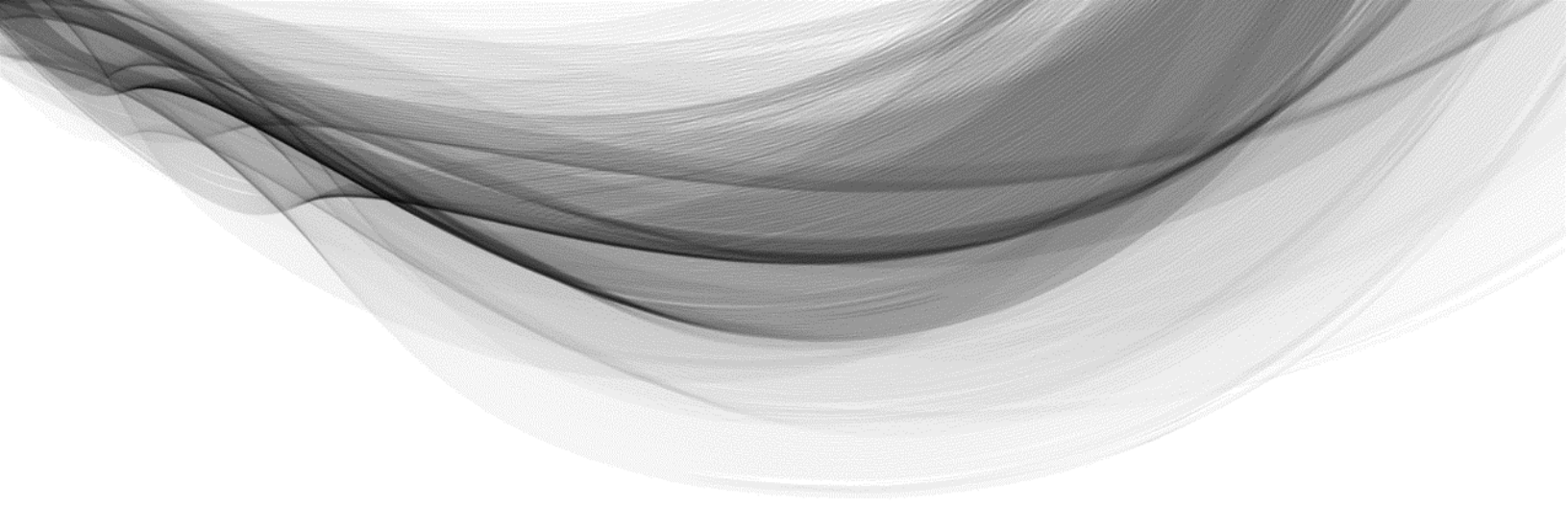




Research, build and deploy a Virtualised Enterprise network

L5 – Network Operating Systems and Services

Module Code: ACCA5023

BSc Computing (Software Engineering)

Contents

1. Introduction	03
2. Architectural and Network Design Considerations	03
2.1 Hypervisor Architecture and Suitability	03
2.2 IP Addressing and Network Communications	03
2.3 Routing Protocols and Approach	04
2.4 Network Service Features and Best Practices	04
3. Implementation and Documentation	05
3.1 Hypervisor Justification	05
3.2 Environment Setup and Development	05
3.3 IP Addressing Implementation	08
3.4 Testing and Troubleshooting	09
4. Reflection	11
4.1 Technical Reflection	11
4.2 Personal Reflection	11
5. References	12

1. Introduction

NOSS2026 is a Multinational Corporation operating across two locations within the United Kingdom. The organisation requires the implementation of a structured network across both Swansea and London that aligns with their proposed topology. The primary aim of this deployment is to establish a functional network environment that accommodates the hosting of both Windows Server 2022 and Debian systems, with IP address settings configured to support communication between defined machines.

To support an effective deployment of the proposed topology, this report analyses the organisation's operational needs prior to implementation. This includes research into appropriate hypervisor architecture, IP addressing, routing, and network services. The findings of said research shall be used to implement an informed and structured solution of NOSS2026's topology.

2. Architectural and Network Design Considerations

This section aims to critically analyse the key components of the proposed topology, including hypervisor architecture, IP addressing, routing protocols and common network services. This research is later used to justify decisions regarding the implementation of NOSS2026's network.

2.1 Hypervisor Architecture and Suitability

Type 1 and Type 2 hypervisors are software that allow users to run multiple virtual machines (VM) on a single physical system. A Type 1 hypervisor, also known as a bare metal hypervisor, is installed directly onto a machine's physical hardware in place of an operating system (OS). This approach enables direct negotiation with server hardware, allocating dedicated resources to VMs. A Type 2 hypervisor, or hosted hypervisor, interacts with the host machine's hardware via the machine's OS. Once installed on a machine, hosted hypervisors run as an application, negotiating with the OS for system resources. This approach leads to the host OS prioritising its own function over the hypervisor's [1].

While Type 1 hypervisors are more typically associated with enterprise-scale infrastructure, offering both increased security and performance, hosted hypervisors remain appropriate in resource-limited environments. Considering the proposed topology consists of a limited Windows Server 2022 and Debian deployment, the performance loss of the shared layer associated with a Type 2 hypervisor is negligible, making it a suitable choice for NOSS2026's network. While bare metal hypervisors are inherently more secure due to their smaller attack surface, hosted hypervisors can be secured through methods such as continuous monitoring of both the hypervisor itself and the host OS. Guidance on virtualisation security measures can be observed from leading cybersecurity organisations such as The National Institute of Standards and Technology (NIST) [2].

2.2 IP Addressing and Network Communications

Internet Protocol (IP) addressing enables the identification of devices within and across computer networks, allowing the transfer of data across multiple systems through the use of packets. Each packet contains both the source and destination IP addresses. When a packet is generated, the host applies a network mask to the destination network address in order to determine whether the destination is within the same network. If a packet's destination resides

outside of a local network, the packet is forwarded to the default gateway. The router then compares the destination IP address with its routing table in order to determine through which interface the packet should be sent [3].

IPv4 is a logical address composed of 32-bit Dotted Decimal Notation (DDN) containing 4 octets ranging from 0 to 255. A subnet mask is used to identify the network and host portions of this address via a process known as ANDing. In contrast to IPv4 addressing, IPv6 addresses are 128-bits in length and are written in hexadecimal. These addresses are not case-sensitive and are formatted as x:x:x:x:x:x:x:x, with each x representing individual hexets [3]. This approach significantly increases address capacity while maintaining the same underlying logic [4].

2.3 Routing Protocols and Approach

Routing enables communication between separate networks, forwarding packets based on a destination IP address. Routers in the distribution layer have the ability to limit broadcasts to the local network while increasing security by separating and protecting certain groups of computers that may contain sensitive information. Security is further upheld by hiding the addresses associated with internal systems from the outside world and controlling who can get into or out of the local network. Routers located in the distribution layer can also be used to interconnect local networks that are geographically separated, while logically grouping users who require access to common resources. These functions are achieved through the use of routing tables, where the destination IP address is compared against known networks to determine the interface to forward the packets out of [5].

Two key routing protocols common within modern networks are static and dynamic routing. Static routes are manually configured, requiring administrative intervention, while dynamic routes automatically adapt to changes within a topology. The configuration complexity associated with static routing increases with a network's size due to its inability to adapt to changes within a network's topology, while dynamic routing's complexity does not increase with a network size as routes are learnt automatically, however this approach requires more system resources. Within NOSS2026's topology, static routing is appropriate due to the limited number of routers and stable topology [5].

2.4 Network Service Features and Best Practices

A Virtual Private Network (VPN) is a network service that simulates a private network over a public network by establishing encrypted tunnels [6]. This approach ensures that sensitive data transmitted by both organisations and individuals remains protected from unauthorised access [7]. National Cyber Security Centre (NCSC) guidance regarding VPNs includes client certificates for machine authentication, allowing the revocation of just one certificate from a network while ensuring private keys are stored securely [8].

Dynamic Host Configuration Protocol (DHCP) is a network service that automates both the management and allocation of IP addresses and related network configurations. This reduces the necessary manual input of network administrators while minimising errors and ensuring the efficient use of IP address resources within a network [9]. Common best practices regarding DHCP include ensuring software is up to date and that a failover DHCP server is configured [10].

Active Directory Domain Services (AD DS) stores directory data within a network while making this data available to both users and administrators. This data is queried in order to manage users, computers and resources within a hierarchical organisation of directory information [11]. Best practices include reducing potential attack surface through methods such as least-privilege access, implementing multifactor authentication (MFA), and the use of secure administrative hosts [12].

A Certificate Authority (CA) is a network service that performs certificate issuing, renewal and revocation, acting as a trusted component within a Public Key Infrastructure (PKI). Best practices include outlining a backup and recovery plan in the case of failure as well as the secure handling of private keys [13].

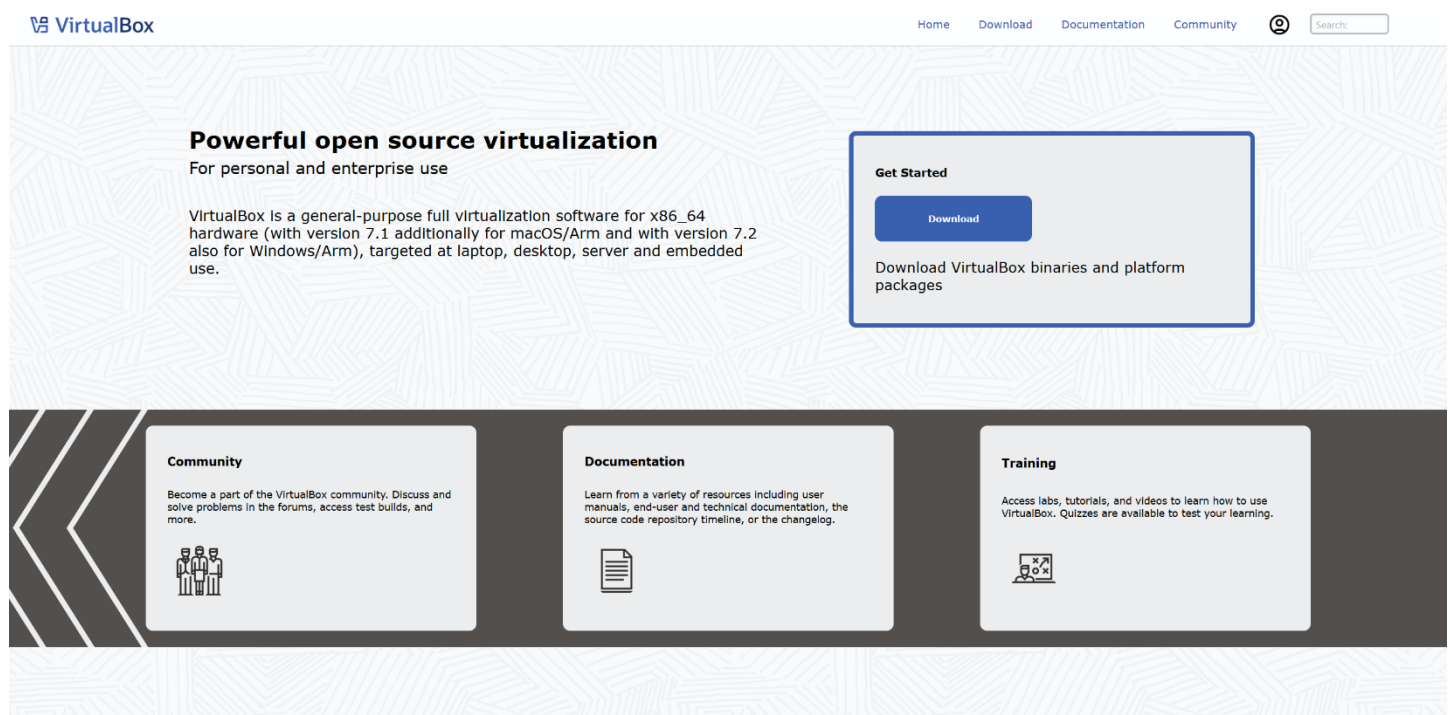
3. Implementation and Documentation

This section of the report covers the practical implementation of NOSS2026's topology supported by screenshots as evidence of configuration and testing. Justification for the chosen hypervisor Type is also provided with reference to research outlined within Section 2.

3.1 Hypervisor Justification

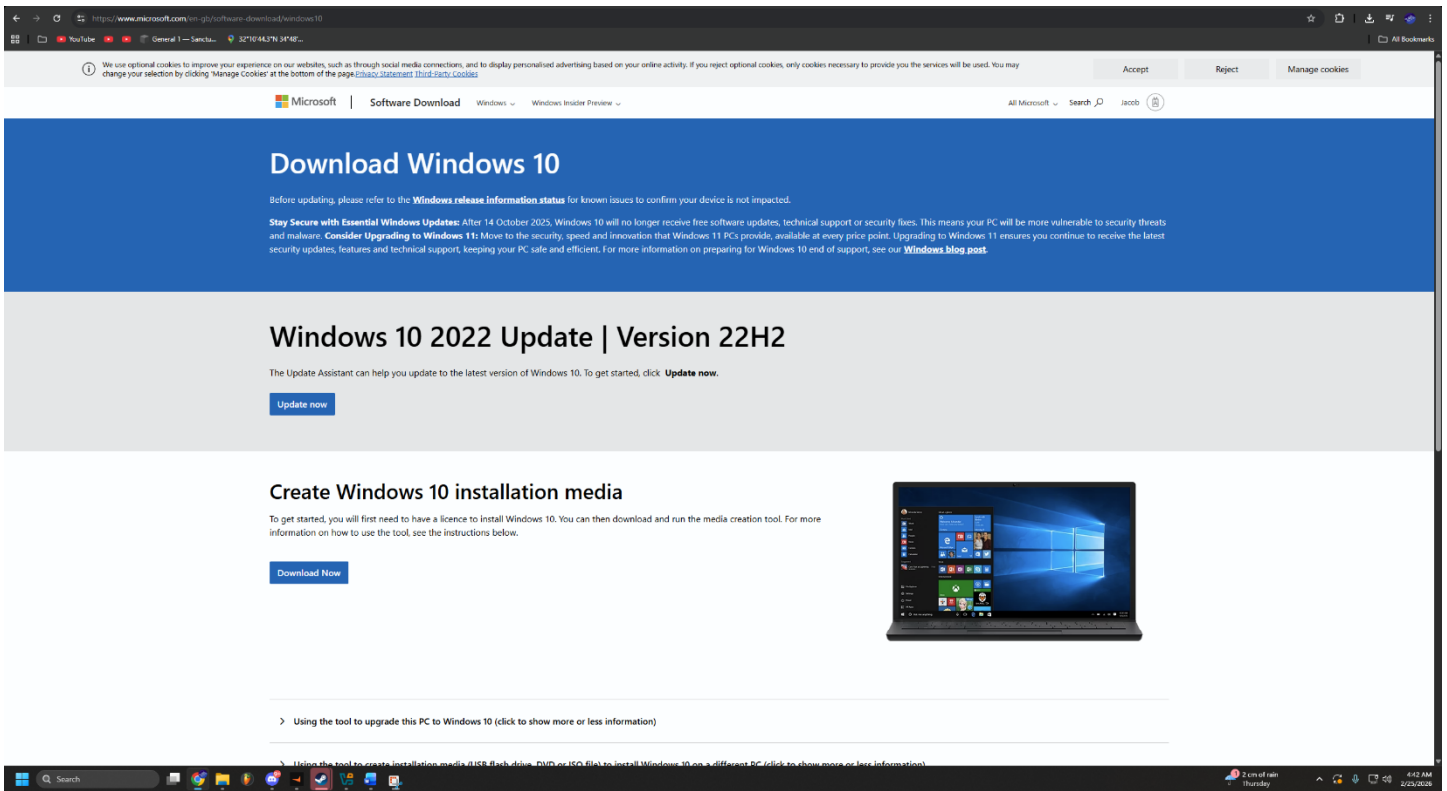
While Type 1 hypervisors offer stronger isolation and are more common in enterprise networks, a Type 2 hypervisor was chosen for the implementation of NOSS2026's topology. Due to the limited number of VMs, the performance gains of a bare metal hypervisor are outweighed by the flexibility and ease of deployment associated with a hosted hypervisor. While Type 1 hypervisors are inherently more secure, a Type 2 hypervisor can be secured through best practices such as continuous monitoring, a principle of the Zero Trust Architecture.

3.2 Environment Setup and Deployment

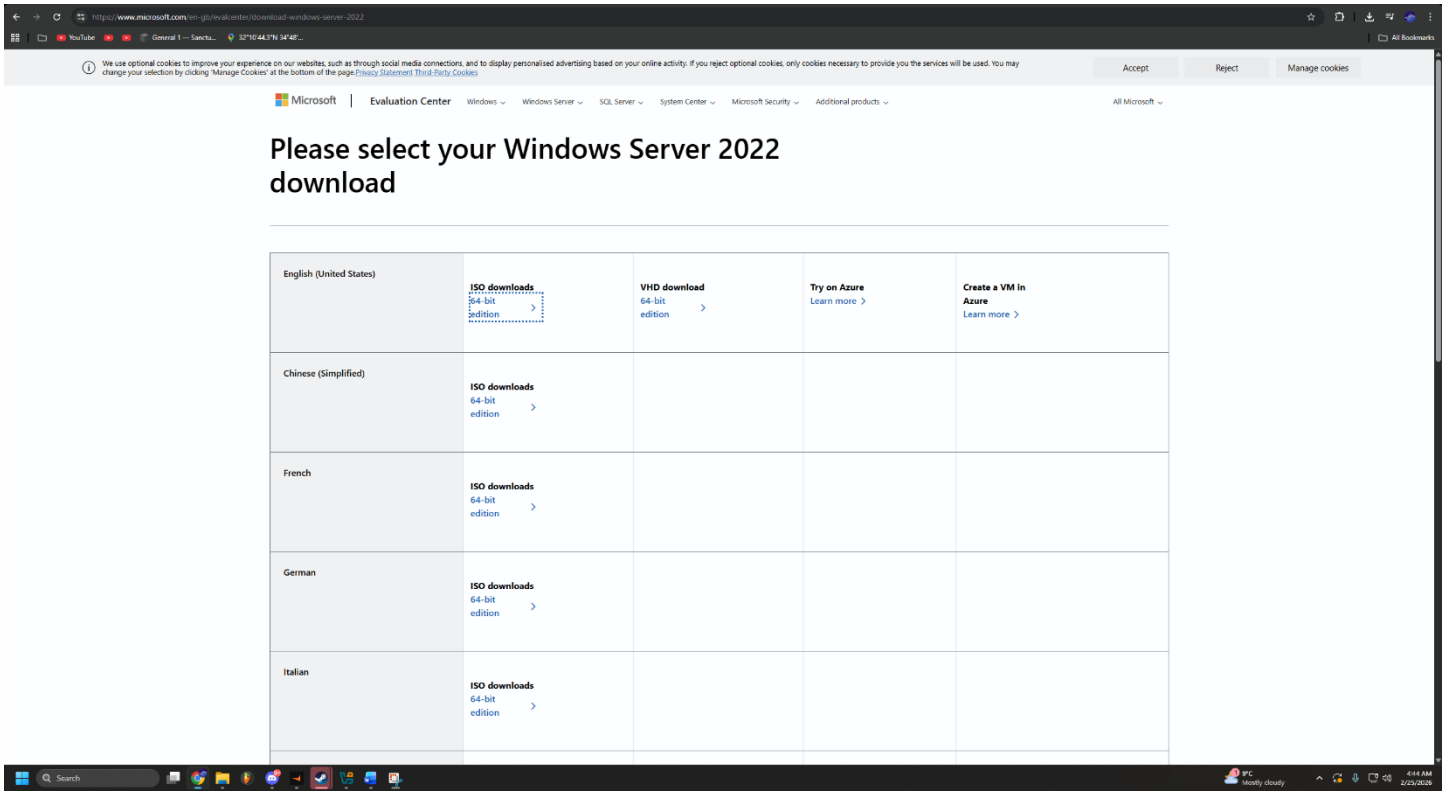


[Figure 1: VirtualBox Source]

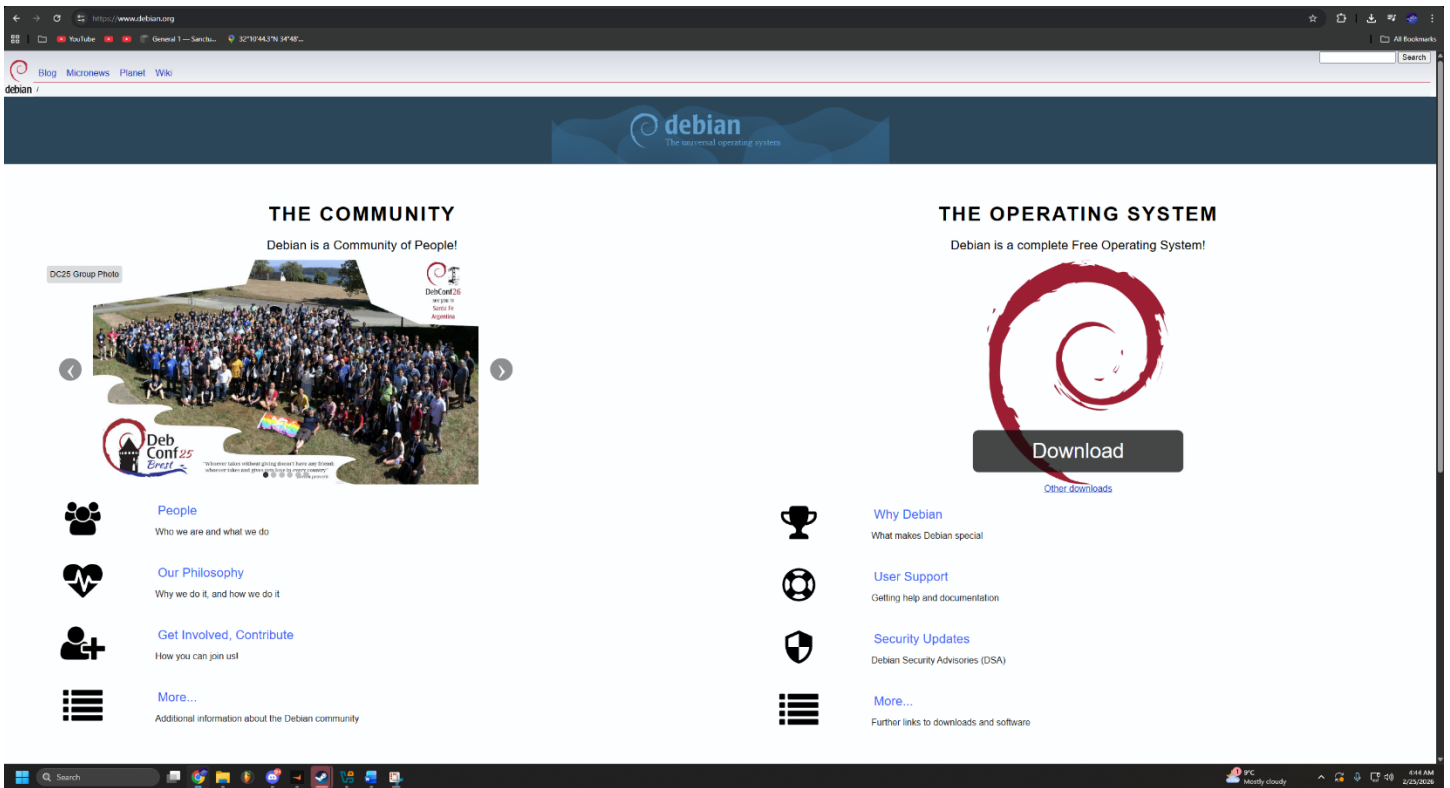
The chosen hypervisor software was VirtualBox, due to its ease of configuration and a prior familiarity with the application. The latest stable release was downloaded from the official website and installed in preparation for deployment of the VMs.



[Figure 2: Windows 10 Client Source]

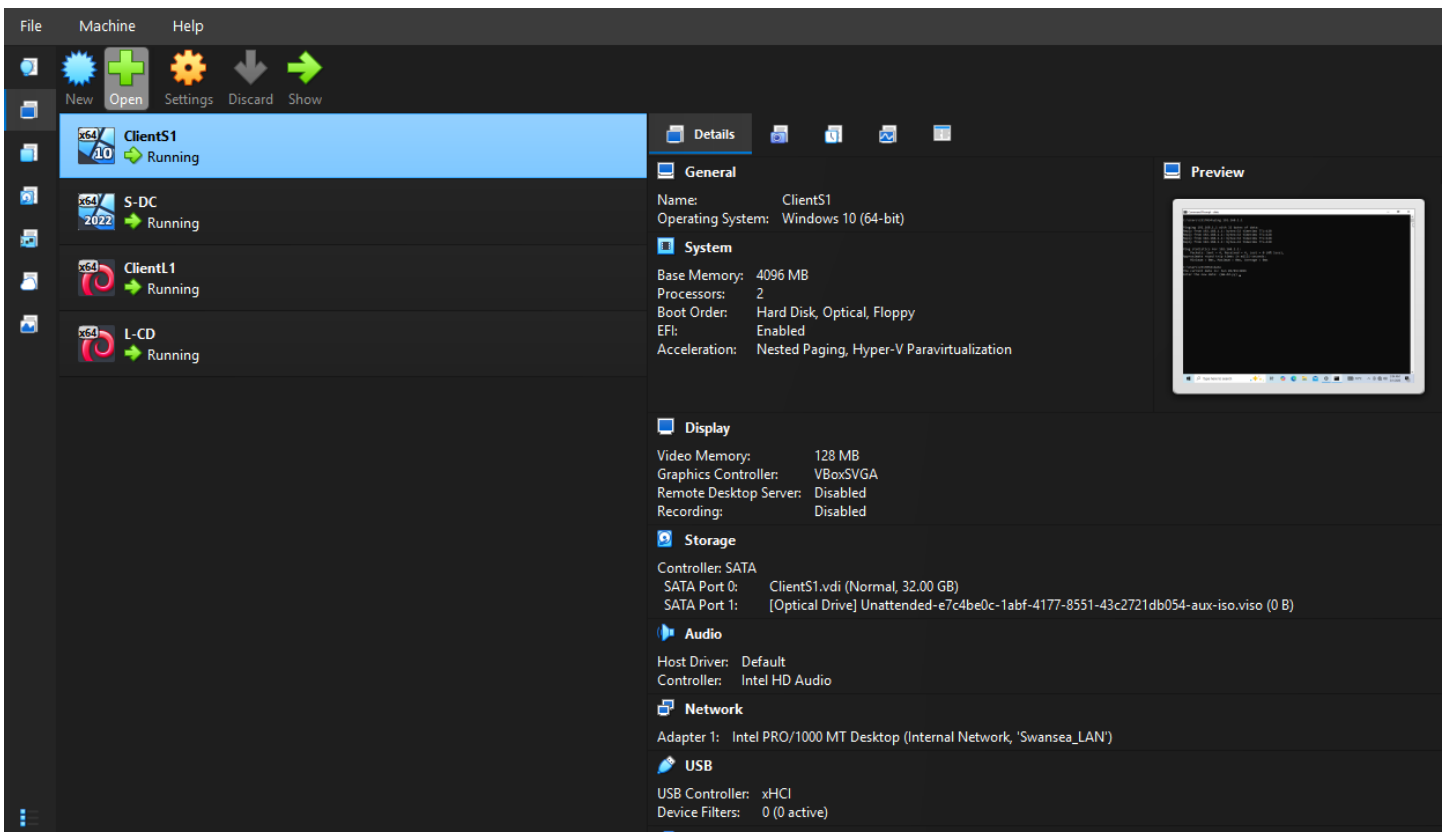


[Figure 3: Windows Server 2022 Source]



[Figure 4: Debian Source]

Windows 10 client, Windows Server 2022 and Debian ISOs were obtained from their respective official sources. The most recent stable release was selected in order to ensure both compatibility and security.



[Figure 5: Virtual Machine Deployment]

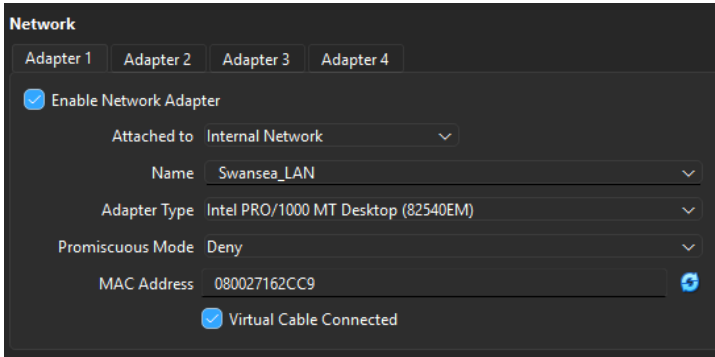


[Figure 6: CPU Allocation]

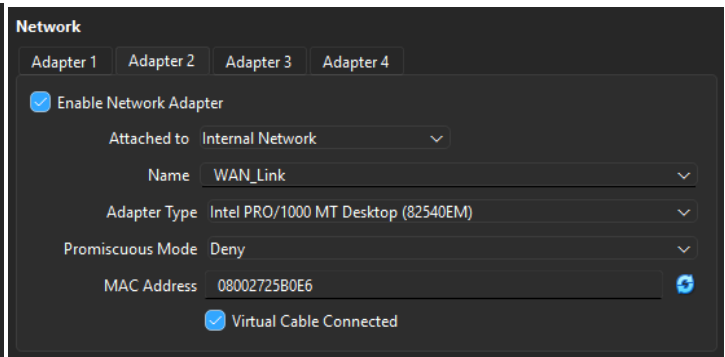


[Figure 7: RAM Allocation]

The three ISOs were installed onto four individual VMs, with the Debian distribution providing both the CLI and GUI environments for the simulated server and client. Each VM was allocated 2 virtual CPUs, 4096 MB of RAM and between 32 GB and 64 GB of virtual disk storage, depending on operating system requirements. This allocation was selected to provide sufficient processing and memory capacity to support the stable operation of each virtualised environment without overcommitting the host machines system resources.



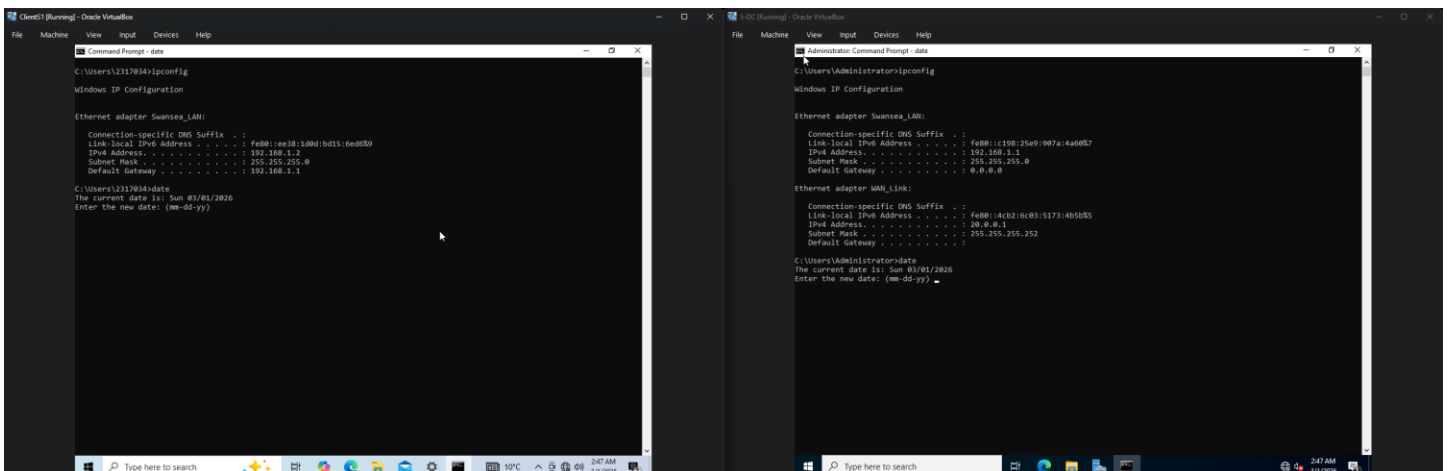
[Figure 8: LAN Adapter Setup]



[Figure 9: WAN Adapter Setup]

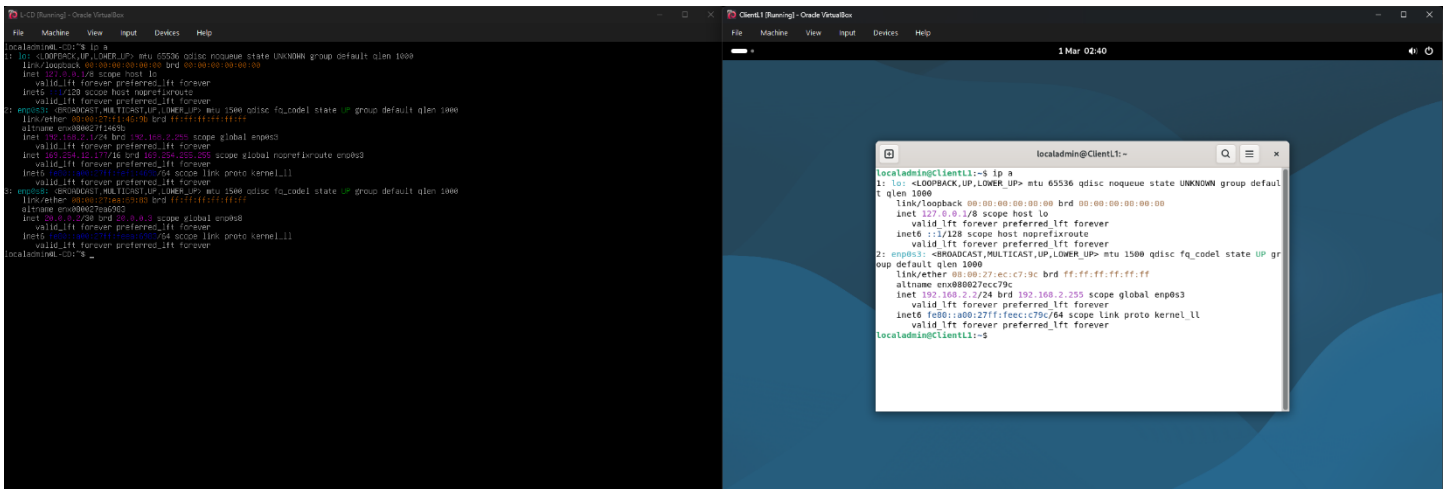
Both the WAN and LAN network adapters were set up within their respective VMs. All VMs were configured with LAN adapters, enabling communication within their assigned subnets. Both the Debian and Windows Server 2022 VMs were configured with an additional WAN adapter in order to facilitate communication between the two subnets. All adapters were configured with VirtualBox's Internal Network mode to simulate the isolated network segments while the "Virtual Cable Connected" option ensured a link between individual interfaces.

3.3 IP Addressing Implementation



[Figure 10: Windows Adapter Configuration]

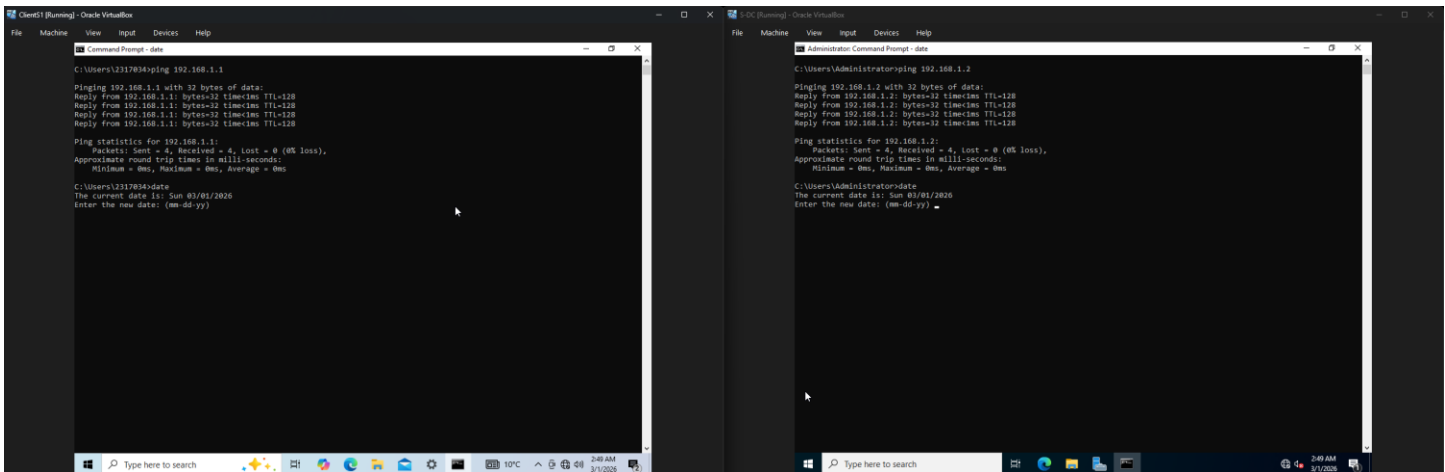
Both Windows machines were configured using the provided IP address schema within NOSS2026's topology. LAN adapters were assigned static IP addresses and subnet masks to ensure communication within their subnets. The Windows client was also assigned a default gateway pointing to the server. The WAN adapter on the Windows Server 2022 did not require a default gateway and therefore was left blank due to it functioning as a router between subnets.



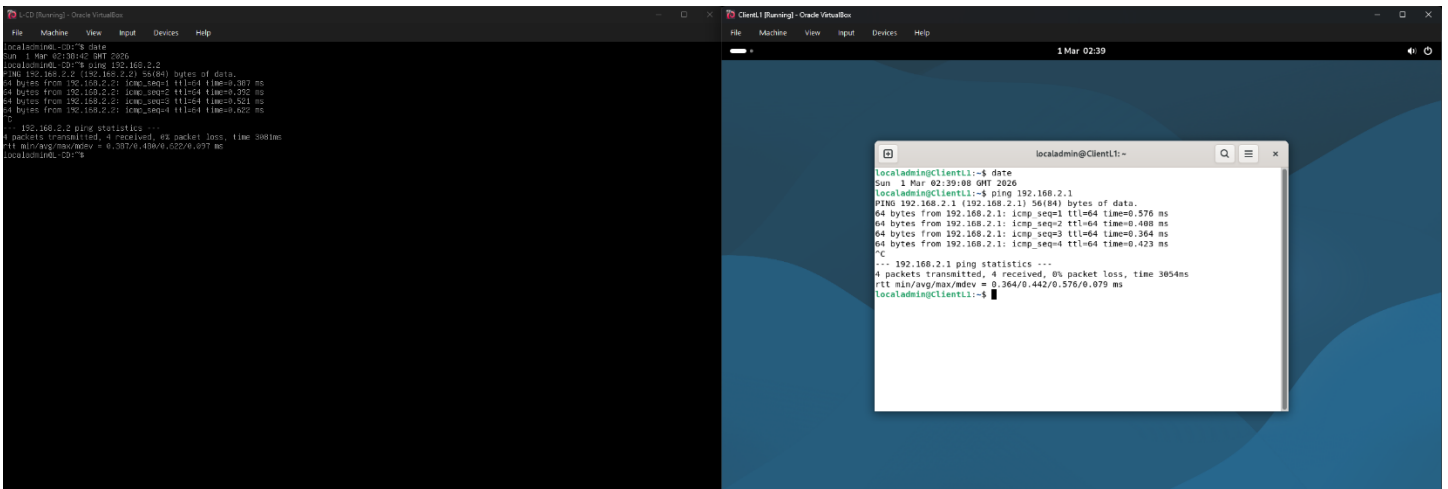
[Figure 11: Debian Adapter Configuration]

Both Debian machines were configured using the provided IP address schema within NOSS2026’s topology. The architecture remained the same as the two Windows systems with both the client and the server being assigned static IP addresses, subnet masks and default gateways where applicable. The WAN adapter on the Debian server was also configured according to the provided topology.

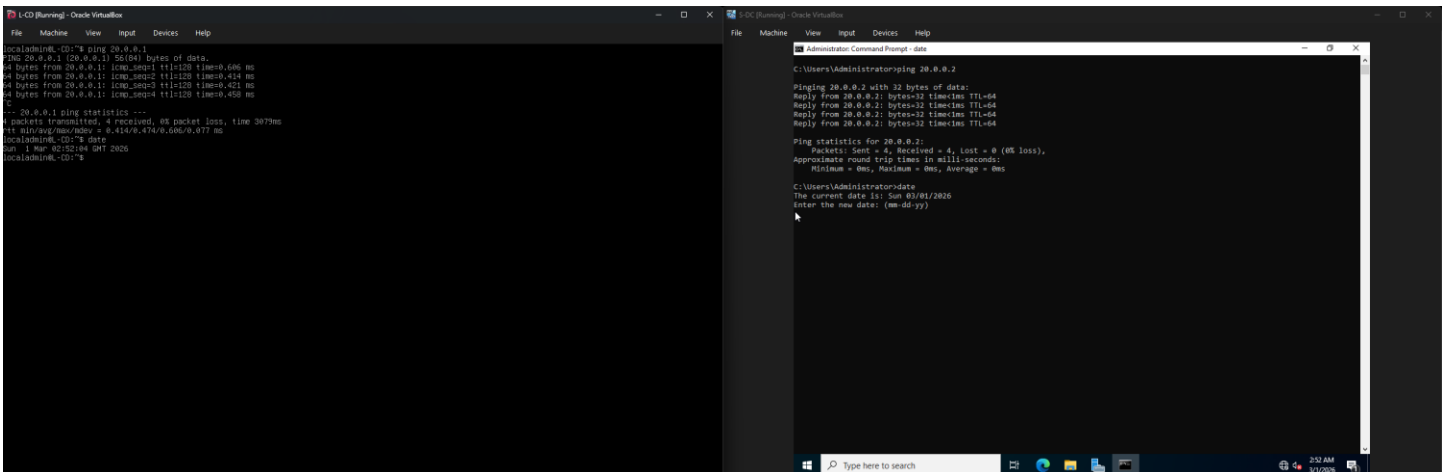
3.4 Testing and Troubleshooting



[Figure 12: Windows VMs Ping]

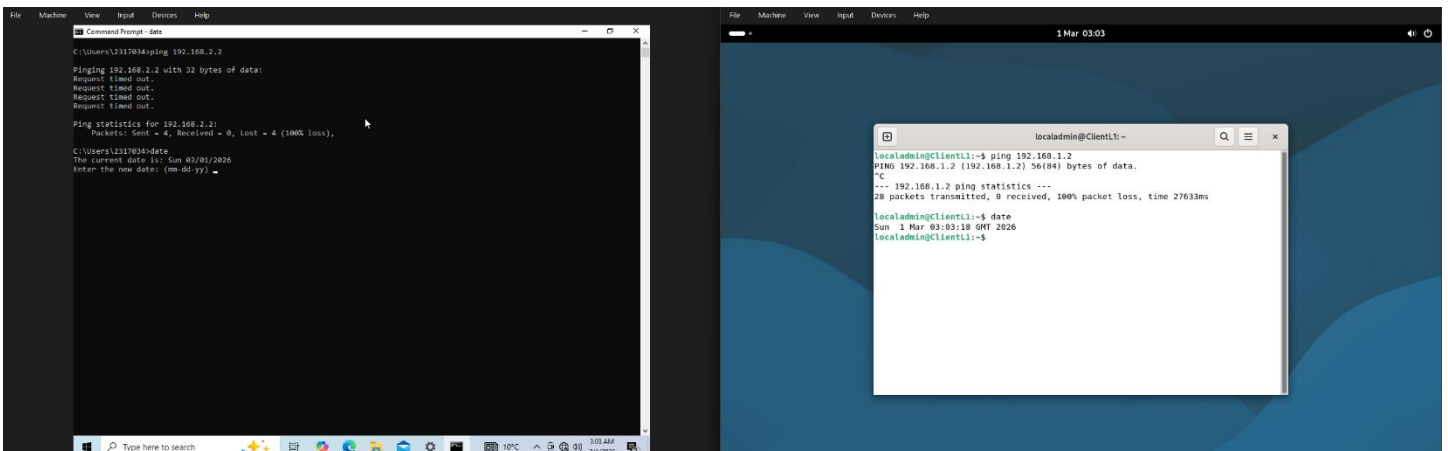


[Figure 13: Debian VMs Ping]



[Figure 14: Windows Debian VMs Ping]

Once all IPs were configured within their respective VMs, connectivity testing was performed by sending a ping. As demonstrated in Figure 12 and Figure 13, a successful ping was sent between both the servers and clients, showcasing successful connectivity within the same subnet. Figure 14 further illustrates a successful ping between each subnet via both the Windows Server 2022 and Debian systems.



[Figure 15: Failed Ping between Networks]

Figure 15 illustrates an unsuccessful ping between the two clients located within separate subnets. This confirms direct communication across two networks was restricted, satisfying Outcome 2: Unsuccessful connectivity within different networks.

4. Reflection

This section covers both a technical and personal reflection regarding the implementation of NOSS2026's topology.

4.1 Technical Reflection

NOSS2026's provided topology was implemented successfully, using VMs to simulate a segmented network environment while configuring both static IPs and routing to enable communication between systems and subnets. During development connectivity issues occurred when initially trying to ping between Windows client and server due to misconfigured adapter properties within VirtualBox. This was diagnosed using the command `ipconfig` within the terminal to check adapter properties, showing that all network adapters were attached to NAT in place of Internal Network. In order to resolve this issue all adapters within VirtualBox were attached to Internal Network and all names were adjusted to ensure clients match their corresponding server. Following this adjustment, connectivity between systems was reinstated.

4.2 Personal Reflection

Throughout this assignment, I feel I have gained a practical understanding of segmented networks, routing and hypervisors. The implementation of the provided topology has further reinforced my theoretical knowledge, giving me a deeper understanding of how interconnected networks function. Deploying the Debian server has also made me more confident working with command line tools, an area I was reasonably unfamiliar with before this project. While implementation was a success, I recognise I could have managed my time more effectively, which could have allowed me to design and implement my own IP schema.

5. References

- [1] Amazon Web Services, "Type 1 vs Type 2 Hypervisors - Difference Between Hypervisor Types - AWS," *Amazon Web Services, Inc.* Available: <https://aws.amazon.com/compare/the-difference-between-type-1-and-type-2-hypervisors/> (Accessed: Feb. 28)
- [2] K. Scarfone, M. Souppaya, and P. Hoffman, "Guide to Security for Full Virtualization Technologies Recommendations of the National Institute of Standards and Technology Special Publication 800-125." Available: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-125.pdf> (Accessed: Feb. 28)
- [3] N. Kaliyamurthy, *Understanding Networks – Network Operating Systems and Services (ACCA5023)*, Week 1 Lecture Slides, Applied Computing – WISA, University of Wales Trinity Saint David (Accessed: Feb. 28)
- [4] C. Semeria, "Understanding IP Addressing," Available: www.osburn.com <https://www.osburn.com/ip/> (Accessed: Feb. 28)
- [5] N. Kaliyamurthy, *Routing – Network Operating Systems and Services (ACCA5023)*, Lecture 4 Slides, University of Wales Trinity Saint David, Applied Computing – WISA, 2026 (Accessed: Mar. 1)
- [6] P. Ferguson and G. Huston, "What is a VPN?," 1998. Available: <http://sol.te.net.ua/www/nanog/vpn.pdf> (Accessed: Mar. 1)
- [7] Microsoft Azure, "What is a VPN? Why Should I Use a VPN?," *azure.microsoft.com*, 2024. Available: <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn> (Accessed: Mar. 1)
- [8] NCSC, "Virtual Private Networks (VPNs)," *www.ncsc.gov.uk*, Jun. 29, 2021. Available: <https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks> (Accessed: Mar. 1)
- [9] Microsoft, "Dynamic Host Configuration Protocol (DHCP)," *learn.microsoft.com*, May 13, 2025. Available: <https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top> (Accessed: Mar. 1)
- [10] P. V. Mockapetris, "Defending your DNS & DHCP — Best Practices," *Network Security*, vol. 2003, no. 6, pp. 7–10, Jun. 2003, Available: [https://doi.org/10.1016/s1353-4858\(03\)00609-3](https://doi.org/10.1016/s1353-4858(03)00609-3) (Accessed: Mar. 1)
- [11] Microsoft, "Active directory domain services overview," *Microsoft*, Mar. 11, 2025. Available: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview> (Accessed: Mar. 1)
- [12] Microsoft, "Best Practices for Securing Active Directory," *learn.microsoft.com*, Nov. 10, 2023. Available: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory> (Accessed: Mar. 1)
- [13] "Certificates Authorities should be highly available and resilient to both attack and failure," *Ncsc.gov.uk*, 2024. Available: <https://www.ncsc.gov.uk/collection/in-house-public-key-infrastructure/pki-principles/certificates-authorities-should-be-highly-available-and-resilient-to-both-attack-and-failure> (Accessed: Mar. 1)