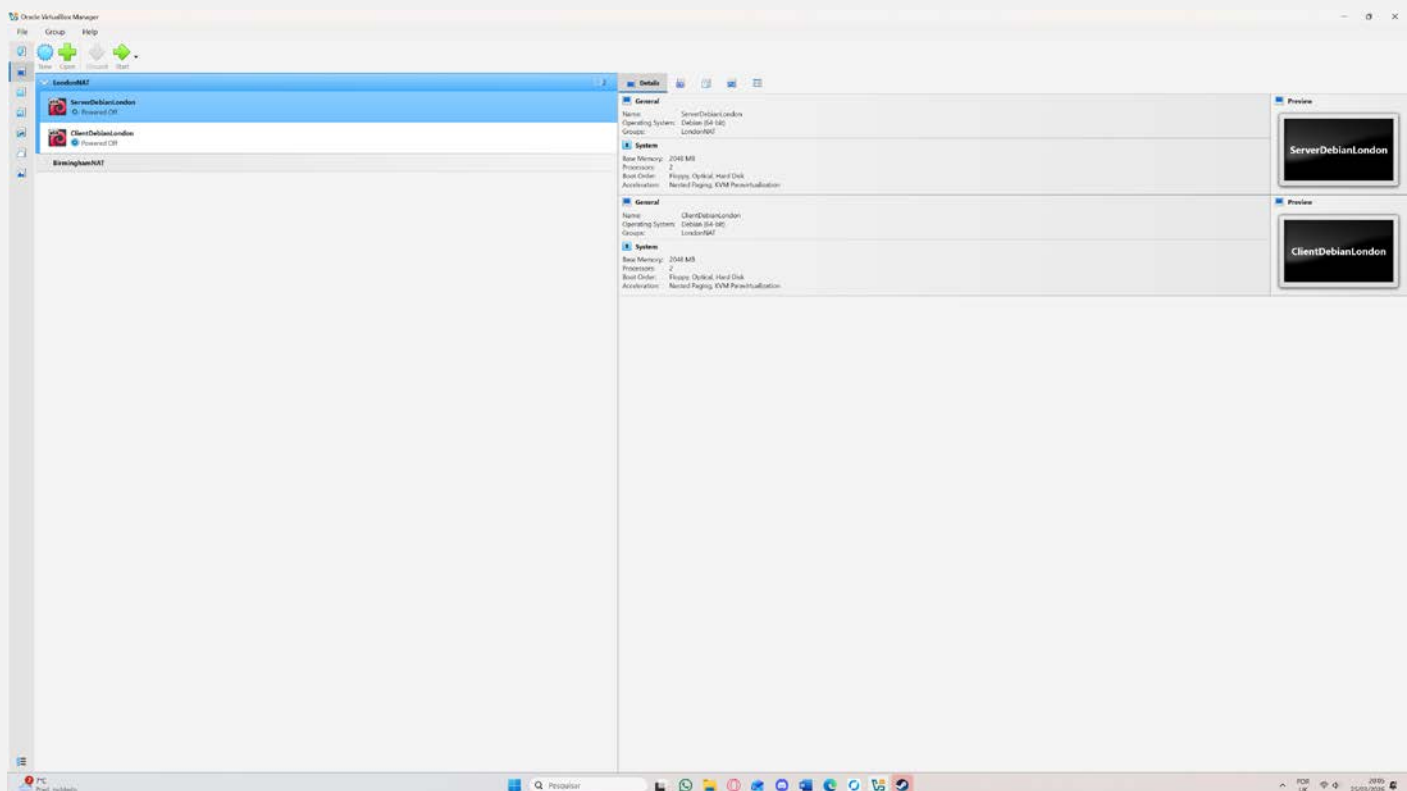


Figure 2: For London Debian Server & Client Virtualbox are created.

2. Installation of windows and Linux OS (Start 4 Machines and take desktop screenshots) (4 screenshots)

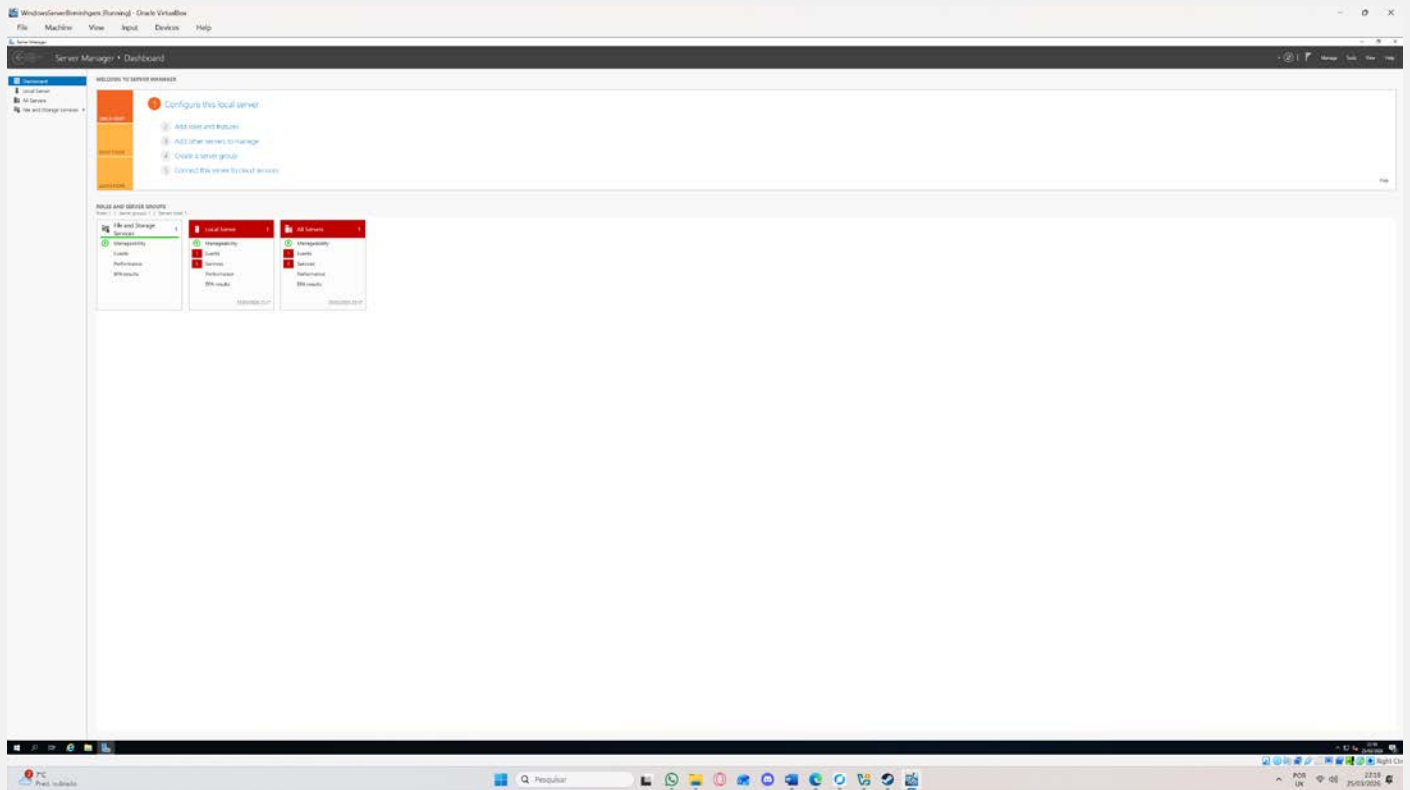


Figure 3: Windows 2019 Server Installed.

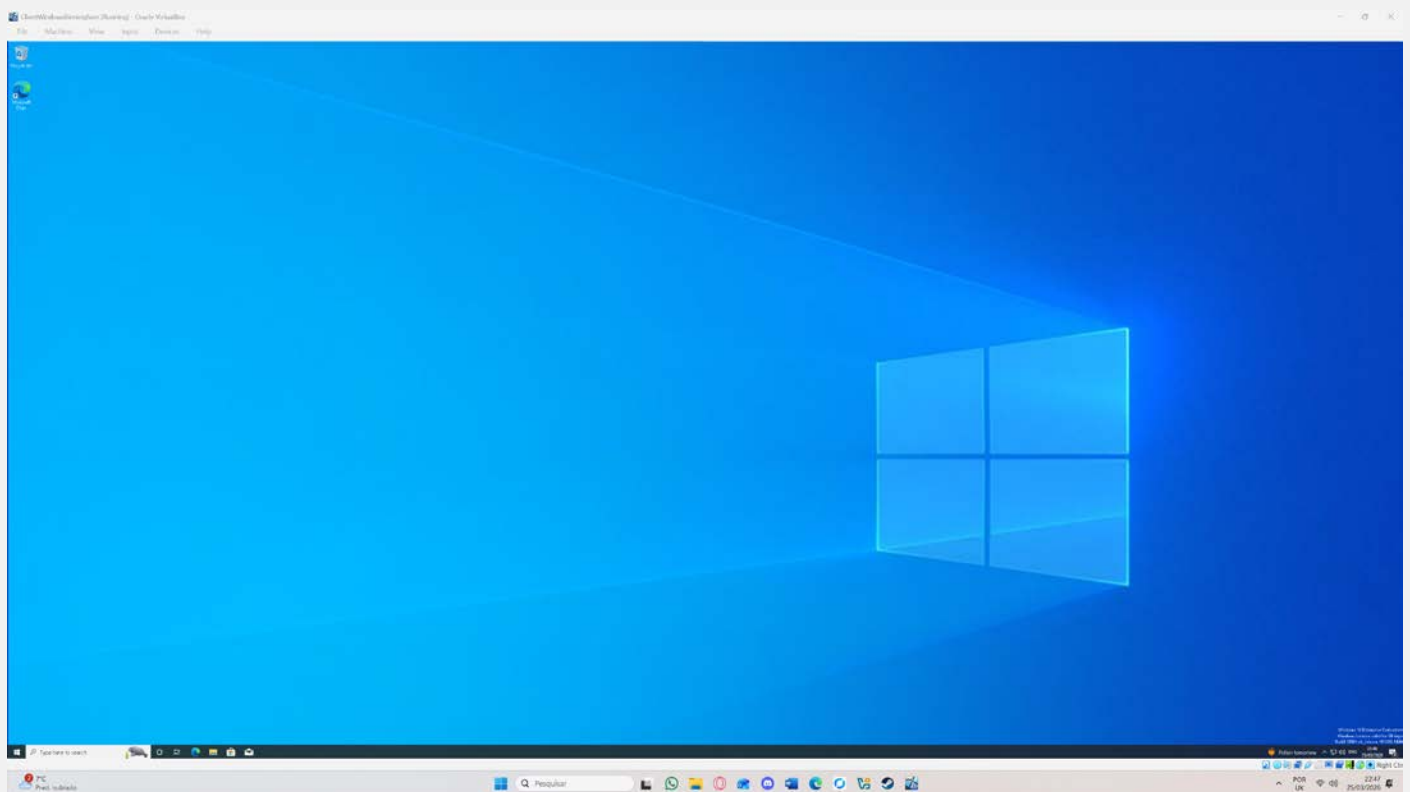


Figure 4: Windows 10 Client Installed

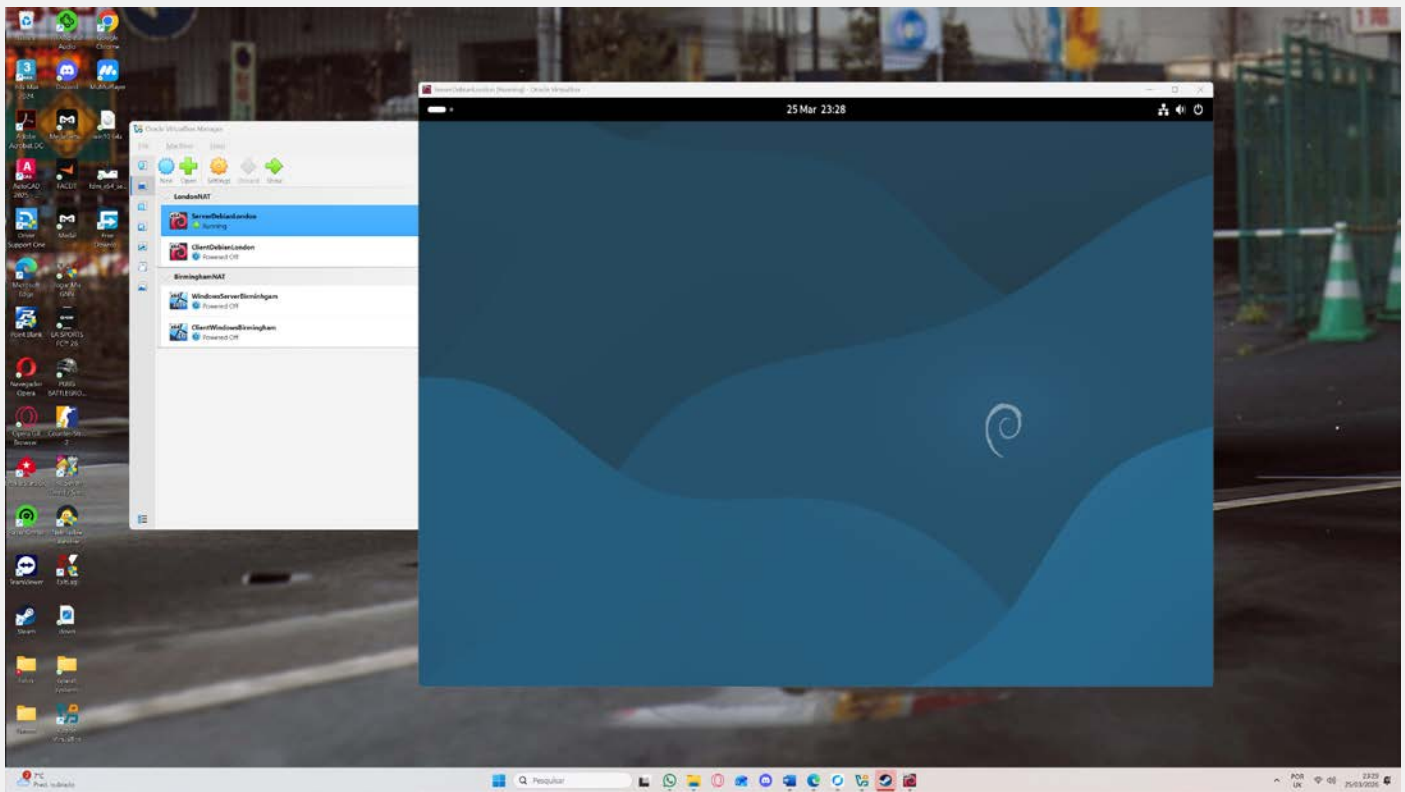


Figure 5: Linux Debian Server Installed.

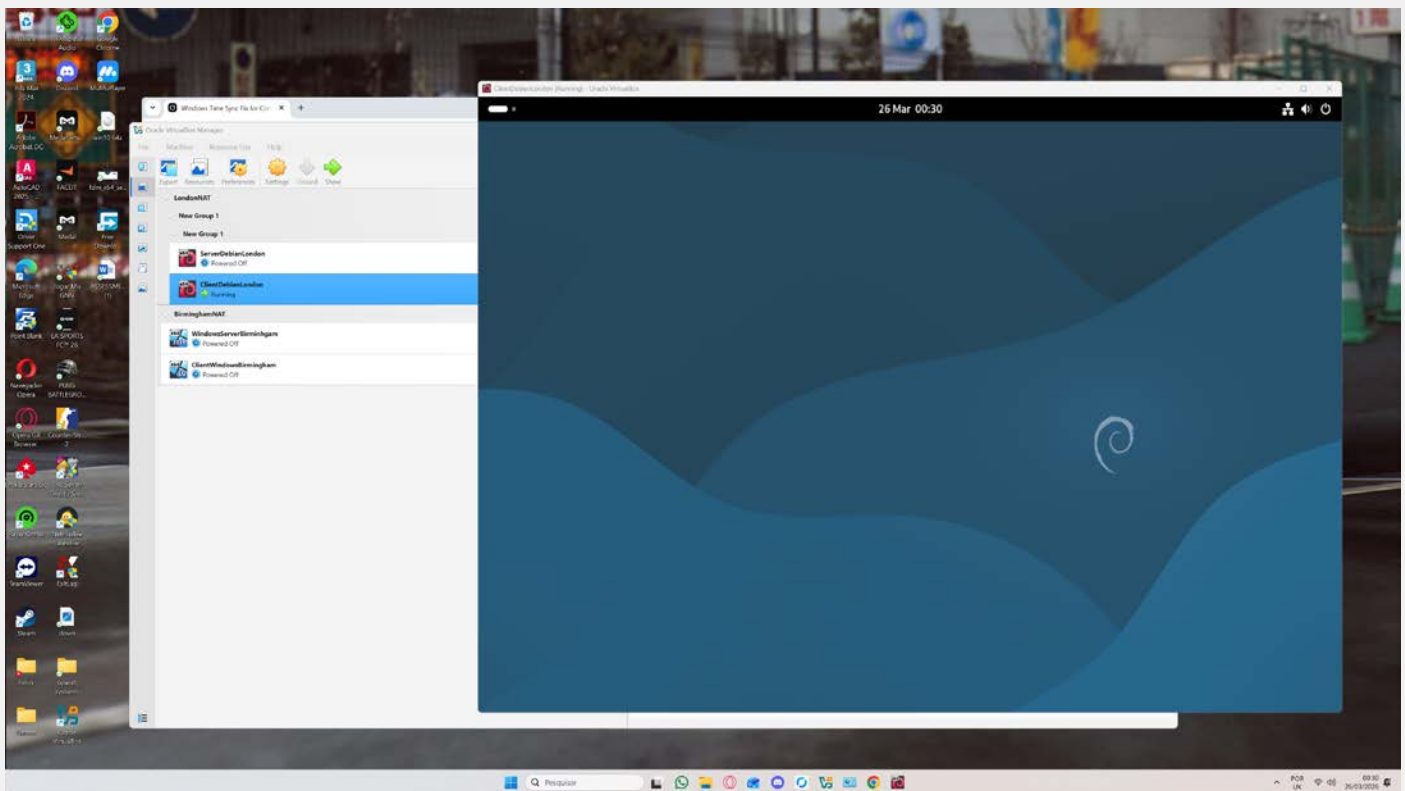


Figure 6: Linux Debian Client Installed.

2.2.2 Deploy your network as per the given topology:

1. Creation of Network with NAT Network1 for windows (1 screenshot)

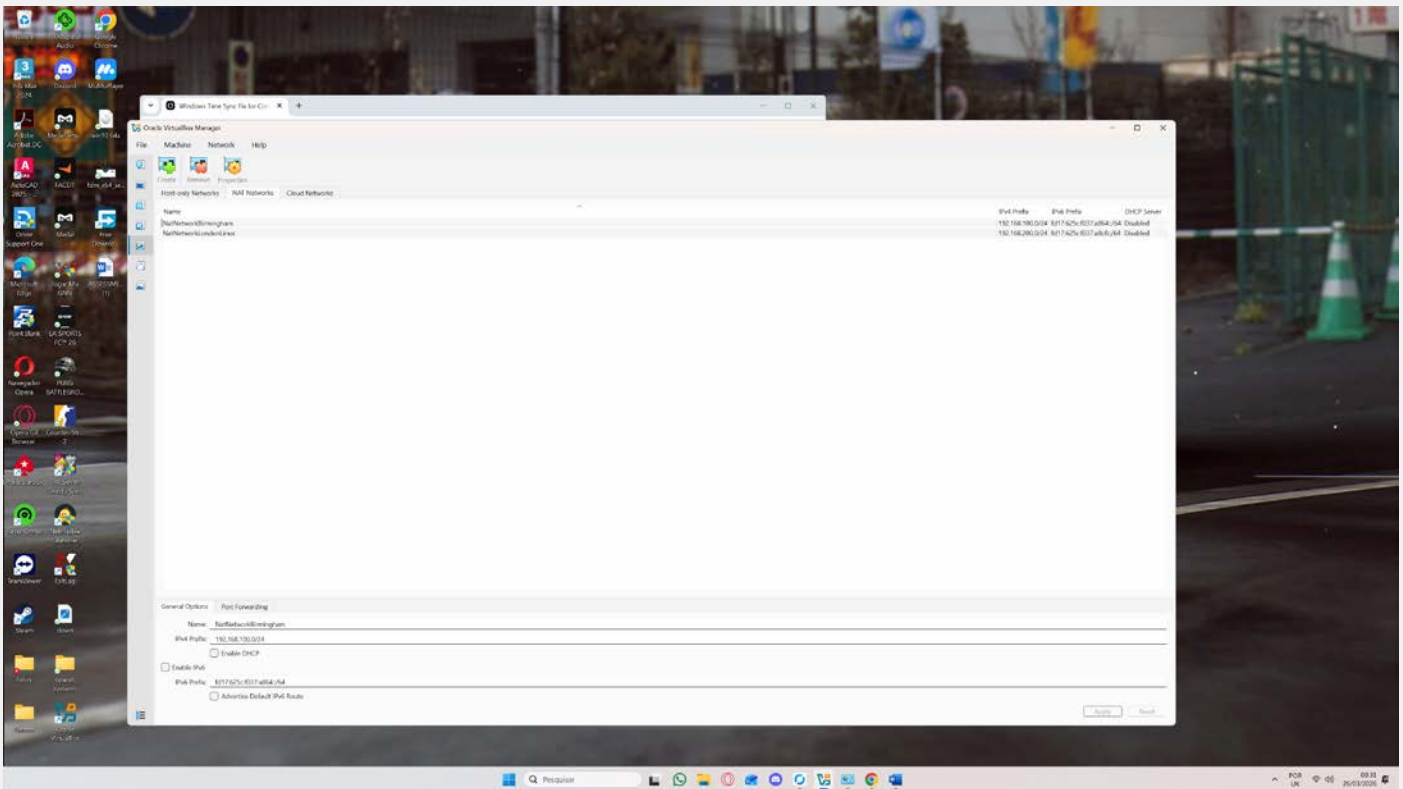


Figure 7: NAT Config for Birmingham Windows.

2. Creation of Network with NAT Network 2 for Linux (1 screenshot)

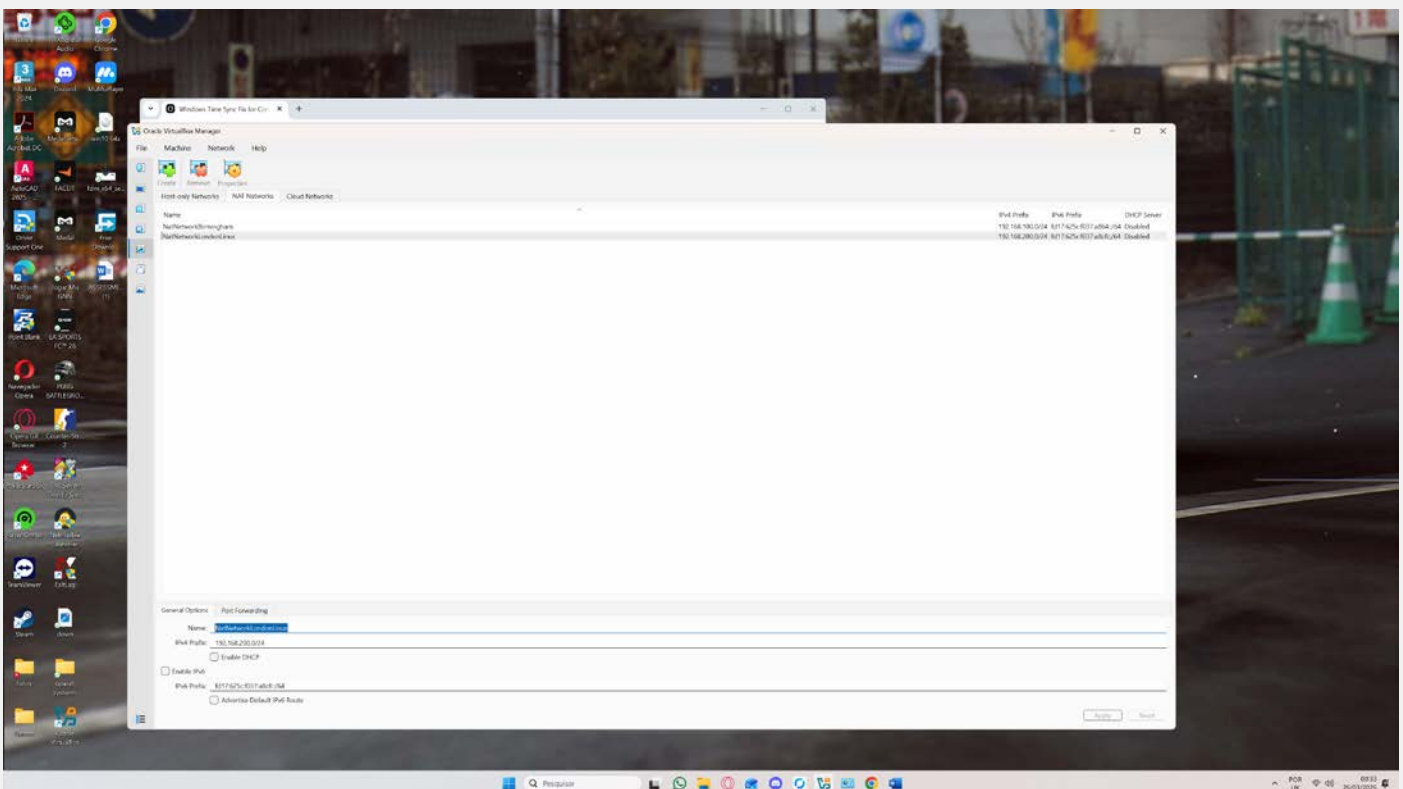


Figure 8: NAT Config for London Linux.

3. Evidence of 2 Windows PCs are connected with NAT Network1 (2 screenshot)

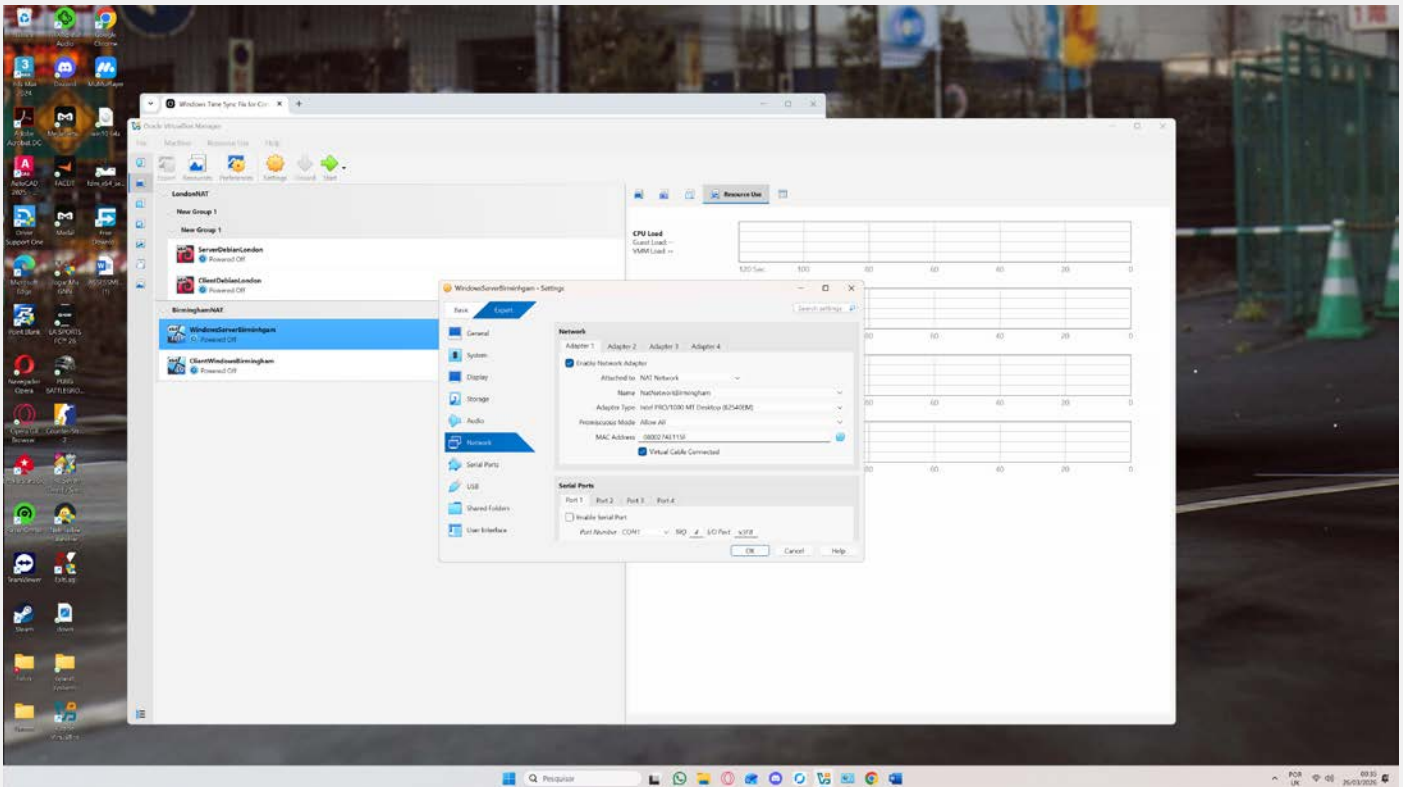


Figure 9: Windows Server config to Birmingham network.

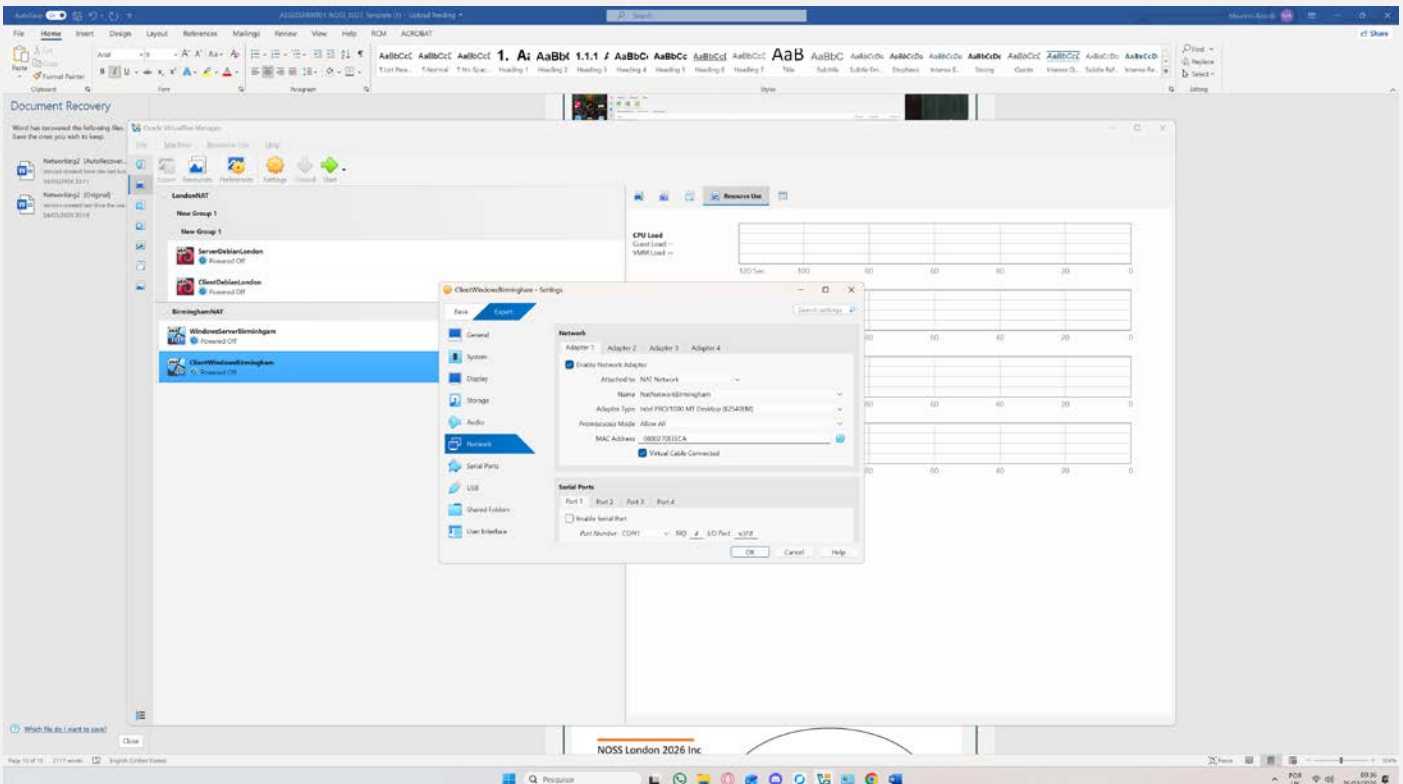


Figure 10: Windows Client config to Birmingham Network.

4. Evidence of 2 Linux PCs are connected with NAT Network2 (2 screenshot)

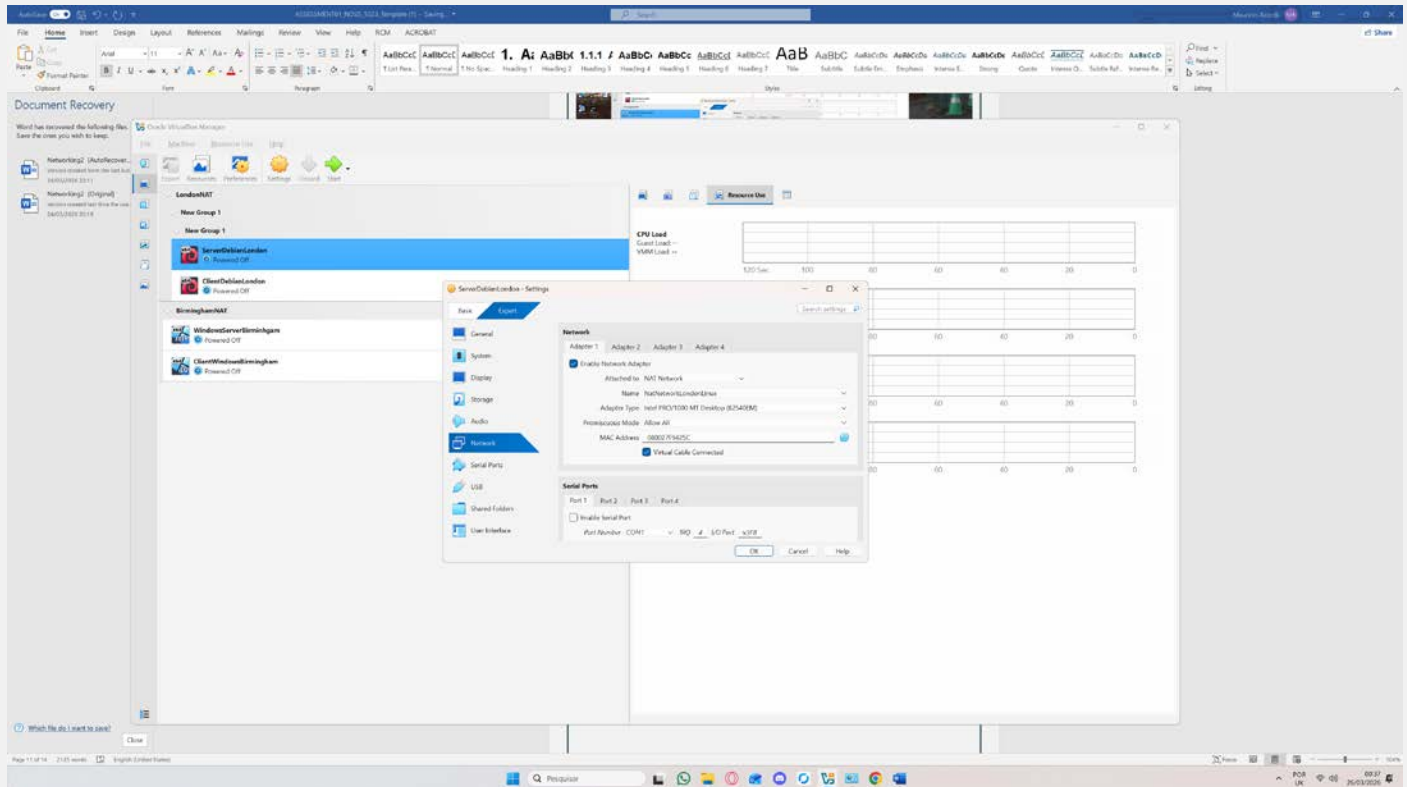


Figure 11: Linux Server config London Network.

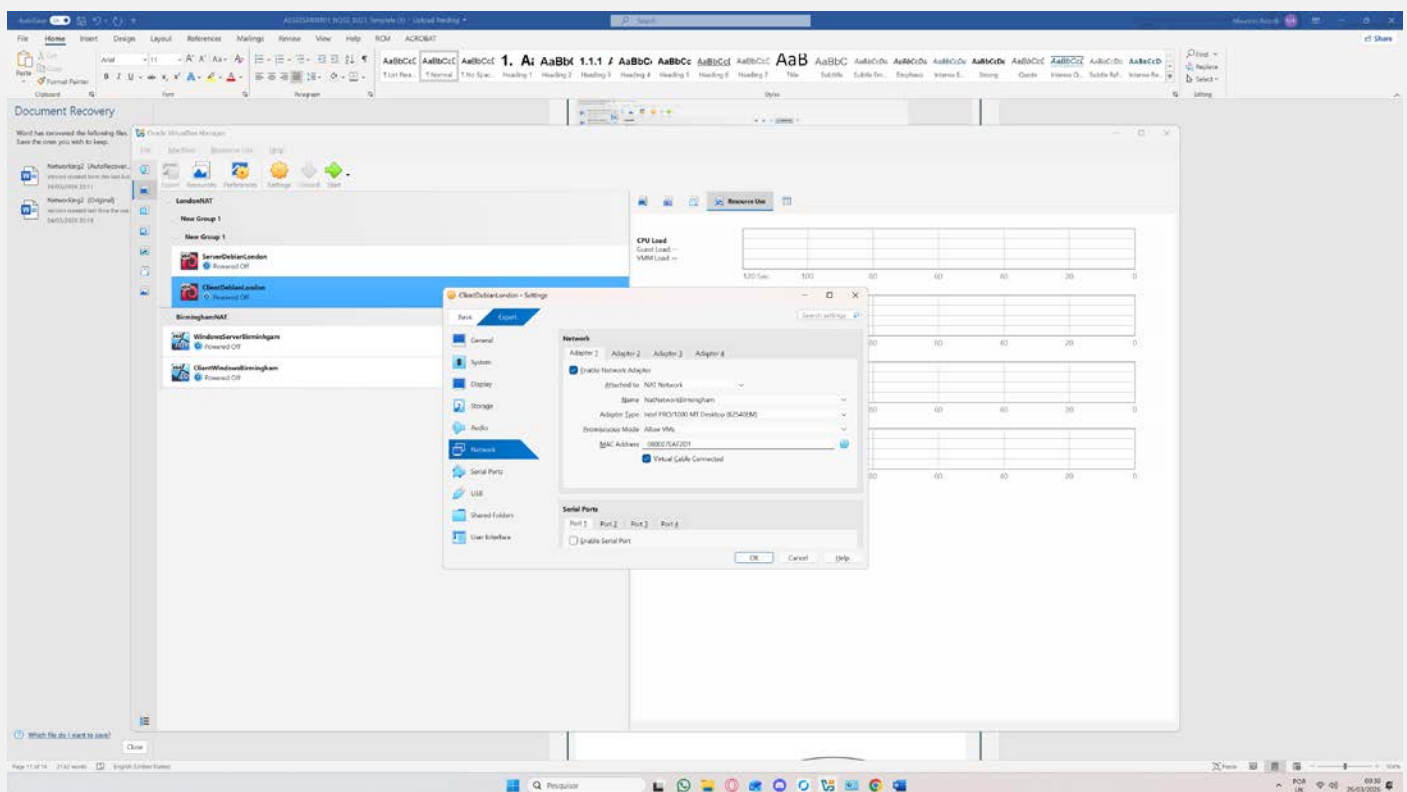


Figure 12: Linux Client config London Network.

2.2.3 IP addressing :

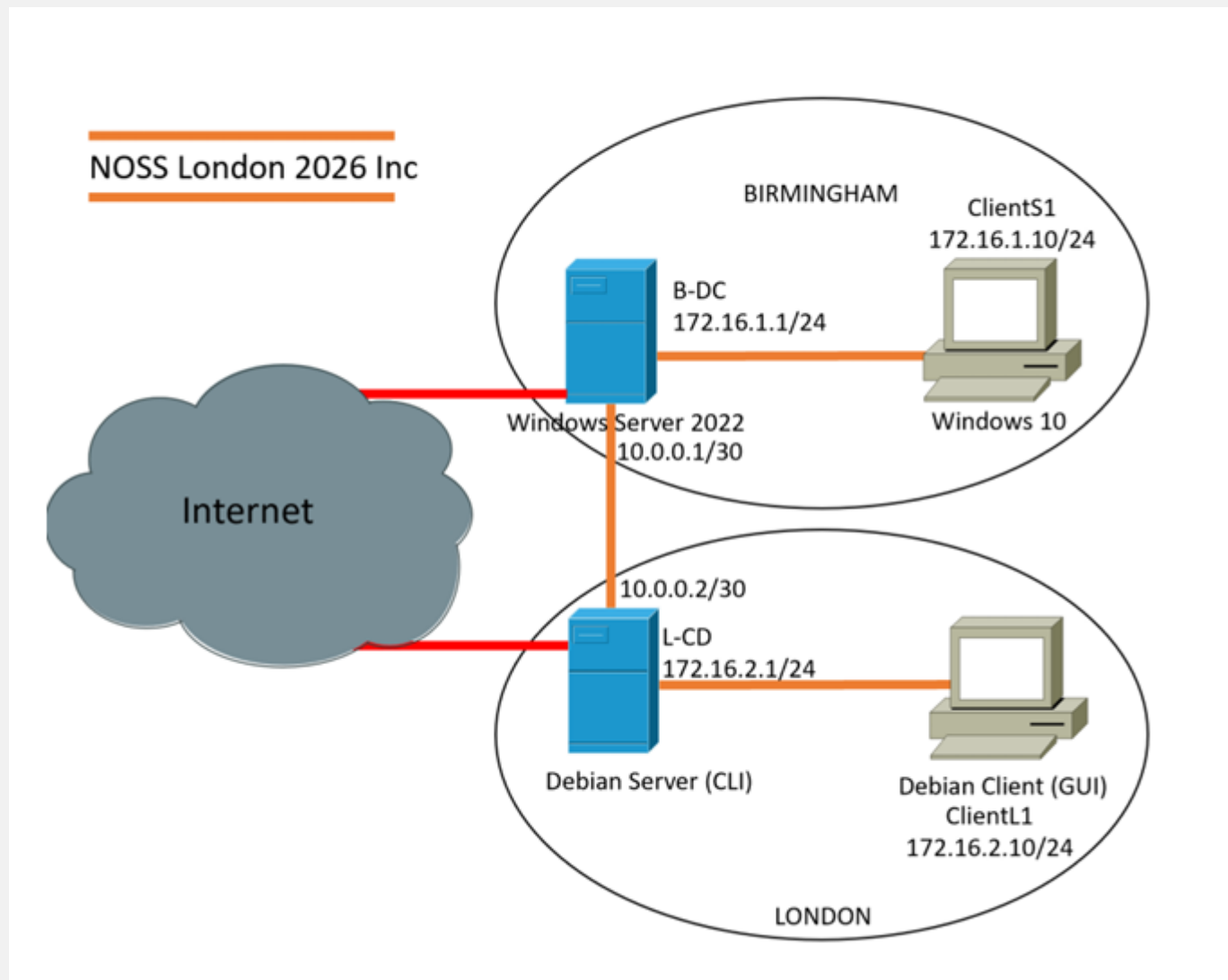


Figure 13

Machine	OS	Ipaddress	Network
Server01	Windows Server2019	192.168.100.10/24	Birmingham
Client01	Windows 10 Pro	192.168.100.20/24	Birmingham
DebianServer	Debian 13	192.168.200.10/24	London
DebianClient	Debian 13	192.168.200.20/24	London

Table 1

2.3. Configure IP Addressing

2.3.1. Use appropriate IP addresses to configure your network.

1. Evidence of IP addresses set up in 2 Windows and 2 Linux machine(for windows command is ipconfig and for Linux use the command ip add show)

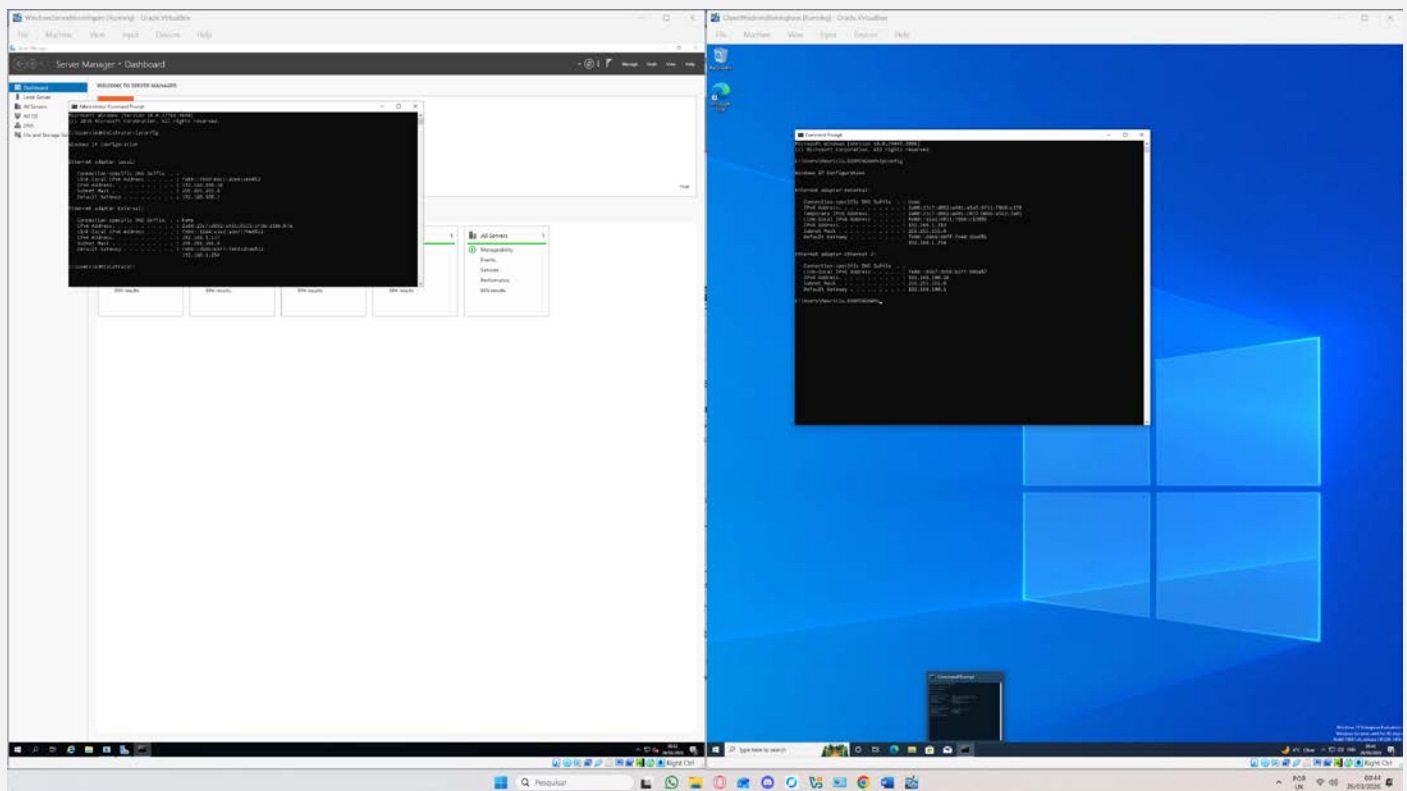


Figure 14: Windows Server and Client Networking configuration.

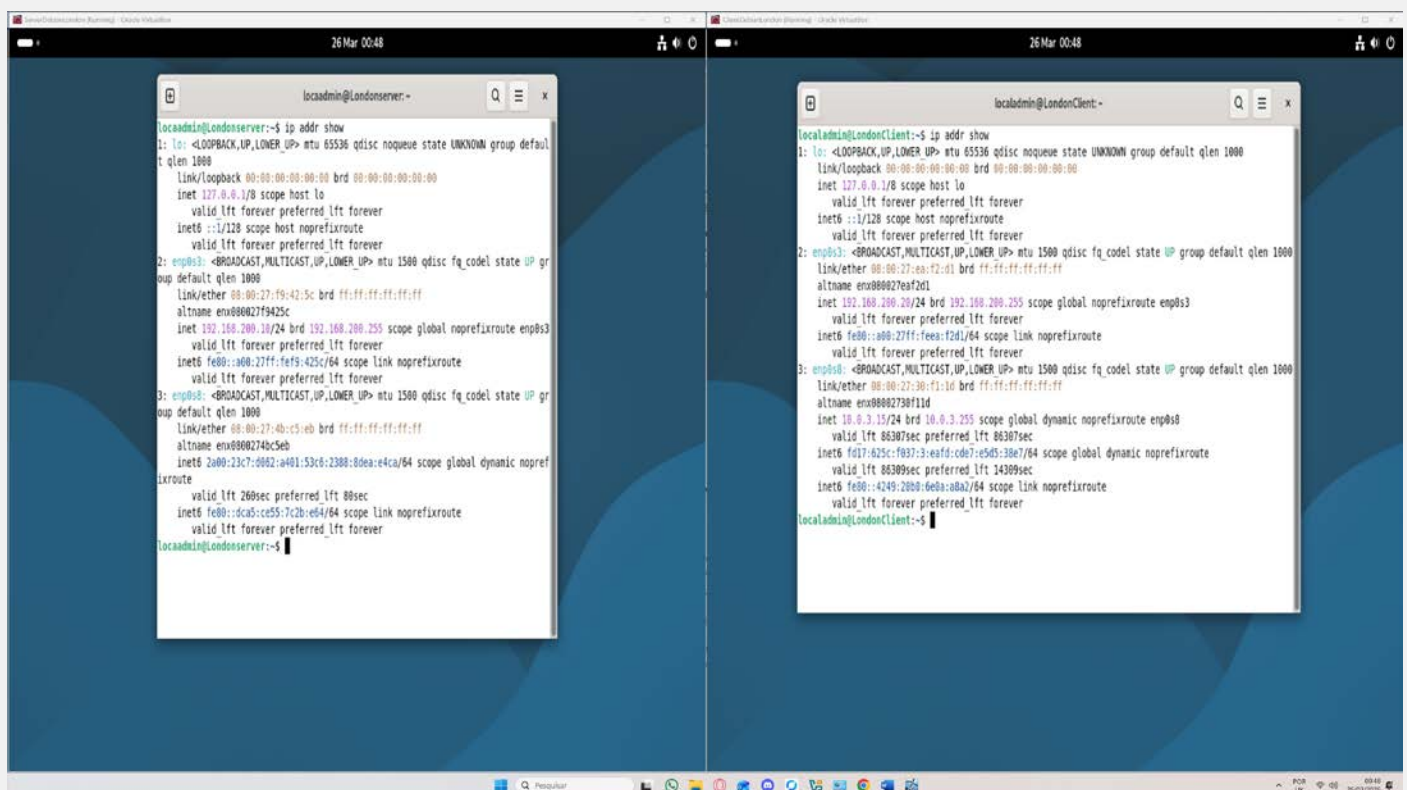


Figure 15: Linux Server and Client Networking configuration.

2.3.2. The above topology gives network address for the networks

1. Network IP address from NAT Network1 for windows.

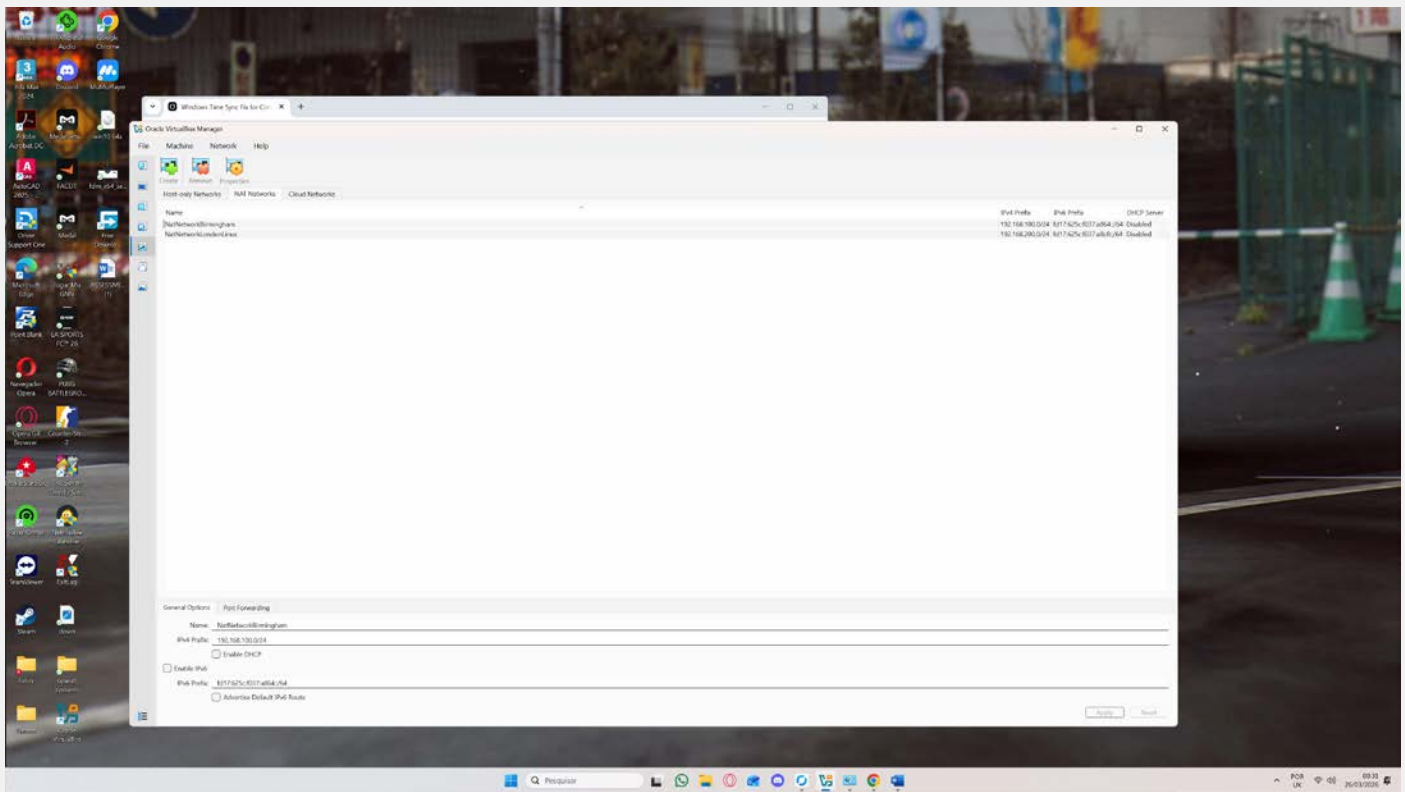


Figure 16: NAT Config for Birmingham Windows.

2. Network IP address from NAT Network 2 for Linux

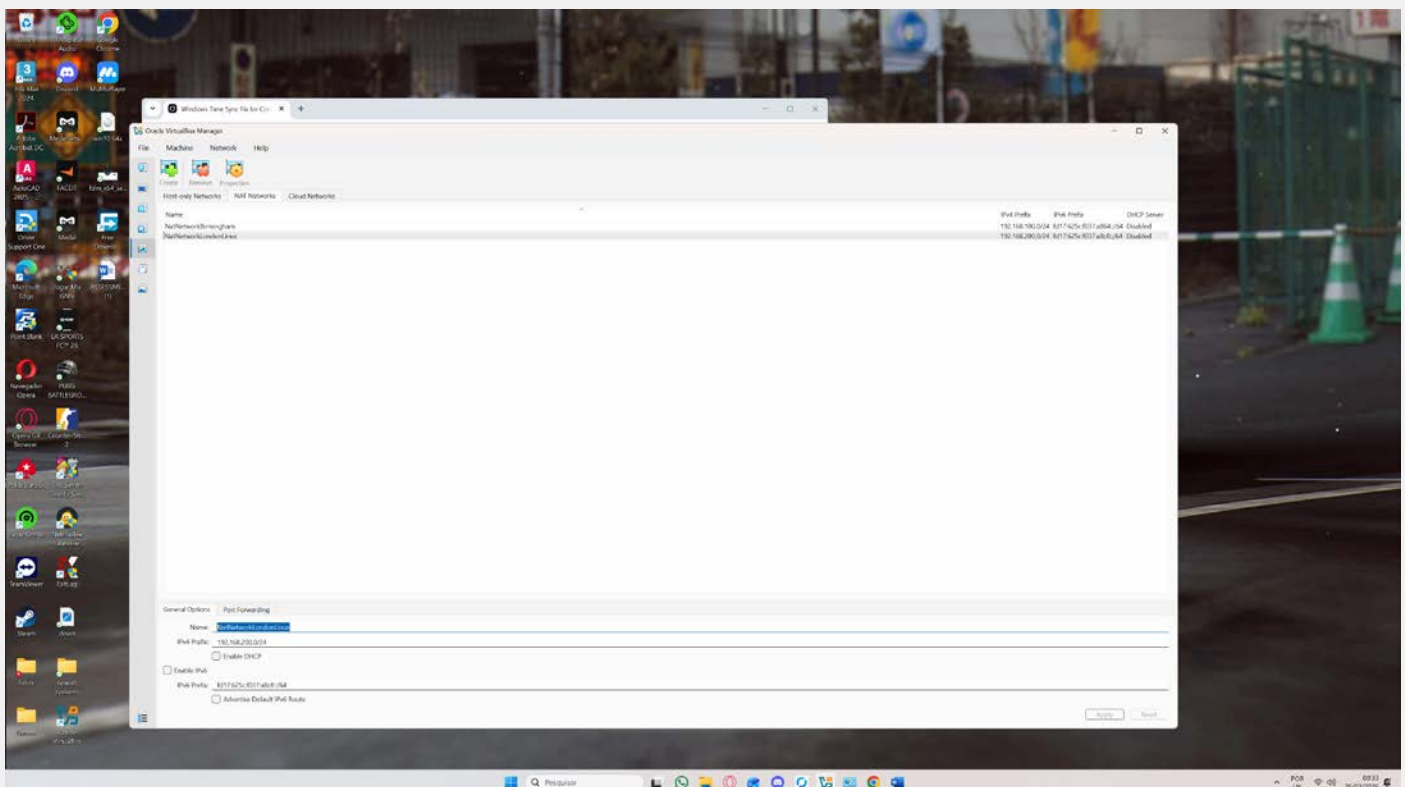


Figure 17: NAT Config for London Linux.

2.4. Test and Troubleshoot

2.4.1. Perform Connectivity tests

1. Outcome 1: Successful connectivity within windows network.(Ping 192.168.100.10 and Ping 192.168.100.20)

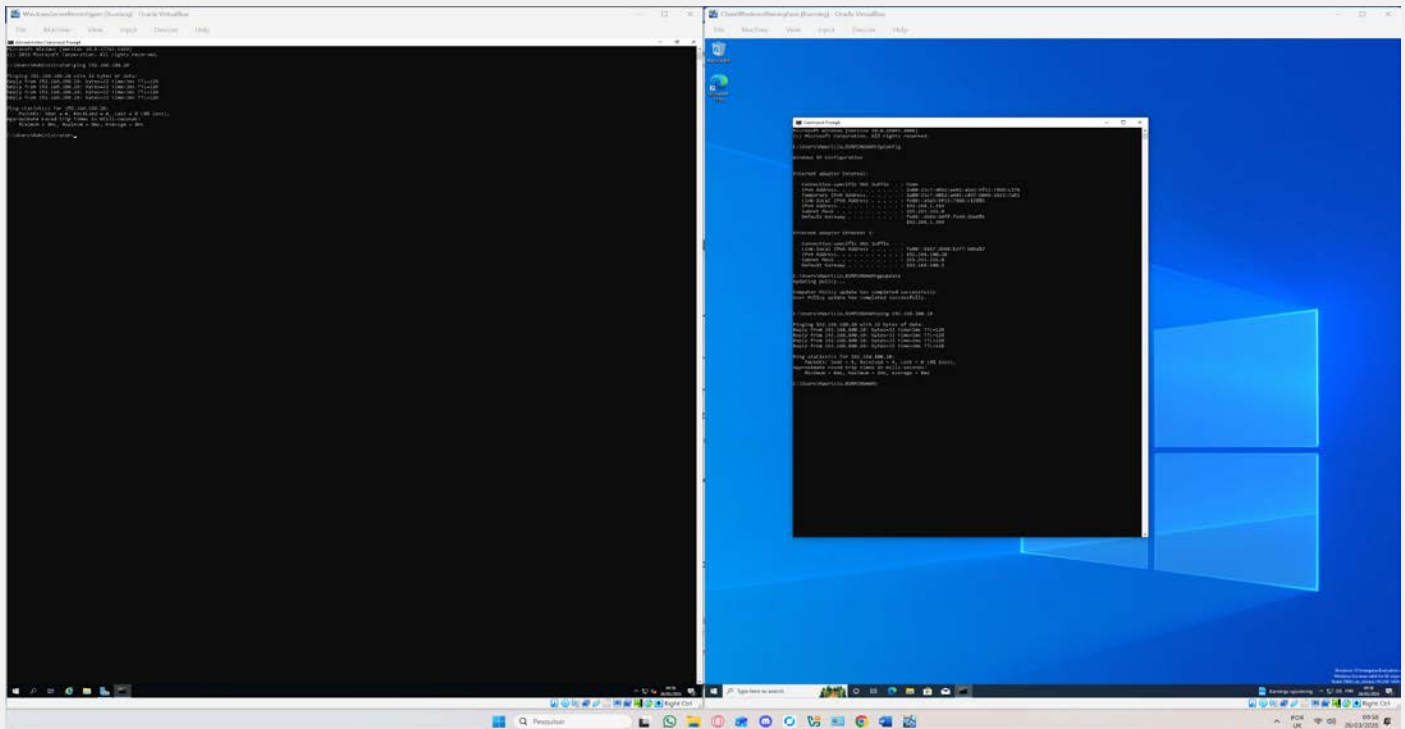


Figure 18: Windows Server and Client Networking ping success.

2. Successful connectivity within Linux network.(Ping 192.168.200.10 and Ping 192.168.200.20)

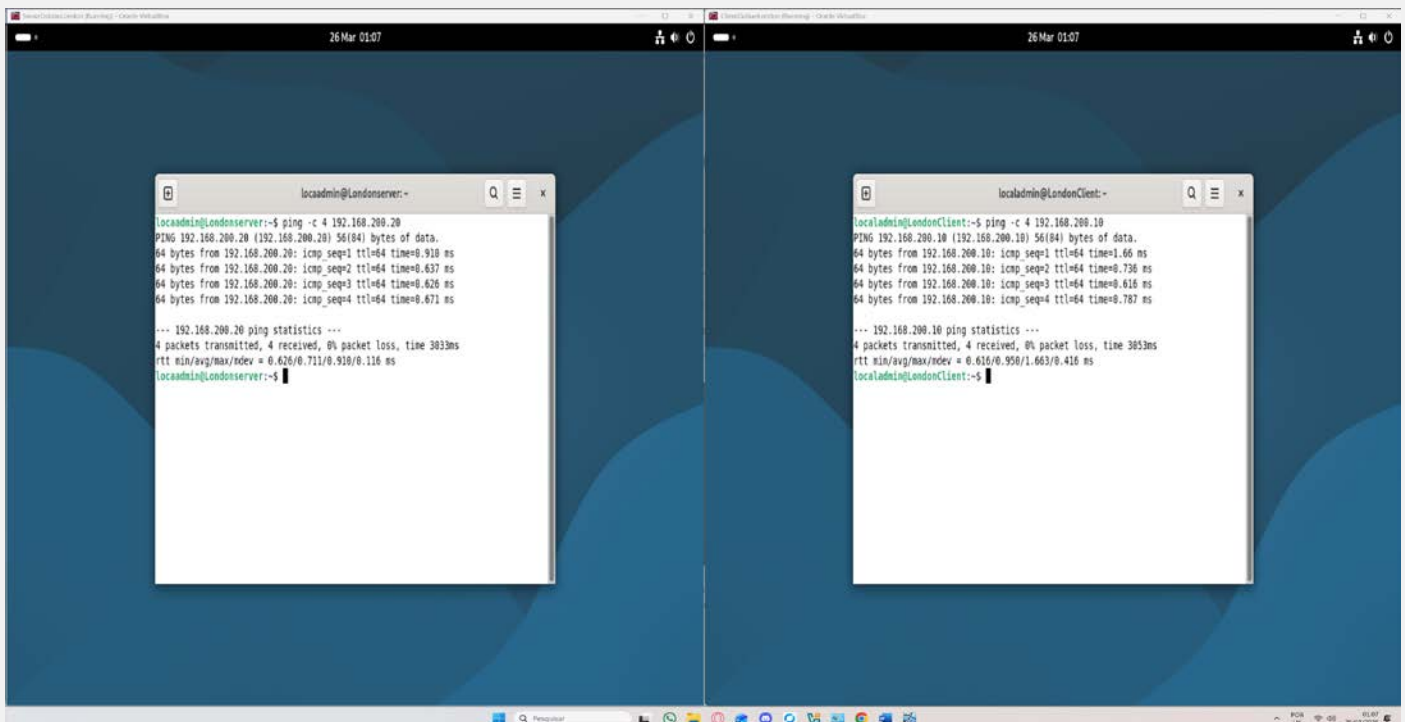


Figure 19: Linux Server and Client Networking ping success.

3. Outcome 2: Unsuccessful connectivity between Linux and windows networks.

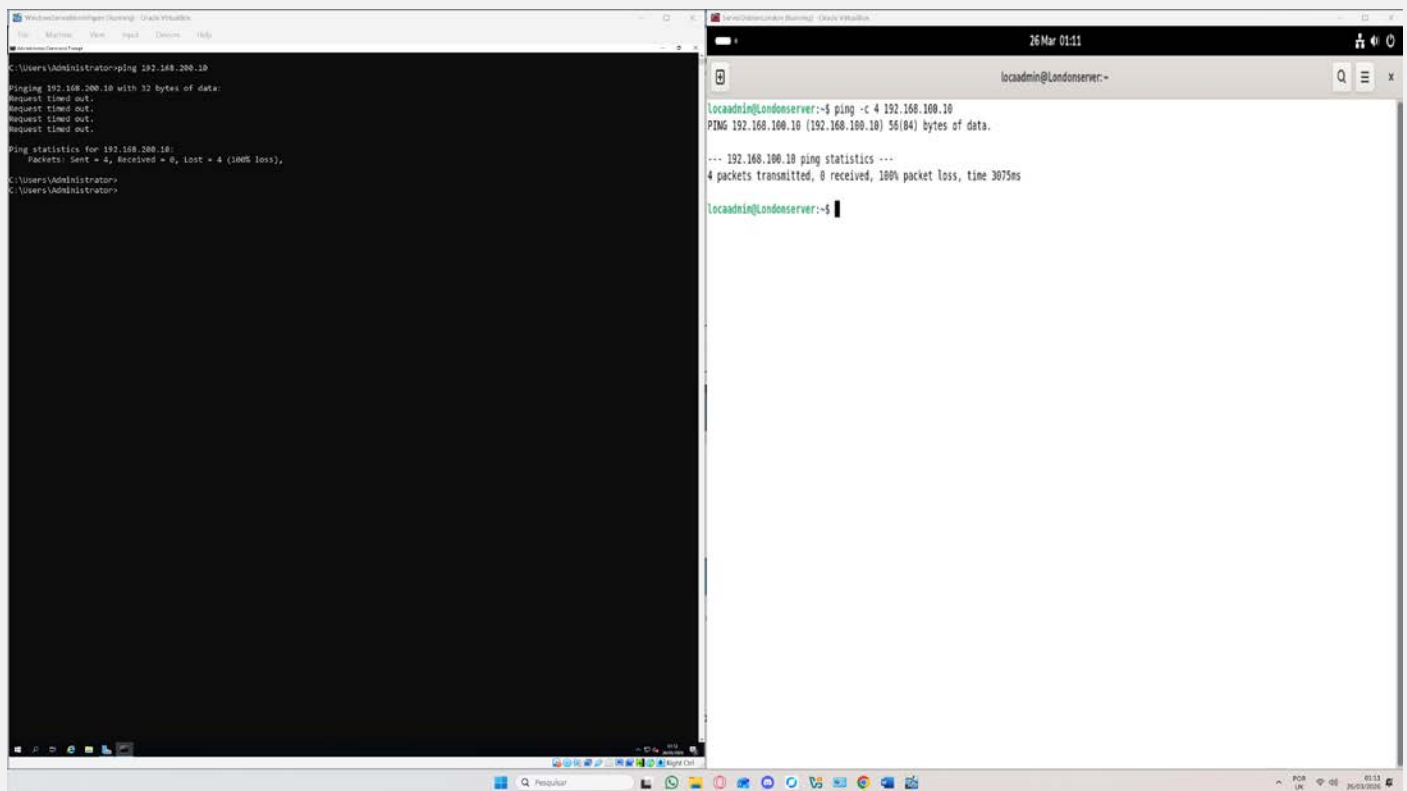


Figure 20: Windows and Linux Servers are not pinging because both are in different network and need to configure.

Task 3

3.1.1. Technical Reflection

During the deployment of the virtualised enterprise network, several technical challenges were encountered and systematically resolved. The primary challenge involved properly isolating the network segments in Oracle VM VirtualBox. Initially, deploying standard "NAT" adapters allowed internet access but prevented the virtual machines from communicating with one another. To resolve this, I diagnosed the issue by reviewing the hypervisor's network abstraction layers and subsequently reconfigured the adapters to use "NAT Network" ensuring VMs on the same subnet shared the same virtual switch environment.

Additionally, I faced several failures due to corrupted ISO files and architecture mismatches. The main issue occurred when I mistakenly attempted to deploy 32-bit Windows versions instead of the required 64-bit architecture, which caused several installation failures and compatibility errors. After identifying the mistake and sourcing the correct 64-bit images, I was able to successfully provision the virtual machines and align the IP addressing for both sites. Solving these technical errors was actually very helpful, as it forced me to pay closer attention to hardware requirements and improved my troubleshooting skills for the rest of the project.

3.1.2. Personal Reflection

This coursework significantly enhanced the practical understanding of translating theoretical network topologies into functional virtualised environments. It helped me understand things I thought I already knew. Setting up the IP addresses manually made me realise I had never really thought about subnetting properly before. I was just following examples without fully getting why.

The part that surprised me most was the Windows firewall blocking the ping tests. I spent a while thinking it was a network configuration problem before I figured out it was just a firewall rule. That was a good lesson in not jumping to conclusions when something stops working.

Overall I feel more ready for the next phase of the project than I expected. Having the four machines running and talking to each other is a good starting point, and I now know the environment well enough to build on it.

References

- [1] M. Portnoy, *Virtualization Essentials*, 2nd ed. Indianapolis, IN, USA: John Wiley & Sons, 2024.
- [2] IBM, "What is a Hypervisor?," IBM Cloud Education, 2025. [Online]. Available: <https://www.ibm.com/topics/hypervisors>. [Accessed: Mar. 25, 2026].
- [3] B. Jolly, *Hands-On Virtual Computing with Oracle VM VirtualBox*, 3rd ed. Boston, MA, USA: Cengage Learning, 2024.
- [4] Oracle, "Oracle VM VirtualBox User Manual," Oracle Corporation, 2025. [Online]. Available: <https://www.virtualbox.org/manual/UserManual.html>. [Accessed: Mar. 25, 2026].
- [5] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, 8th ed. Hoboken, NJ, USA: Pearson, 2021.
- [6] G. C. Anderson, *Modern Subnetting: Design and Implementation of VLSM*, London, UK: Academic Press, 2023.
- [7] IETF, "IPv4 Address Depletion and the Transition to IPv6," RFC 9501, 2025. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc9501>. [Accessed: Mar. 25, 2026].
- [8] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 6th ed. Boston, MA, USA: Pearson, 2024.
- [9] Cisco Systems, "Static vs Dynamic Routing in Enterprise Branch Offices," White Paper, 2025. [Online]. Available: <https://www.cisco.com/c/en/us/td/docs/solutions/enterprise/static-routing-design.html>. [Accessed: Mar. 25, 2026].
- [10] W. Odom, *CCNA 200-301 Official Cert Guide, Volume 1*, 2nd ed. Indianapolis, IN, USA: Cisco Press, 2023.
- [11] Microsoft, "Dynamic Host Configuration Protocol (DHCP)," Microsoft Learn, 2025. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top>. [Accessed: Mar. 25, 2026].
- [12] W. R. Stanek, *Active Directory Administrator's Pocket Consultant*, 2nd ed. Redmond, WA, USA: Microsoft Press, 2024.
- [13] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering: Design Principles and Practical Applications*, 2nd ed. Indianapolis, IN, USA: Wiley, 2024.
- [14] J. L. Hanley, *Windows Server 2022 & 2025 Administration Guide*, 2nd ed. Birmingham, UK: Packt Publishing, 2025.