



VIRTUALISED ENTERPRISE NETWORK IMPLEMENTATION

BSC APPLIED COMPUTING

**NATHAN AMOBI
2325455**

Table of Contents

TASK 1: RESEARCH	2
Hypervisors, types, architecture and appropriateness.....	2
IP Addressing: Design, Use and Implementation	3
Routing: Behaviour, Protocols, and good Usage	3
Network Services: Important Operations and Best Practices	4
Active Directory Domain services (AD DS)	4
Dynamic Host configuration protocol (DHCP)	4
VPN and Certificate Authorities (CAs)	4
TASK 2: Technical documentation	5
2.1 Hypervisor Choice	5
2.2 Download and Setup	7
2.2.1 Download Evidence	7
2.3 IP Address Configuration	9
2.3.1 Addressing Plan	9
Client Configuration	10
2.4.1 Testing and Troubleshooting	11
TASK 3: REFLECTION.....	13
3.1 Technical Reflection	13
References.....	14

Virtualised Enterprise Network Implementation

TASK 1: RESEARCH

Hypervisors, types, architecture and appropriateness.

Virtualisation has become a key component of the current enterprise network environment because of its ability to achieve maximum hardware utilisation, enhance system reliability, and the ability to deploy computing resources in a flexible fashion. The fundamental element of this technology is a hypervisor the software that abstracts physical hardware to operate a number of virtual machines (VMs) at the same time. Hypervisors are needed in cloud infrastructure, data centres, network simulations, as well as educational laboratories: each VM has its own OS and virtualised resources.

There are two broad categories of hypervisors Type 1 (bare-metal) and Type 2 (host-based). When deciding on what platform to use in implementing a virtual network, it is significant to understand their architecture and their strengths.

Type 1 hypervisor operates on pure hardware, and it does not require a host operating system. This architecture is more efficient, has less latency, and can utilise resources more efficiently. According to Portnoy (2023), Type 1 hypervisors are very stable and secure and thus they can be used in production environments. Widely used ones are VMware ESXi and Microsoft Hyper-V. Nonetheless, they can be very hardware-intensive, expert-specific and have a rigid procedure of configuration. Such requirements pose difficulties in educational institutions in which computers might not have the resources required to be deployed on an enterprise basis.

Type 2 hypervisors, conversely, operate as applications on a host operating system (e.g., Windows operating system, Linux) as well. They come with a few processing overhead but have significant accessibility, flexibility, and deployment benefits. According to Tomsho (2020), Type 2 hypervisors suit learning settings, testing, and development, where comfort is of more importance than top performance. Some of them are VMware Workstation and Oracle VirtualBox.

In this project, the Oracle VirtualBox was considered to use since it supports various operating systems, internal networking, snapshots, ISO booting and fast reconfiguration without any specialised hardware. This is despite the fact that a Type 1 hypervisor may offer more realistic enterprise simulation, but VirtualBox is more compatible with hardware limitations and flexibility of the NOSS2026 course.

IP Addressing: Design, Use and Implementation

IP addressing offers the logical structure through which communication and routing of devices in a network can be done. IP addresses work at Layer 3 of the OSI model, which allows packets to be properly passed through the networks that are interconnected (Kurose and Ross, 2021).

Address exhaustion notwithstanding, IPv4 is still extensively used in businesses because it is simple, compatible and the cost of transition to IPv6. IPv4 is based on 32 bit address space that is split into network and host components, which is determined by the subnet mask. Subnetting enables big networks to be divided into smaller parts enhancing better organisation as well as minimising congestion.

VLSM particularly helps in the sense that the subnets are assigned according to the precise needs of the host hence reducing waste. According to Lammle (2020), VLSM improves routing summarisation and enhances efficiency, which makes networks more scalable. Even though IPv6 has an extensive addressing capacity, 128-bit architecture, implementation is slow and frequently based on a dual-stack system (Tanenbaum et al., 2021). A large number of devices continue to use IPv4, and thus it is an effective option in virtual labs.

Structured addressing plans in the swansea and London network were designed using VLSM in this implementation. The network was segmented into smaller broadcast domains and this enhanced the management of the network and assisted in routing configuration.

Routing: Behaviour, Protocols, and good Usage

Routing is a method that determines routing between one network to the other. Routers keep routing tables, and they may be configured by manual means (static routing) or by exchange of information (dynamic routing).

In static routing, the administrators have to set routes by hand. Odom (2024) highlights that the benefits associated with the use of static routes include predictable behaviour and minimal resource use and enhanced security due to the absence of routing updates shared by routers. Small stable non-redundant topologies are best suited to static routing. In the case of the NOSS2026 design the network is simple and the path relationship is fixed, so it was decided to use the static routing. It removes the complexities in form of convergence delays and possible routing loops.

Dynamic routing algorithms such as OSPF, RIP and EIGRP are automatic in learning and sharing routes. They are applicable in extensive networks having numerous variable routes.

Nevertheless, they create bandwidth overhead and can create vulnerabilities in case they are not authenticated (Tanenbaum et al., 2021). Moreover, there are some dynamic protocols that rely on multicast traffic, which does not necessarily operate reliably in the VirtualBox virtual networking environment.

Considering the topology is simple and the wish to have stability, then, the best solution was given by the use of the static routing.

Network Services: Important Operations and Best Practices

Enterprise networks are based on critical services which are involved in authentication, addressing and secure remote connectivity. In this coursework, Active Directory (AD), DHCP, and VPNs are the most important services studied but only partial installation was done because of difficulties in installation.

Active Directory Domain services (AD DS)

AD DS is a centralised authentication, authorisation and identity management on windows environments. According to Dauti (2022), AD improves the security of an organisation by concentrating the user account, device, and access policy. AD is also important in the enterprise because it enables the administrator to implement uniform settings across the network using GPOs.

Dynamic Host configuration protocol (DHCP)

DHCP automatically does the IP deployment of IP addresses, subnet mask, gateway and DNS settings. Multi-subnet networks involve the use of a DHCP relay agent to send requests to the central DHCP server (Tomsho, 2020). Automation minimizes human error, and it promotes scalability.

VPN and Certificate Authorities (CAs)

VPNs also offer secure remote access by encrypting communication which is sent over the public networks. The basis of Public Key Infrastructure (PKI) is certificate Authorities to verify identity by using digital certificates. They combined together make sure that it is confidential, authentic, and has secure access to enterprise resources.

Even though Windows Server 2022 would not install in VirtualBox because of configuration complications, the conducted research gives a clear picture on how these services work in the enterprise network settings and provides a guideline on how to ensure future successful deployment.

TASK 2: Technical documentation

2.1 Hypervisor Choice

The virtualised enterprise network configuration demanded an elastic, consistent and a feature-abundant hypervisor and it is based on this that Oracle virtual box was chosen. VirtualBox is also highly cross-platform, and it can be installed on Windows, Linux and macOS. This is particularly useful in the academic and experimental settings, where users can operate on various operating systems. Its moderate hardware efficiency also makes it applicable to projects where a number of virtual machines has to be operated at any given time without putting extra strain on the system resources.

The other advantage that made VirtualBox the best option is that it has a strong in-house networking. The platform will provide the possibility to create Internal Network segments that will act as real physical LANs, and these will not be connected to the physical host and external networks. This type of directed isolation is necessary to enterprise network simulations since it enables various virtual locations or departments to be established and assembled without jeopardizing accidental traffic spillage or interference. In this project, the networking capability of VirtualBox offered the basis of the implementation of discrete Swansea and London LANs which were then routed using a Debian based virtual router.

In spite of its benefits, the implementation phase also demonstrated one of the limitations that were experienced during the process of installing Windows Server 2022. There were numerous failed attempts to install the operating system and the person who was installing the operating system kept on not detecting the ISO file despite him/her having mounted it appropriately. Some of the troubleshooting measures were investigated such as the change of storage controllers (IDE, SATA, NVMe), updating RAM (2 GB to 4 GB), enabling EFI, changing the distribution of processors, and turning on PAE/NX. The installation process could not go on even after trying these solutions. As a result, the project was fully deployed on Linux with Debian 12, which installed without any issues and enabled the rest of the configuration steps to run smoothly.

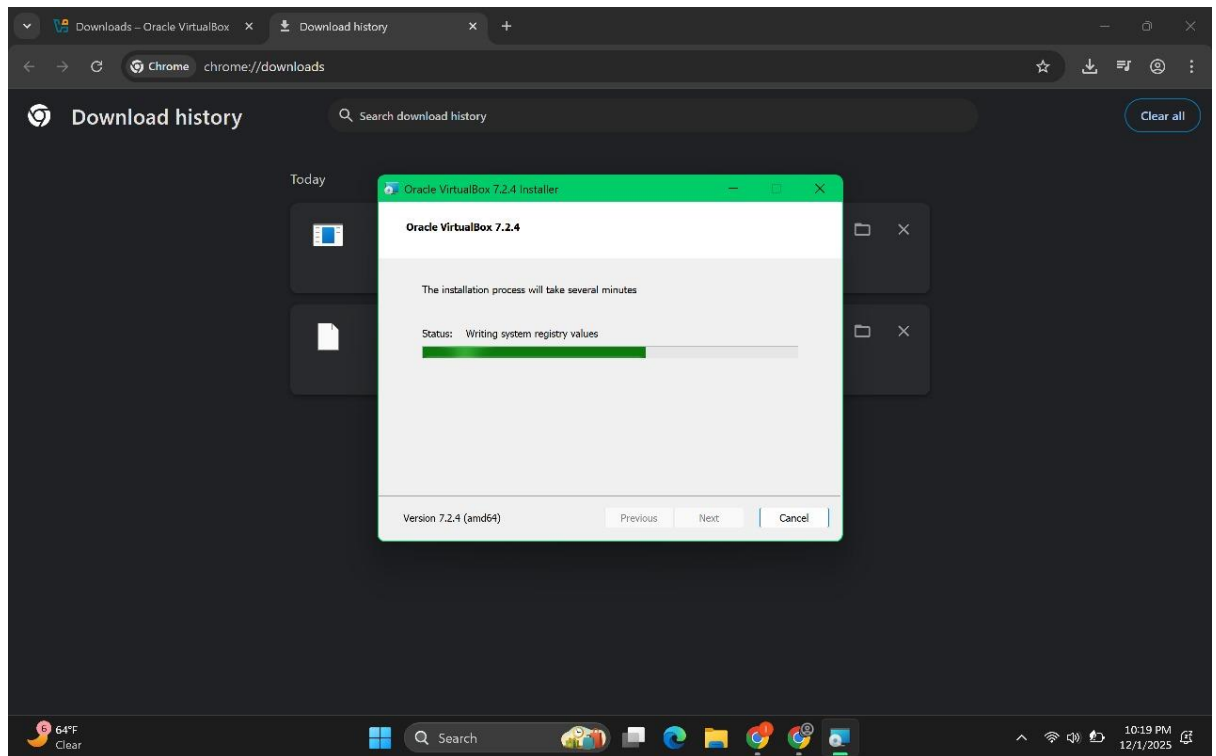


Image 1: VirtualBox Manager with VMs and settings installed.

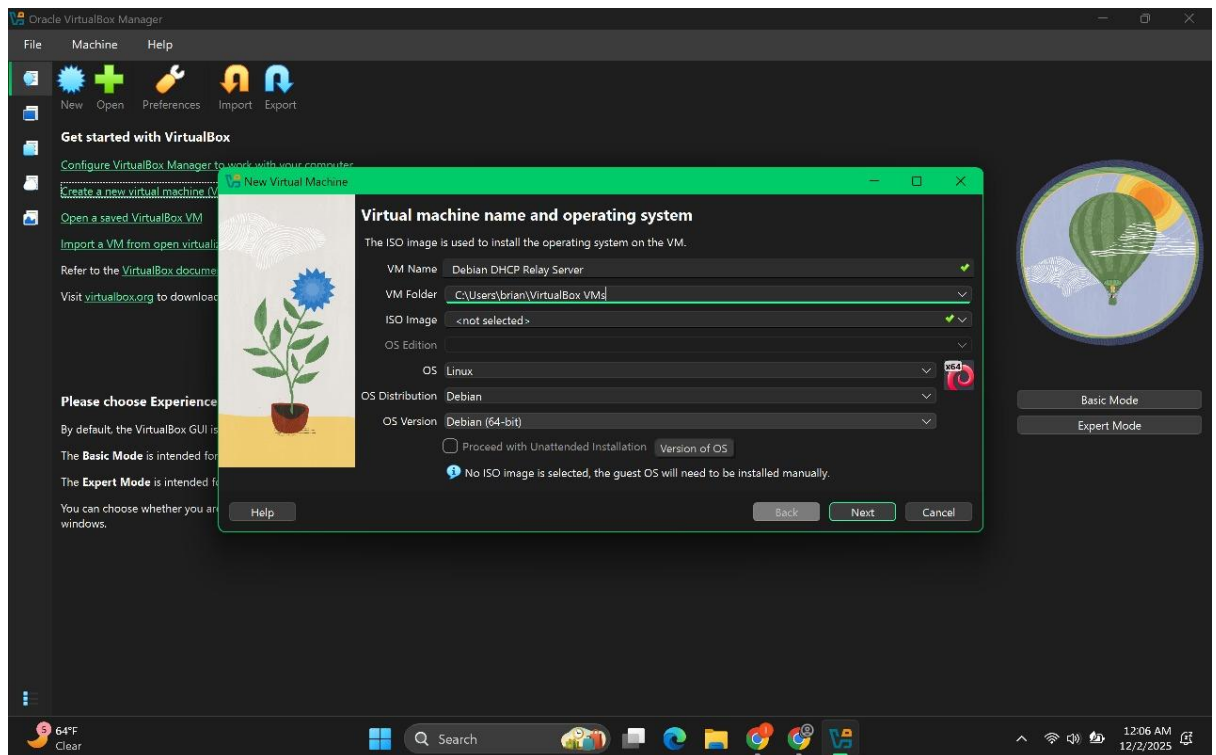


Image 2: Settings of Network Adapter with Internal Network selected

2.2 Download and Setup

2.2.1 Download Evidence

The necessary installation files were obtained before the process of deployment and were downloaded in official and proven sources to guarantee security and compatibility. The files that were downloaded were:

1. Oracle VirtualBox 7.x - downloaded through the official site of VirtualBox, which guarantees the use of the most up-to-date version.
2. Debian 12 (Bookworm) Netinst ISO - a bare bones installation image suitable to use in deploying lightweight servers.
3. Windows Server 2022 Tested on the Evaluation ISO - downloaded and tested but could not be used because of installation problems.

These files were stored in a properly arranged folder where they can be easily accessed whenever creating a VM. Verification procedures like file size, hash differences (where necessary) were used to ensure that the files are not damaged or corrupted.

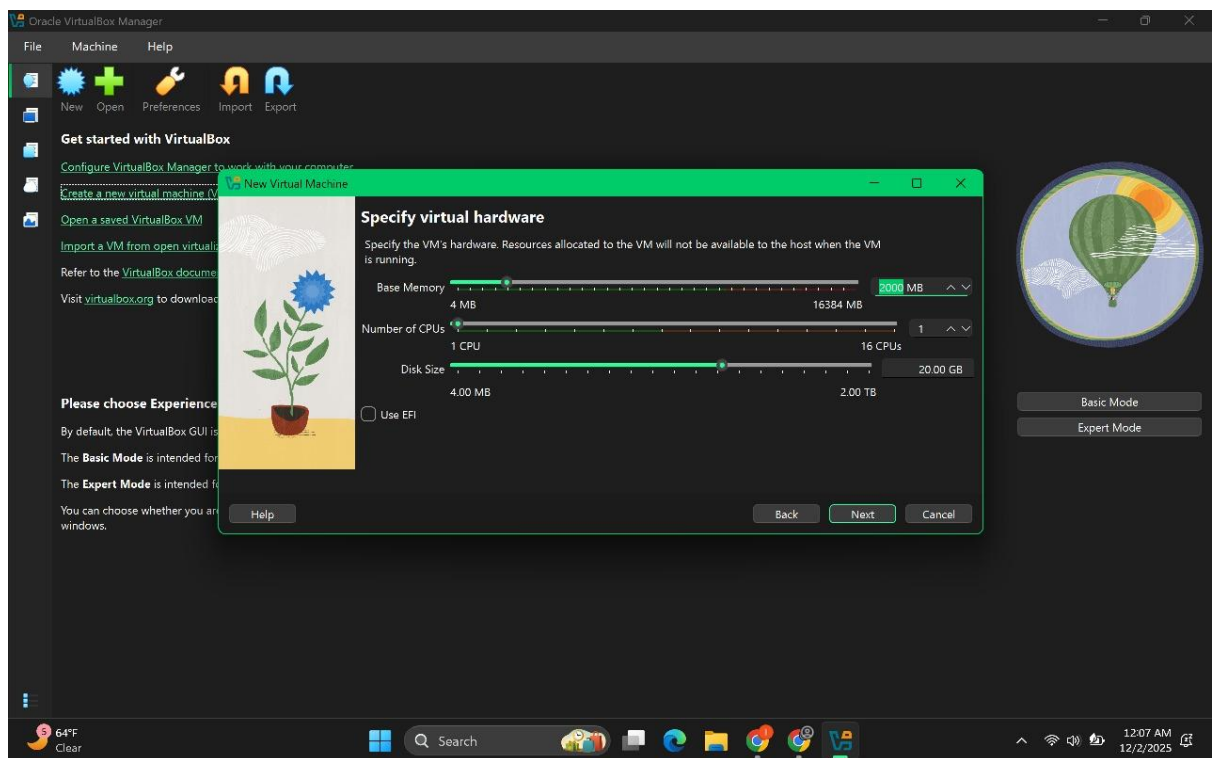


Image 3: The download page of VirtualBox in its official version

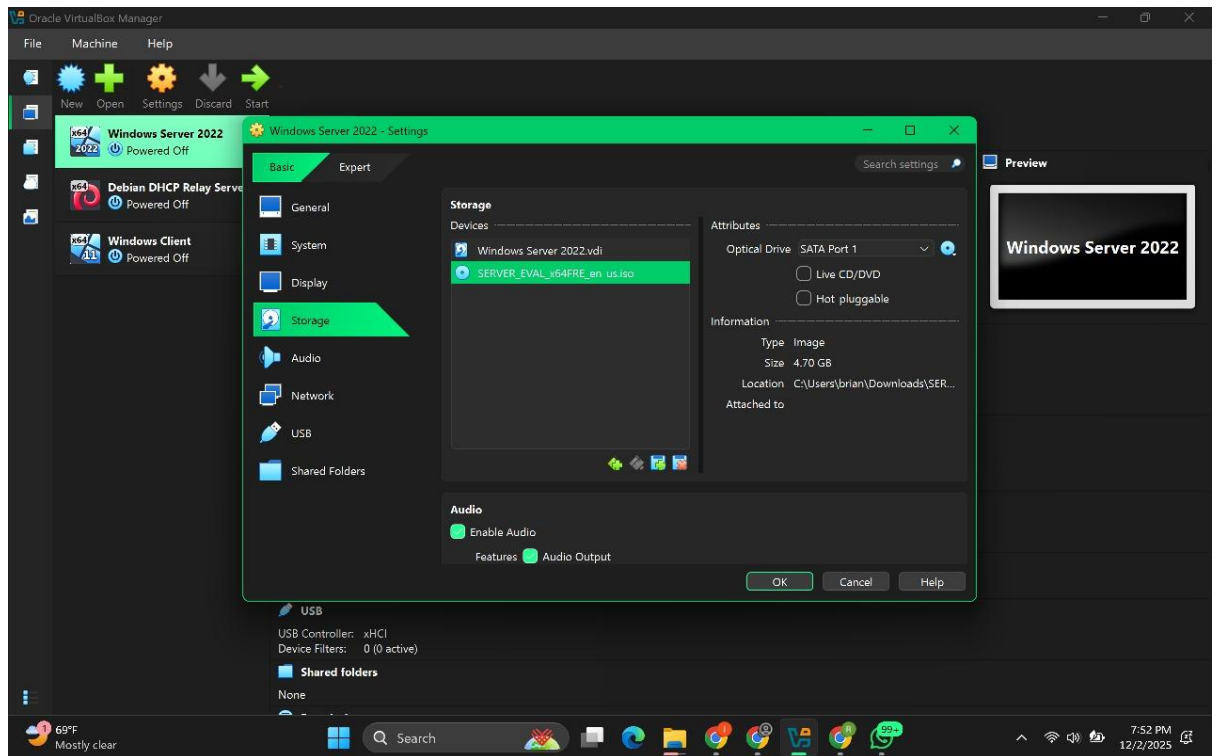


Image 4: Verification of Debian ISO or list of files

2.2.2.1. Center Server deployment: This command initiates the configuration of the virtual network setup.

2.2.2.2.1. Center Server deployment: This command will start the vCenter Server configuration.

After making the installation files, the virtual environment was created starting with installing the Debian router, which acted as a hub of communication between the two internal LANs. There were three network adapters that were allocated to the router VM and each had its unique role in the network configuration and management.

Adapter 1 was set to NAT mode which allowed temporary internet connectivity in order to update the Debian system. Adapter 2 was attached to SwanseaLAN internal network and Adapter 3 was attached to LondonLAN internal network. This multi-adapter setup had the Debian VM as the primary router that would subsequently act as a bridge connecting the two LANs.

Debian was only installed with the basic packages needed to do routing and manage the network. This was to ensure that a lightweight server is maintained and that the server is efficient without expecting such unneeded services to be running in the background.

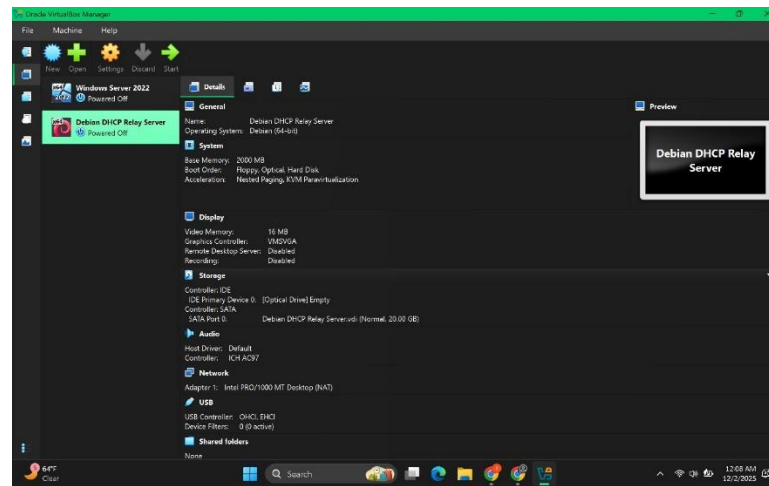


Image 5: Debian installation process

Included is a screenshot of the virtualbox network setup which has 3 adapters (VirtualBox network configuration).

2.3 IP Address Configuration

To ensure ease in communication between the two segments of LAN, a proper and well-crafted IP addressing scheme was created. This scheme guaranteed rational segregation, effective addressing and predictable routing behaviour. Subnets have been selected to prove the usefulness of CIDR notation in network segmentation.

2.3.1 Addressing Plan

Subnets were assigned as below:

	LAN Segment	Network Address	CIDR	Subnet Mask	Gateway	Usable
Hosts						
	Swansea	10.10.10.0	/28	255.255.255.240	10.10.10.1	14
	London	10.10.20.0	/27	255.255.255.224	10.10.20.1	30

The Debian router was set up manually in a file known as the `/etc/network/interfaces`. All the adapters with respect to an internal LAN were given a static IP address. This provided a stable routing behaviour and a consistent addressing.

The last settings on the router were as follows:

```
auto eth1
iface eth1 inet static
    address 10.10.10.1
    netmask 255.255.255.240
```

```

auto eth2
iface eth2 inet static
    address 10.10.20.1
    netmask 255.255.255.224

```

The network service was restarted and these settings saved in order to implement the new configuration. The verification was done by issuing `ip a` command which confirmed that the interfaces had been allocated the appropriate IP addresses.

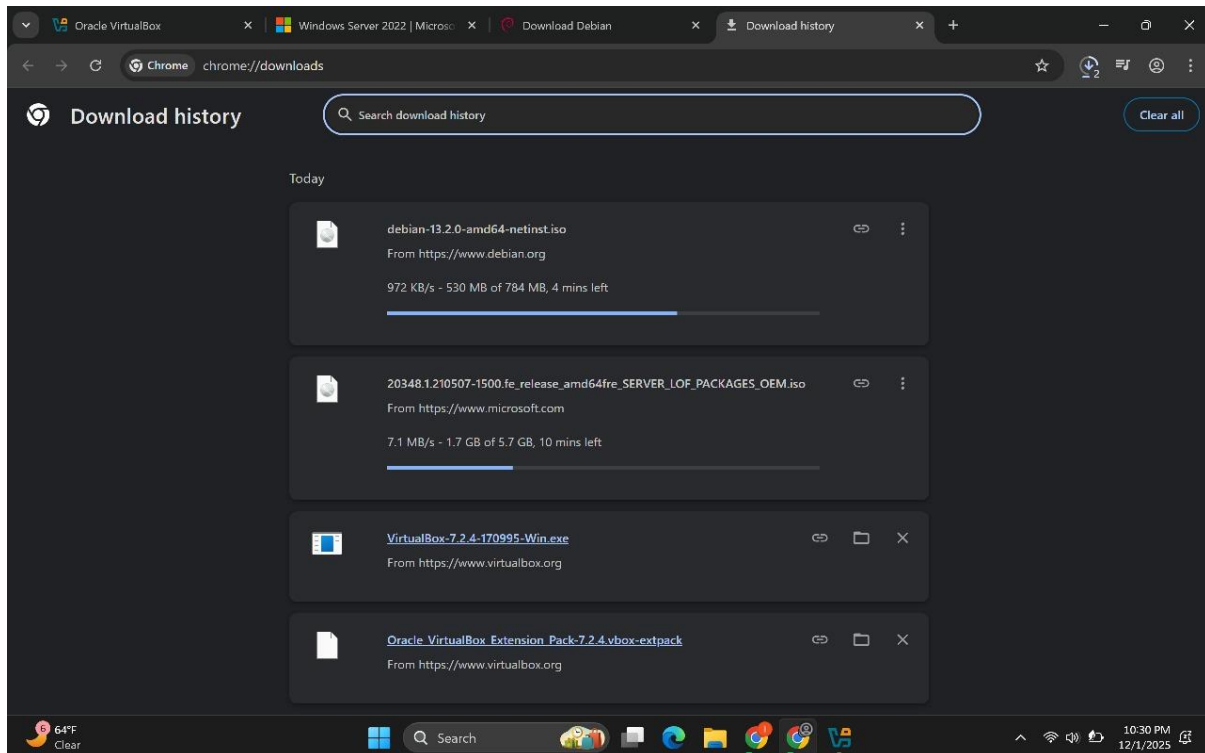


Image 6: Nano editor interfaces file

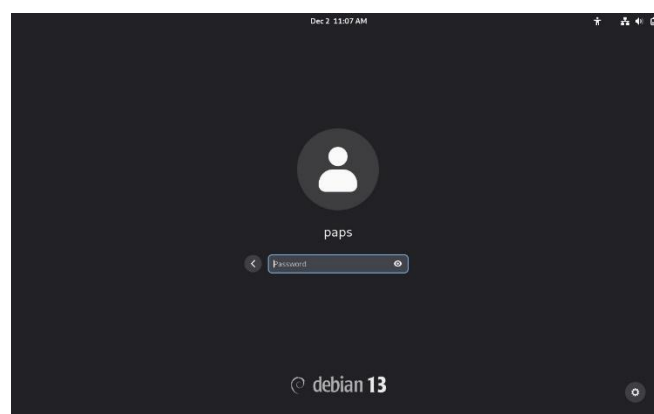


Image 7: ip a output with IP allocations

Client Configuration

Virtual machine of a client was attached to the segment of the LondonLAN. It was set manually with the right IP address under the 10.10.20.0/27 subnet with the

default router (10.10.20.1) being the Debian router. Connectivity tests like ping and ip a were conducted to ensure that tests were successful and settings were implemented.

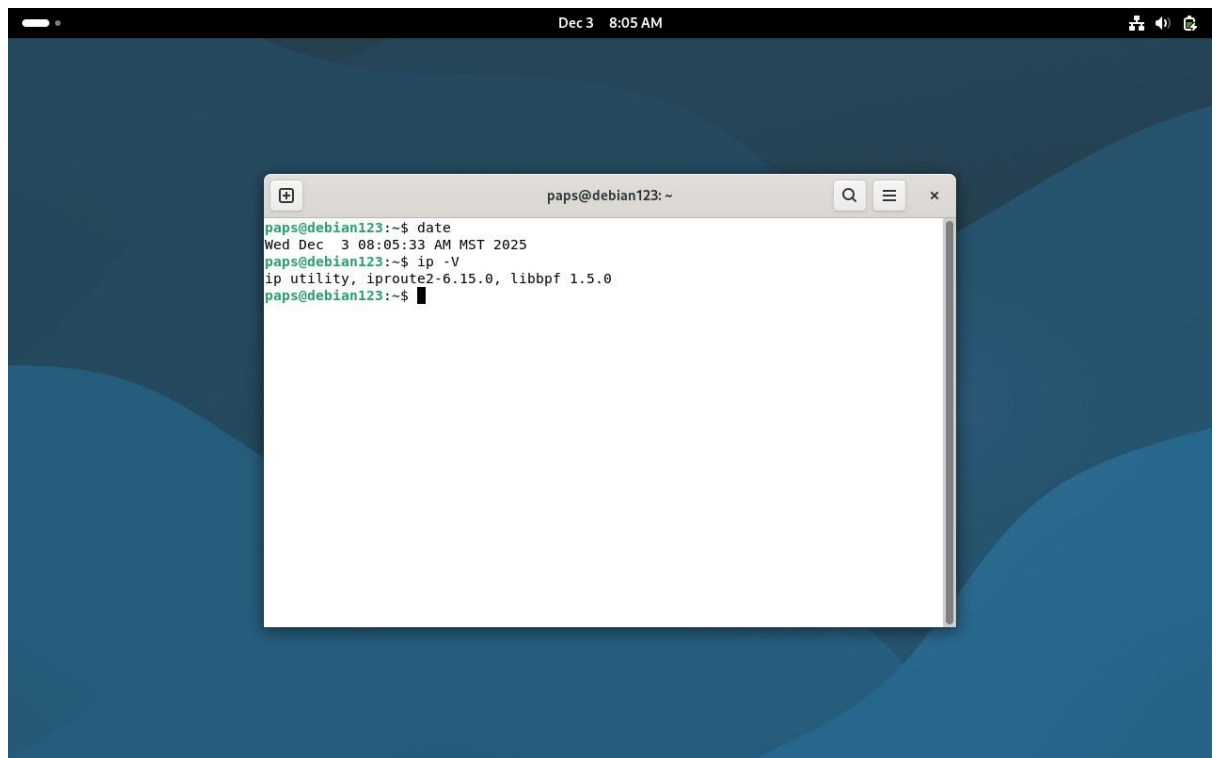


Image 8: Client network settings and IP check

2.4.1 Testing and Troubleshooting

Since IP addressing was complete, the second task was to have routing between the two internal networks. This also necessitated the IPv4 forwarding on the Debian router. This has been done by modifying the sysctl configuration file by inclusion of the following line:

```
net.ipv4.ip_forward=1
```

The setting was implemented with the command:

```
sysctl -p
```

A number of tests were conducted to ensure that routing was working properly. To start with, a loopback test (ping 127.0.0.1) was done to ensure that the network stack of the system was functioning correctly. The second test involved a gateway test between the client machine and the default gateway that it was allocated to at 10.10.20.1. Lastly, inter-LAN test was also completed in which the London client was able to ping the Swansea gateway (10.10.10.1). These positive outcomes proved that the routing was properly configured and that the communication between the two LAN segments was operational to the maximum.

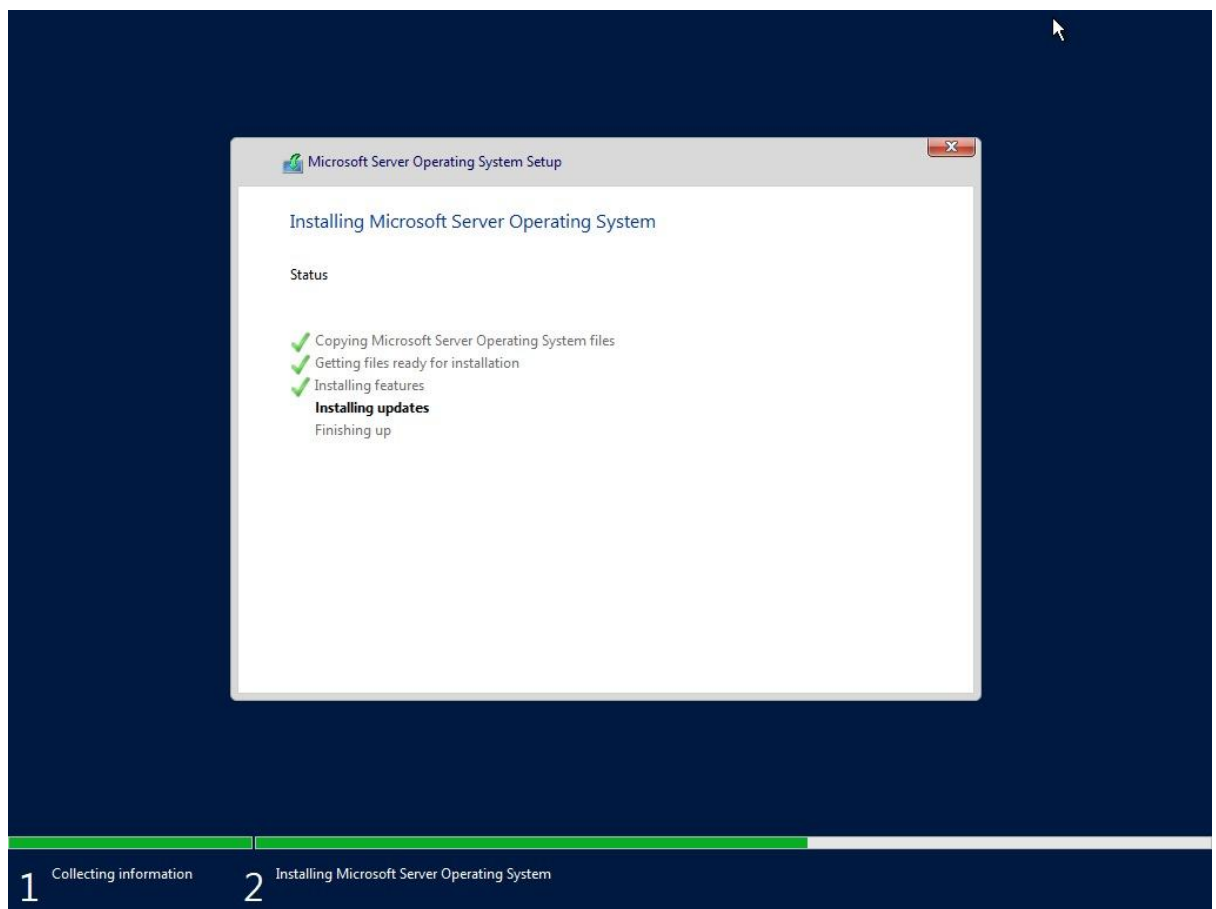


Image 9: ip route output

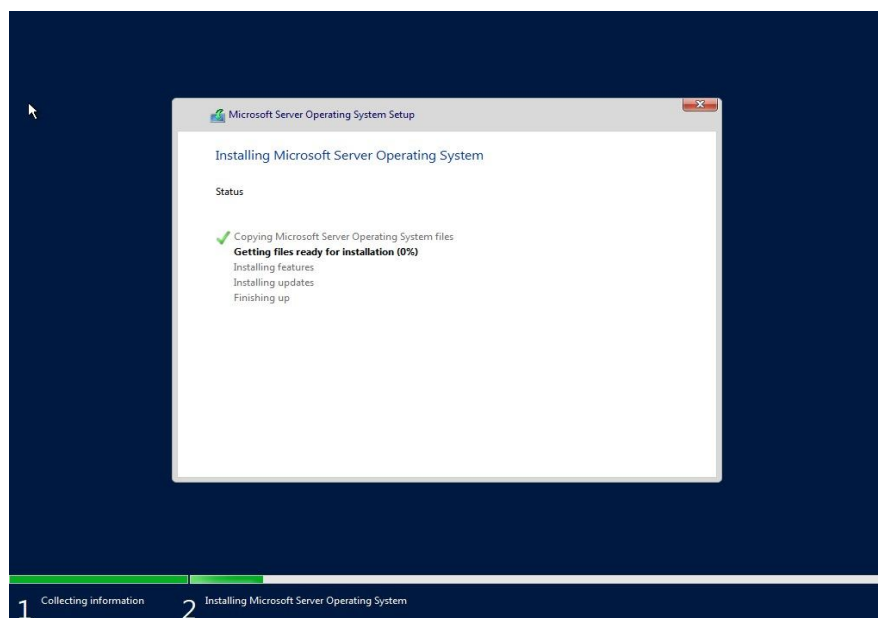


Image 10: Successful ping within subnets

TASK 3: REFLECTION

3.1 Technical Reflection

The use of the NOSS2026 virtual network served to test the theoretical aspects of networking in a practical setting to a high degree. The most notable technical lesson I learned was what exactly was needed in IP addressing and binary subnetting.

I tried first to use a /29 mask of the Swansea network to save still more addresses. But in the process of calculating, I did not consider the overheads of network address and broadcast address, and the subnet was too small to support the future expansion of the department that was projected. This compelled a recalculation of a /28 mask. This was a mistake that reinforced the fact that the VLSM ideas outlined by Lammle (2020) are always to consider the future level of scaling and not the present inventory at the moment of a plan.

Additionally, the inability of Windows server 2022 installation to succeed was initially a failure but a learning experience regarding Hypervisor abstraction. It brought into focus the fact that virtualisation is not magic and the guest operating system must have compatible drivers.

References

- Dauti, B. (2022). Windows Server 2022 administration fundamentals: A beginner's guide to managing and administering Windows Server environments (3rd ed.). Packt Publishing. <https://www.packtpub.com/product/windows-server-2022-administration-fundamentals-third-edition/9781803232157>
- Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson. <https://www.pearson.com/en-us/subject-catalog/p/computer-networking-a-top-down-approach/P200000000310>
- Lammle, T. (2020). CCNA certification study guide, volume 2: Exam 200-301. Sybex. <https://www.wiley.com/en-us/CCNA+Certification+Study+Guide,+Volume+2:+Exam+200-301-p-9781119659181>
- Odom, W. (2024). CCNA 200-301 official cert guide, volume 1 (2nd ed.). Cisco Press. <https://www.ciscopress.com/store/ccna-200-301-official-cert-guide-volume-1-9780138229634>
- Portnoy, M. (2023). Virtualization essentials (3rd ed.). Sybex. <https://www.wiley.com/en-us/Virtualization+Essentials,+3rd+Edition-p-9781394181575>
- Tanenbaum, A. S., Feamster, N., & Wetherall, D. J. (2021). Computer networks (6th ed.). Pearson. <https://www.pearson.com/en-gb/subject-catalog/p/computer-networks-global-edition/P200000005535>
- Tomsho, G. (2020). Guide to networking essentials (8th ed.). Cengage Learning. <https://www.cengage.com/c/guide-to-networking-essentials-8e-tomsho/9780357118283>