



ACCB5023: NETWORK OPERATING

Coursework 1: Research, build, and deploy a Virtualised Enterprise
network

Word count:

Task 1 – 1,039

Task 2 – 1,250 equivalent

Task 3 – 259

Joe Frohwein

2315545

2315545@student.uwtsd.ac.uk
Computing (Software Engineering)

Contents

1. Research	2
1.1. Hypervisor.....	2
1.2. IP Addressing	2
1.3. Routing	4
1.4. Network Services	5
2. Technical Documentation	6
2.1. Choose your Hypervisor	6
2.2. Download and Setup	7
2.2.1. Download the chosen Hypervisor and Server, Client Operating Systems for the relevant Sources	7
2.2.2. Deploy your network as per the given topology	9
2.3. Configure IP Addressing.....	16
2.3.1. Appropriate IP Addressing	16
2.4. Test and Troubleshoot	20
2.4.1. Perform Connectivity tests	20
3. Reflection.....	26
3.1.1. Write a Technical reflection covering network deployment and testing	26
3.1.2. Write your Personal Reflection	26
4. References.....	27

1. Research

1.1. Hypervisor

A hypervisor is “software that creates and runs virtual machines (VMs)”, allowing a host computer to “support multiple guest VMs by virtually sharing its resources, such as memory and processing” [1].

Type-1 (“bare-metal”) Hypervisors run directly on hardware and “negotiate directly with server hardware to allocate dedicated resources to VMs” without a host OS [2], [3]. This reduced architectural layer enhances isolation, scalability and performance, reducing attack surface by eliminating dependency on the host OS.

Type-2 (“hosted”) Hypervisors rely on the host OS for resource allocation, introducing additional processing overhead and increased attack vulnerability due to host OS dependency, meaning a compromised host could impact all VMs. However, as they are installed on the host, requiring no “bare-metal” servers, they are far easier to install [2], [3].

For the specified network topology, the SWANSEA.ACCA domain environment, a Type-2 hypervisor, such as Oracle VM VirtualBox, would be sufficient. As the topology is a controlled desktop development environment rather than an enterprise-level environment, the enhanced scalability and high availability capabilities of type-1 would be surplus to operational requirements, due to its small-scale, fixed size and non-necessity to be operational 24/7. The requirement for cross-platform compatibility between Windows and Debian VMs on an existing host OS, alongside potential limitations in RAM and CPU, further supports this decision.

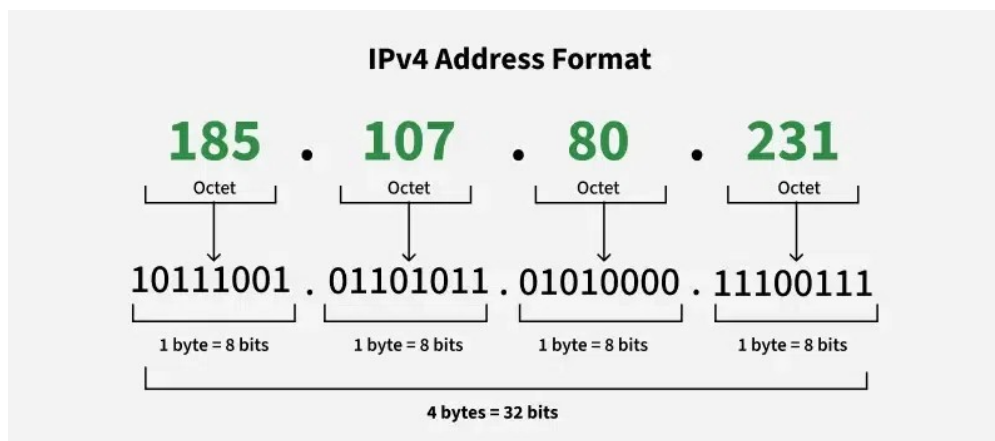
Although a Type-1 hypervisor provides superior isolation, scalability and performance, these advantages would only become essential if the network were to expand to that of an enterprise-level network. Therefore, due to its scale, enhanced performance and isolation are traded for the ease of deployment and management of type-2 [3], [4], [5].

1.2. IP Addressing

An IP address is “the core of the TCP/IP protocol that is responsible for communication between networks and the internet”, defining how data is transmitted [6]. Each network device is assigned a unique identifier. Data transmission involves encapsulating data into a ‘packet’ containing source and destination IP addresses, and forwarding it through routers, which route packets between networks, and switches, which handle packets within a local

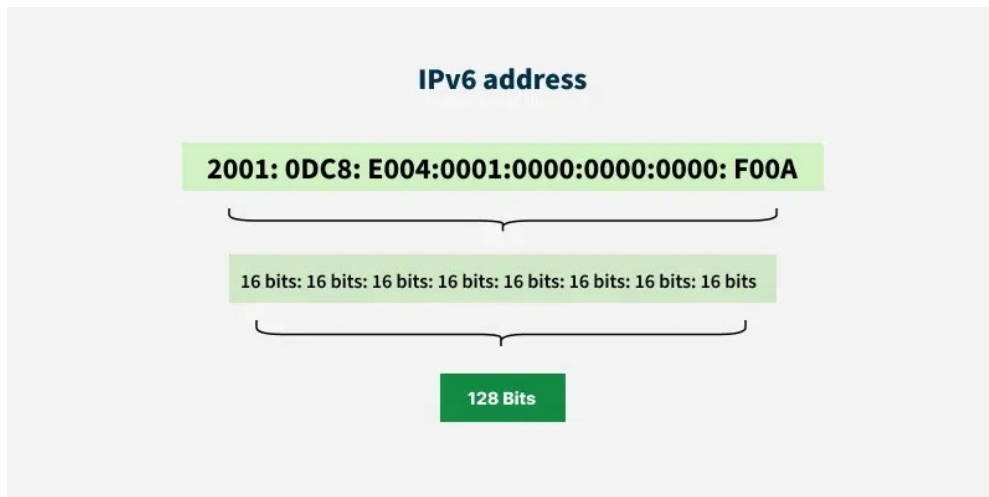
network, until the destination is reached [6]. This demonstrates the contributions of IP Addressing to network functionality through unique device identification and addressing [7], [8].

IPv4 addresses, the most common IP format, are “composed of a 32-bit binary number, divided into four 8-bit segments”, with octets ranging from 0-255 (e.g. 192.168.1.2). Each address contains ‘network’ and ‘host’ identifiers. IPv4’s main limitation is its “finite number of possible combinations”, which, due to the rapid growth of networks, led to the development of IPv6 [9].



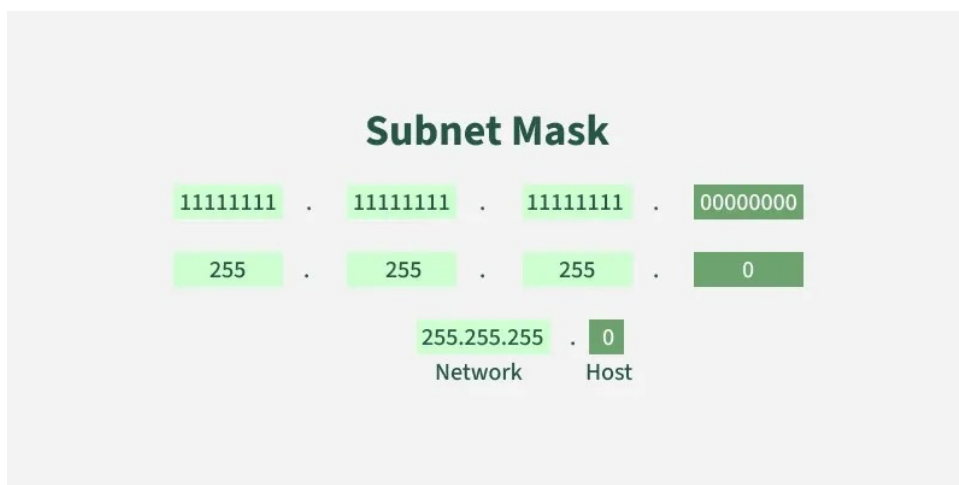
(Figure 1.2.1 – The structure of an IPv4 address [10])

IPv6 addresses are “128 bits long and expressed in hexadecimal notation” (e.g. 2001:0db8:85a3:0000:0000:8a2e:0370:7334), structured to provide “more flexibility and efficiency in routing and addressing allocation”. Each address includes a global routing prefix (2001:0db8:85a3), subnet ID (0000:0000) which “identifies the network”, and interface ID (8a2e:0370:7334) which “distinguishes the individual host”. IPv6 provides “virtually unlimited” scalability, mandatory security specifications, enhanced routing efficiency, and automatic configuration [9], [11].



(Figure 1.2.2 – The structure of an IPv6 address [12])

Subnetting is “used to divide a larger network into smaller sub-networks or subnets”, using a forward-slash at the end of the address to indicate the network portion. For example, “192.168.1.0/24 indicates that the first 24 bits are allocated for the network portion, leaving 8 bits for host addresses”, providing improved performance and efficient IP utilisation [9], [11].



(Figure 1.2.3 – The structure of a subnet mask [13])

1.3. Routing

Routing is a Layer 3 network function in which routers consult routing tables to optimally forward packets between networks, enhancing efficiency, scalability and redundancy [14], [15].

Static routing involves manually configured routes, with a fixed routing table populated by a network administrator [6]. It is used for a single or preferred route, resulting in small routing tables and minimal computation. However, static routes must be reconfigured whenever the

topology changes, reducing adaptability, which can become time-consuming in an expanding network [16].

Dynamic routing uses routing algorithms on each router which automatically “generate and maintain routing tables through the exchange of routing information” [6]. Examples of dynamic routing protocols include RIP, OSPF and BGP [17]. It is better suited to larger or changing topologies as it provides automated re-routing, but it introduces additional complexity and higher bandwidth requirements [16].

In this small-scale network, where the Debian server operates as a DHCP relay forwarding client requests to the Windows server, static routing is sufficient [18]. Because traffic routes are fixed and predictable, static routing provides reliable, efficient delivery with minimal bandwidth and administrative changes required. Dynamic routing would provide unnecessary complexity, exceeding operational needs in this small, fixed network. It could also introduce security risks if automatic updates are not authenticated and secured [19], unlike static routing with fixed entries.

Therefore, static routing meets the operational and security requirements of the SWANSEA.ACCA network, providing predictable, predefined network paths and minimal administrative intervention.

1.4. Network Services

Virtual Private Networks (VPN) “provide secure connectivity between devices in physically separate locations” across untrusted networks by creating encrypted tunnels that protect data integrity and confidentiality. The key features of VPNs are data encryption and tunnelling, providing secure remote access and safeguarding internal networks from external attackers. Best practices include deploying robust encryption standards, implementing multi-factor authentication and enforcing clearly defined access controls to minimise potential attack surface [20], [21].

Dynamic Host Configuration Protocol (DHCP) is “a system for assigning Internet Protocol addresses” providing reliable IP address configuration and server management, reducing administrative overhead and preventing IP conflicts to improve operational efficiency. Structured DHCP policies and audit logging contribute to system governance. Best practices include implementing a structured IP address plan and avoiding overlapping static routes to provide enhanced scalability for future network development [22], [23], [24].

Active Directory Domain Services (ADDS) “stores information about objects on the network” in centralised stores, streamlining operations. It enforces diligent user authentication, ensuring only authorised users can access the data, alongside policy enforcement to maintain consistent security controls. Best practices include granting least-privilege access, securing administrative hosts and domain controllers and regular account and server auditing to reduce attack surface and detect access escalation attempts [25], [26], [27].

Certificate Authorities (CA) are “a trusted organization that issues digital certificates to websites” to validate ownership and enable encrypted communications between servers and clients. Key features include certification issuance, ongoing monitoring, and identity verification. Best practices include strict protection of root keys, controlled certificate issuance, and regular certificate auditing to maintain organisational trust and integrity [20], [21], [22].

2. Technical Documentation

2.1. Choose your Hypervisor

As stated in section 1.1, a type-2 hypervisor is most suitable for implementing the SWANSEA.ACCA network topology. This decision is supported by the considerations of cost efficiency, ease of deployment, scalability and security.

The cost efficiency of a type-2 hypervisor is greater than that of a type-1, as they are installed on existing host OS, eliminating the need for dedicated server hardware. Free and widely supported options, such as Oracle VM VirtualBox, further reduce costs, making them ideal for a small-scale network. As the network isn’t an enterprise-level network, investing in expensive a type-1 hypervisor and the required dedicated hardware, would be economically unjustifiable [23], [24].

A type-2 hypervisor is installed on an existing host OS, functioning as a desktop application, simplifying installation, configuration and management. This ease of use reduces operational overhead and allows simple modifications or expansions of the network, which will be advantageous for future work within this network [23].

Type-2 Hypervisors are scalable, as they can be cloned and deployed virtually to provide additional servers and clients where required. This means that the network can easily accommodate additional Windows or Debian servers and clients without purchasing new hardware, which is again vital for future developments to the network [3].

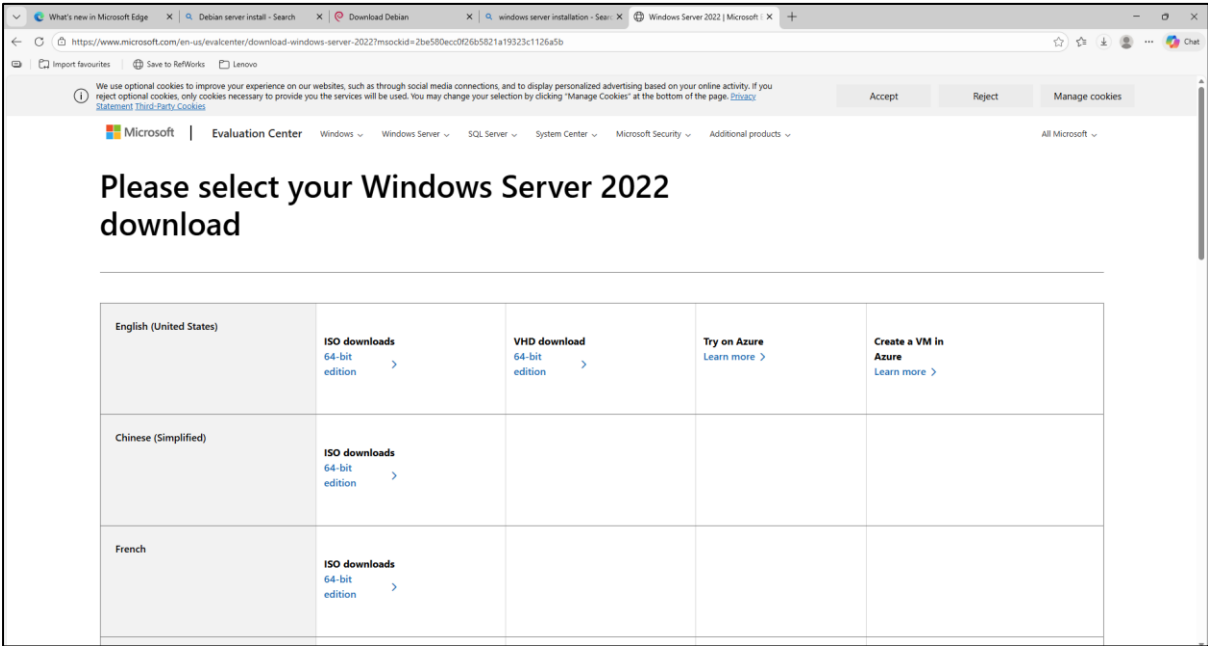
While type-1 hypervisors generally provide superior isolation, type-2 hypervisors are sufficiently secure for a network of this size, provided that the host has adequate and robust security. Given the scale of SWANSEA.ACCA, the risk of a security breach is manageable, through host OS updates and firewalls, and does not outweigh the other benefits previously mentioned [3].

In conclusion, a type-2 hypervisor will be used for the SWANSEA.ACCA network as it balances cost, usability, scalability and security while supporting additional network services which will be crucial for future developments in subsequent coursework.

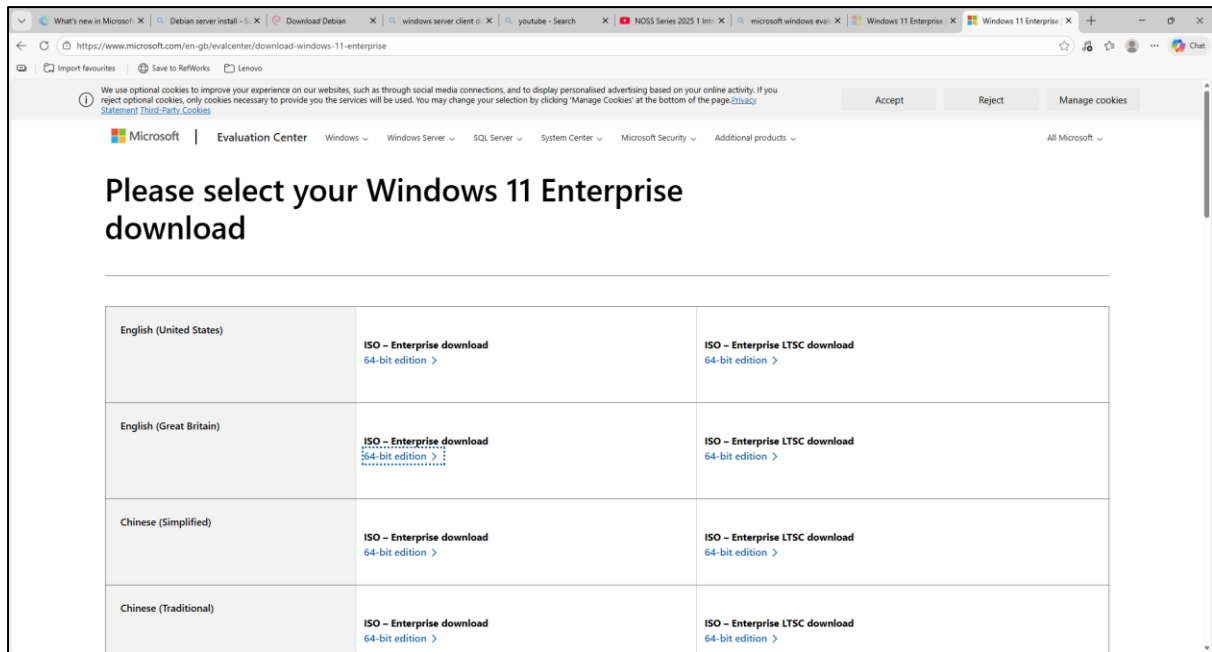
2.2. Download and Setup

2.2.1. Download the chosen Hypervisor and Server, Client Operating Systems for the relevant Sources

The Windows Server and Client ISO’s were downloaded from the official Microsoft website, to ensure that downloads were from reliable sources:

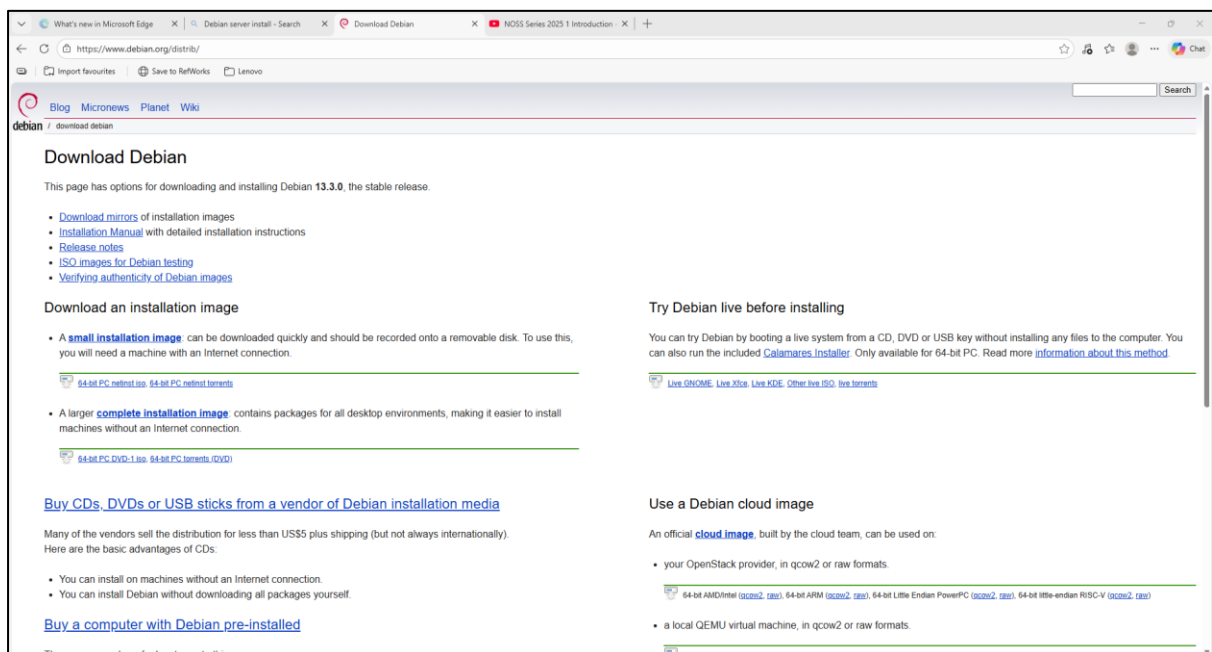


(Figure 2.2.1.1 – Downloading Windows Server 2022 from its relevant source)



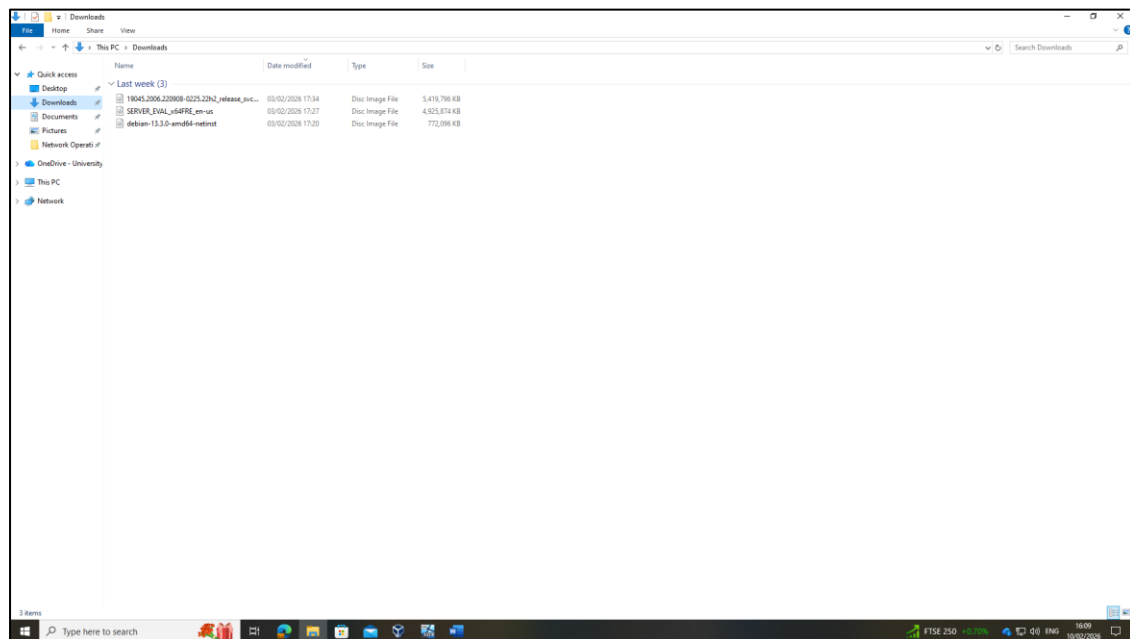
(Figure 2.2.1.2 – Downloading Windows 11 Enterprise from its relevant source)

The Debian ISO was downloaded from the official Debian website:



(Figure 2.2.1.3 – Downloading the Debian ISO from its relevant source)

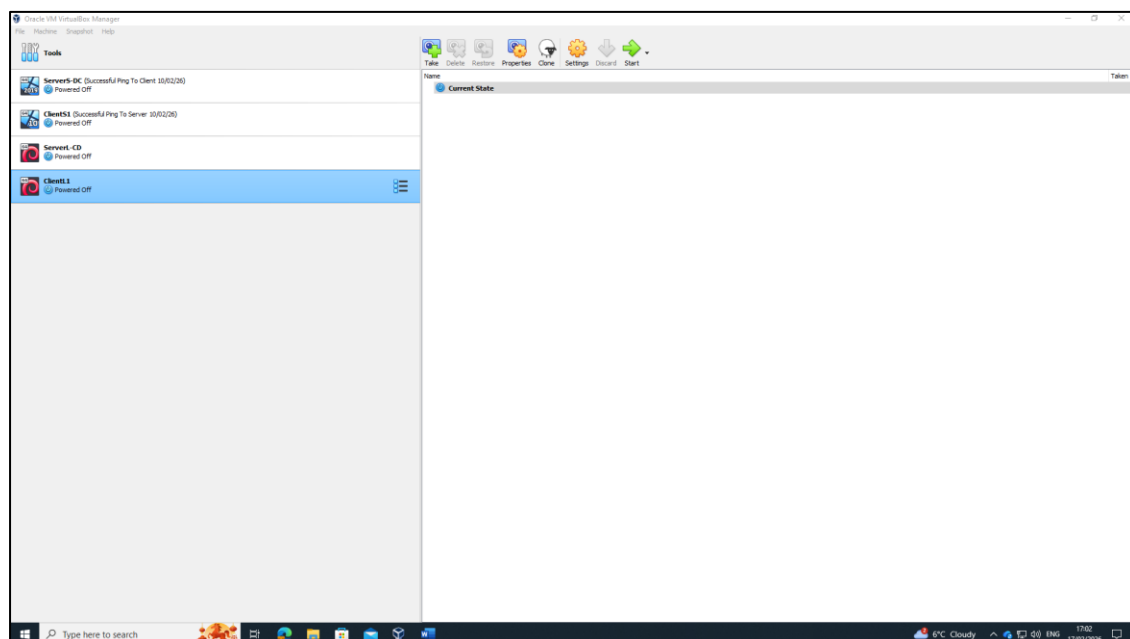
The downloaded ISO's were stored in the 'Downloads' section, ready for use:



(Figure 2.2.1.4 – All successfully downloaded files stored in the 'Downloads' section)

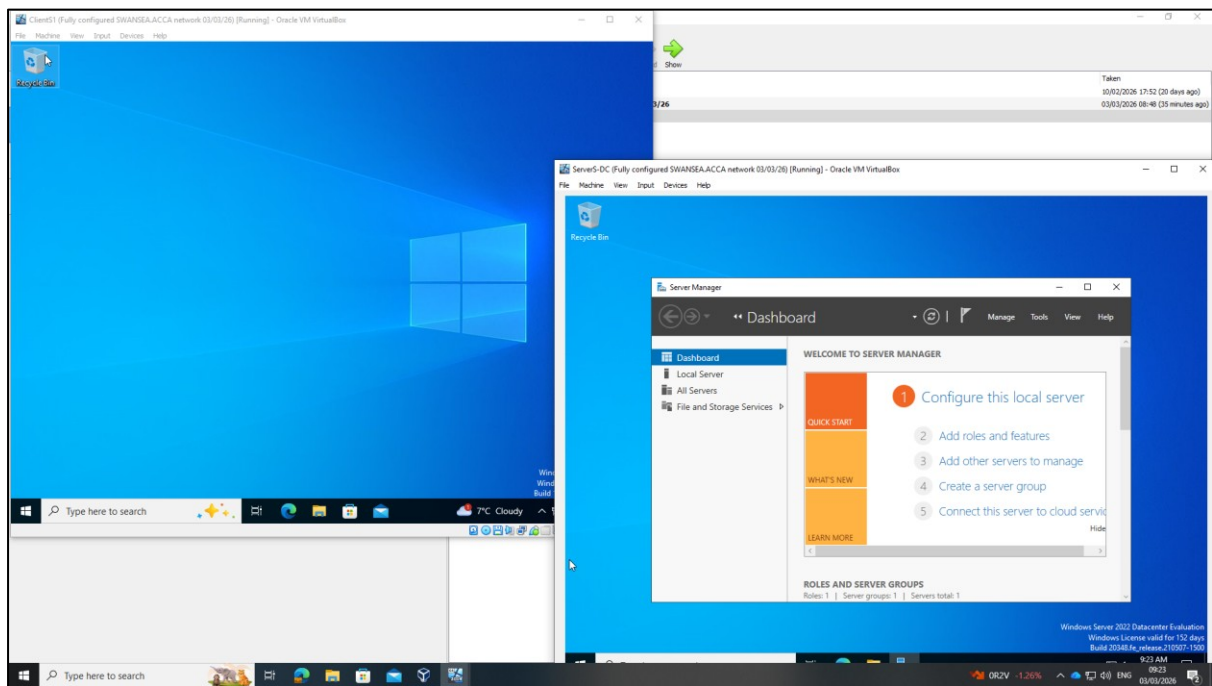
2.2.2. Deploy your network as per the given topology

Using Oracle VM VirtualBox, the Windows server and client VMs were set up, being assigned relevant names in 'ServerS-DC' for the Swansea server, and 'ClientS1' for the Swansea client. The Debian server and client VMs were also set up, being named 'ServerL-DC' for the London server, and 'ClientL1' for the London client:



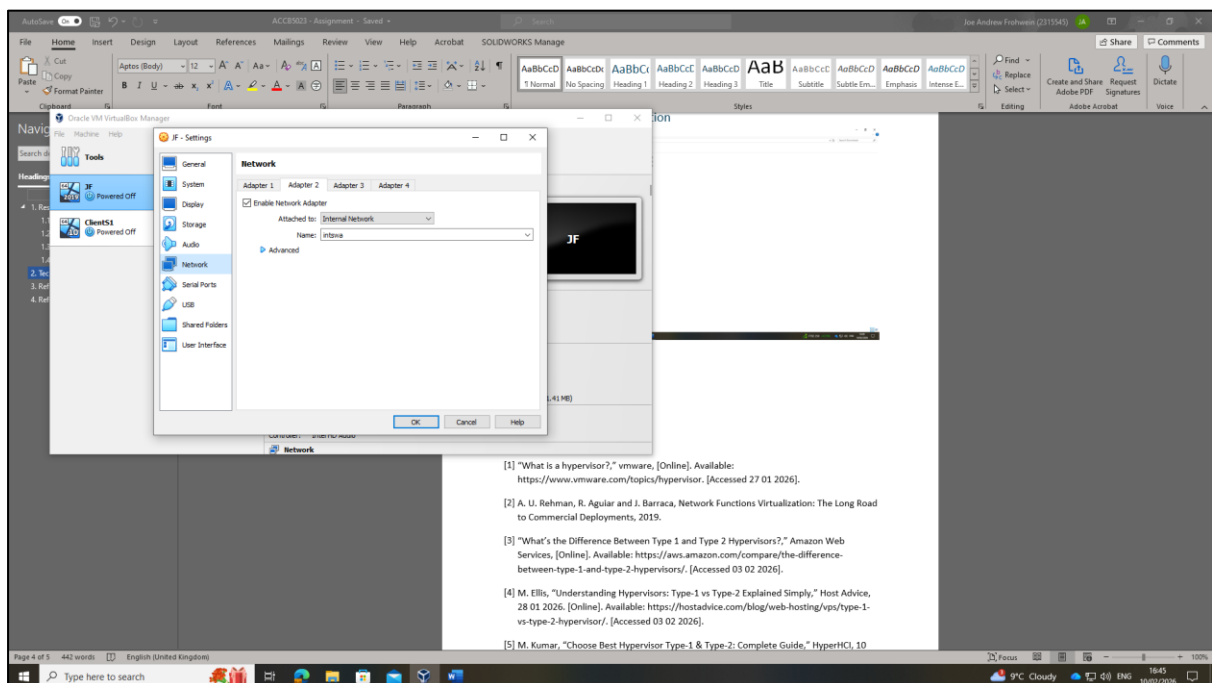
(Figure 2.2.2.1 – All four Virtual Machines successfully set up in Oracle VM VirtualBox)

The Swansea server and client were both functioning:

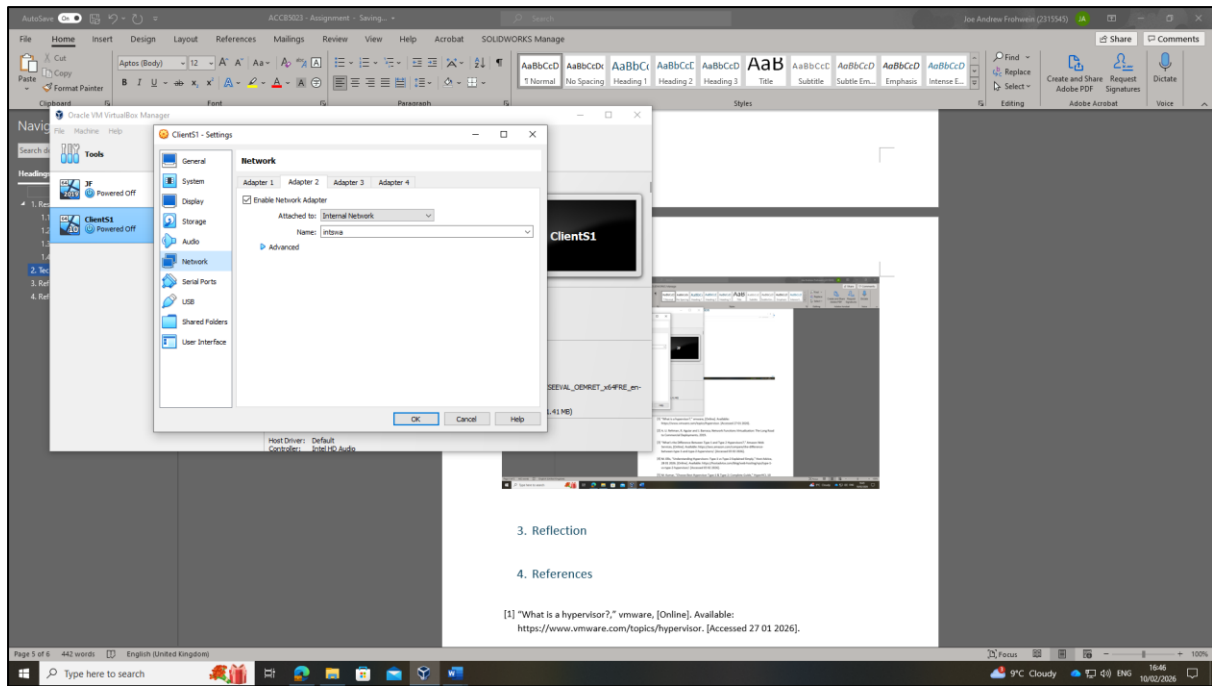


(Figure 2.2.2.2 – The Microsoft server and client both simultaneously running)

The internal adapters between the Swansea server (renamed from ‘JF’ after the following screenshots were taken) and client, named ‘intswa’ were set up on both VMs:

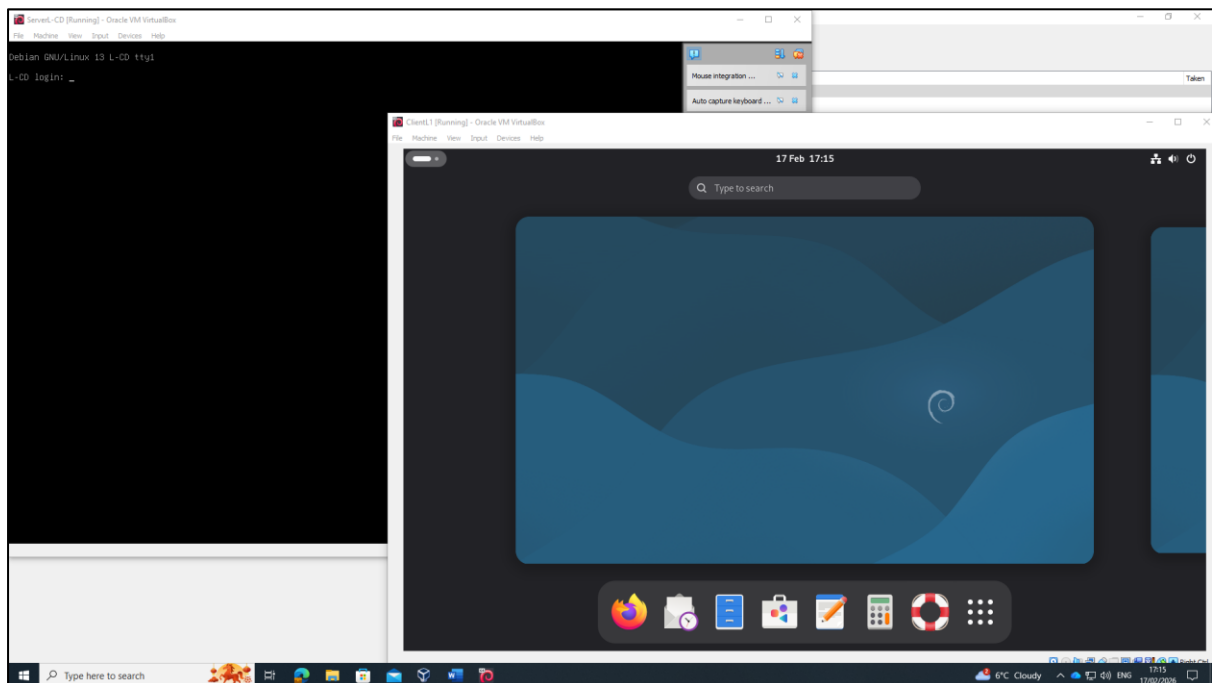


(Figure 2.2.2.3 – the internal adapter on the Microsoft server)



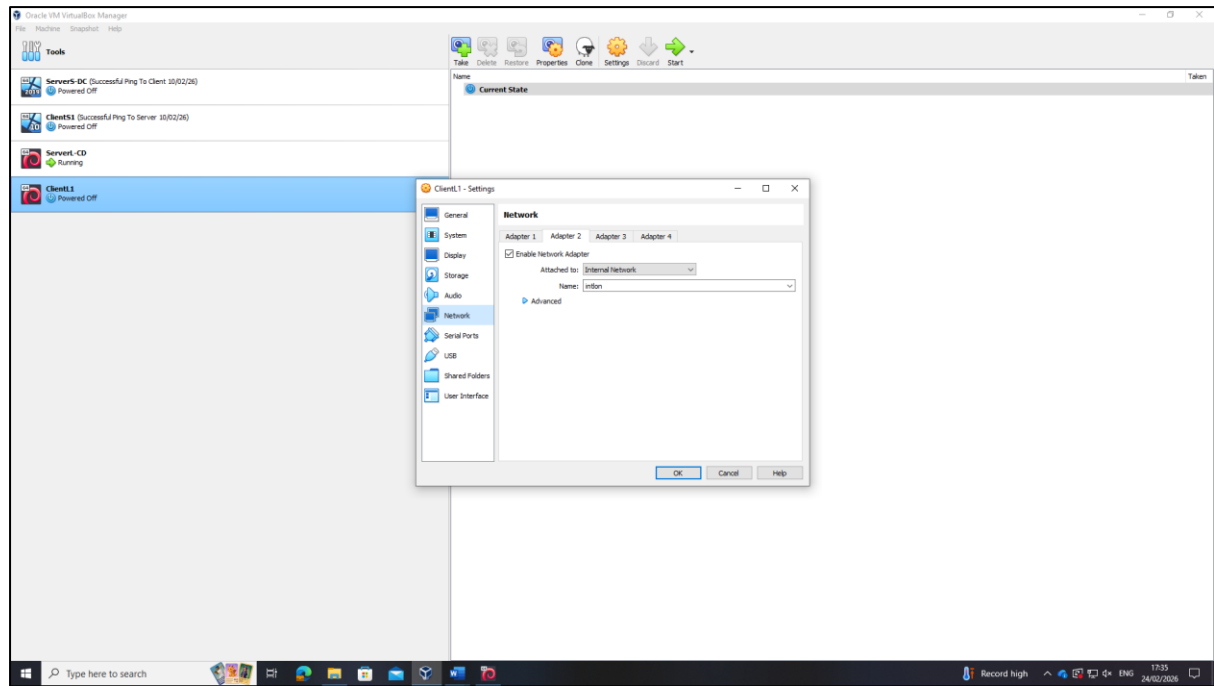
(Figure 2.2.2.4 – the internal adapter on the Microsoft client)

After the Swansea network was set up correctly, the London network was started. The Debian/Linux server and client were both functioning as a Command Line Interface and a Graphical User Interface, respectively:



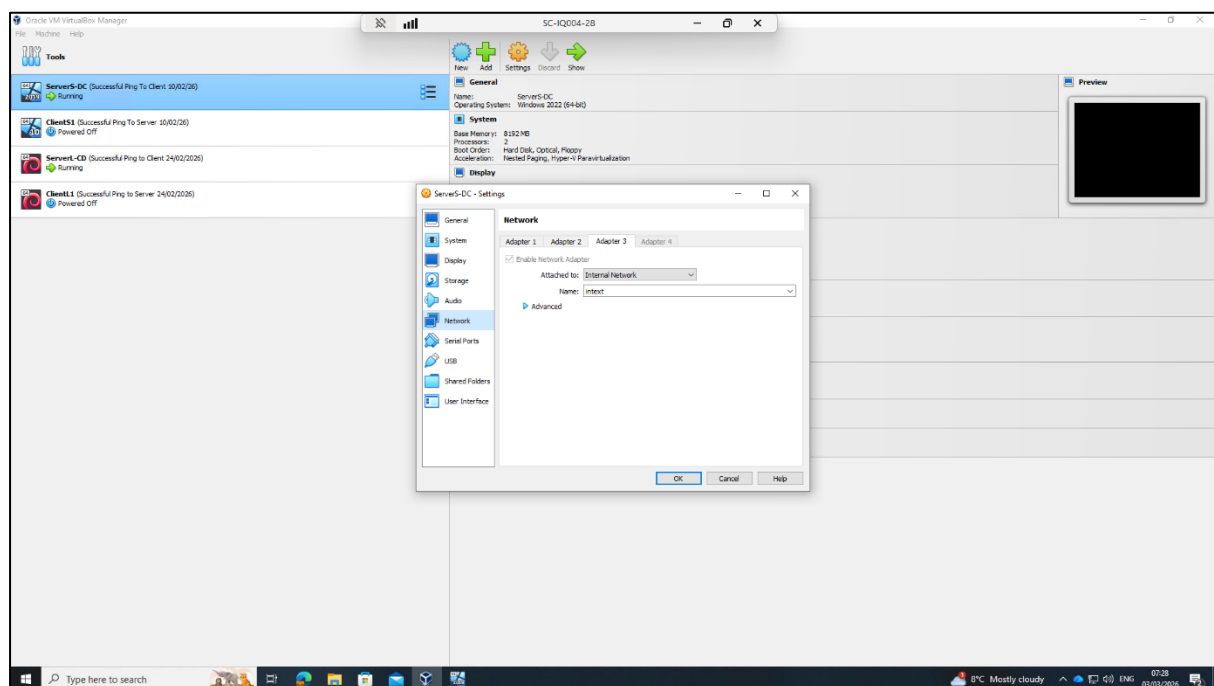
(Figure 2.2.2.5 – The Debian server and client both simultaneously running)

[illegible]

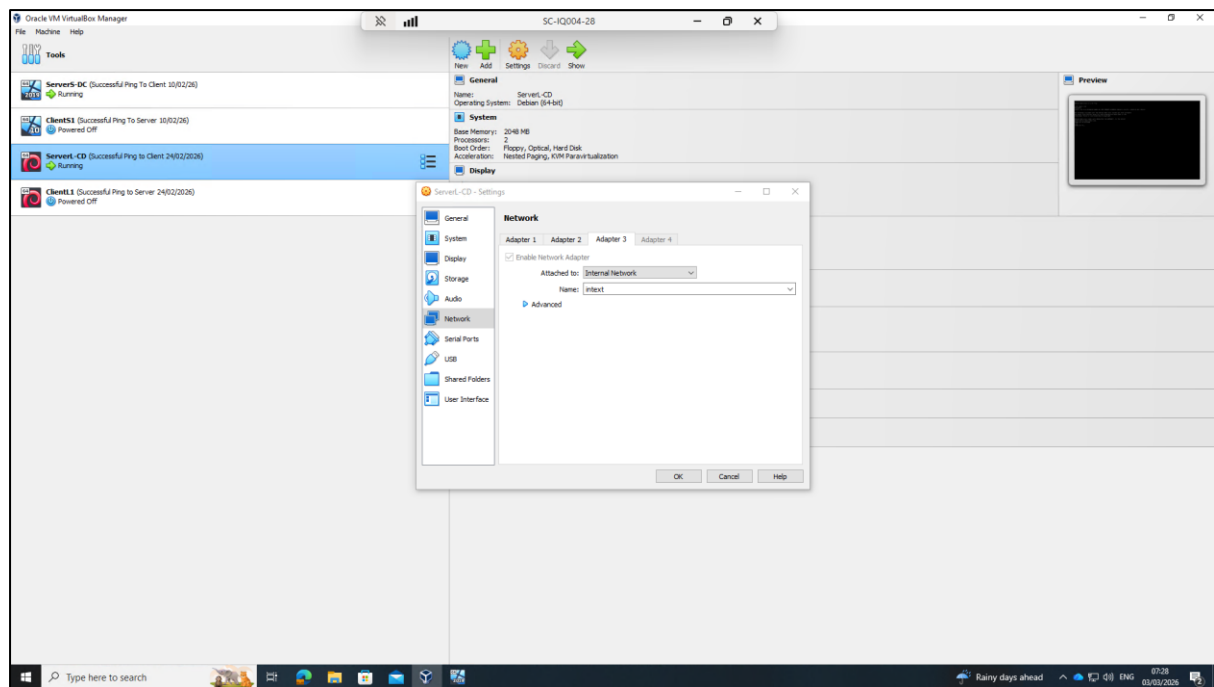


(Figure 2.2.2.8 – the internal adapter on the Debian client)

The external adapters of the two servers, named 'intext' were then set up so that connection could be made between the London and Swansea servers:

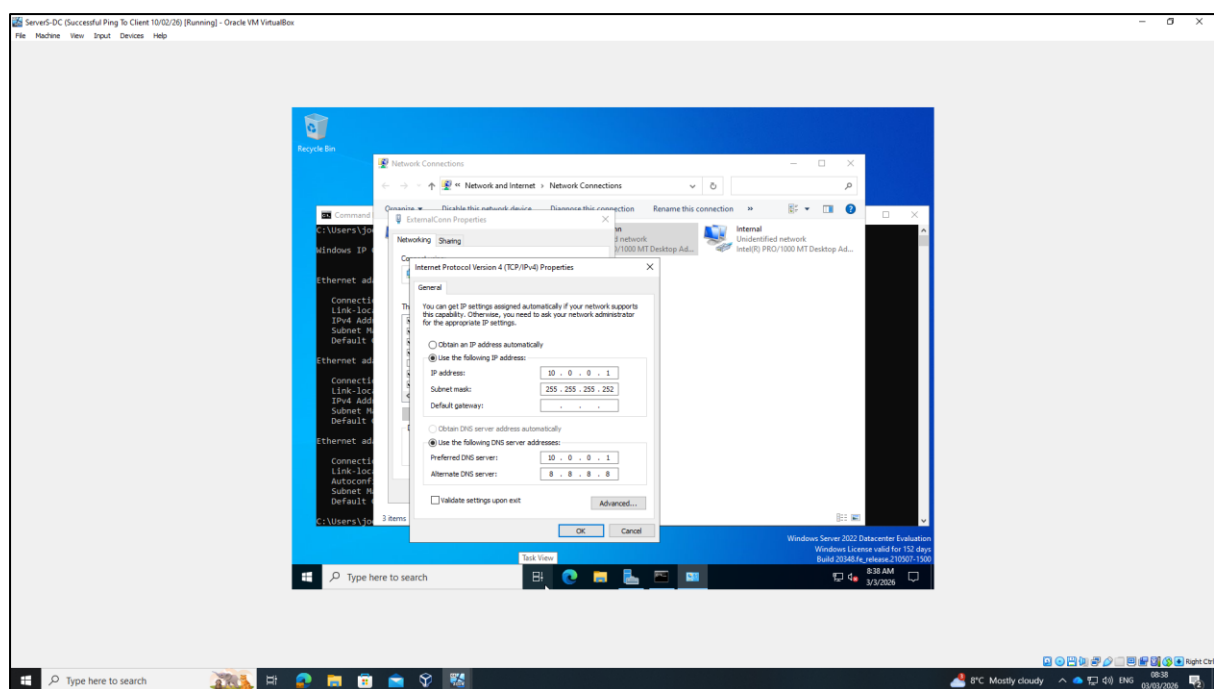


(Figure 2.2.2.9 – the external adapter on the Microsoft server)



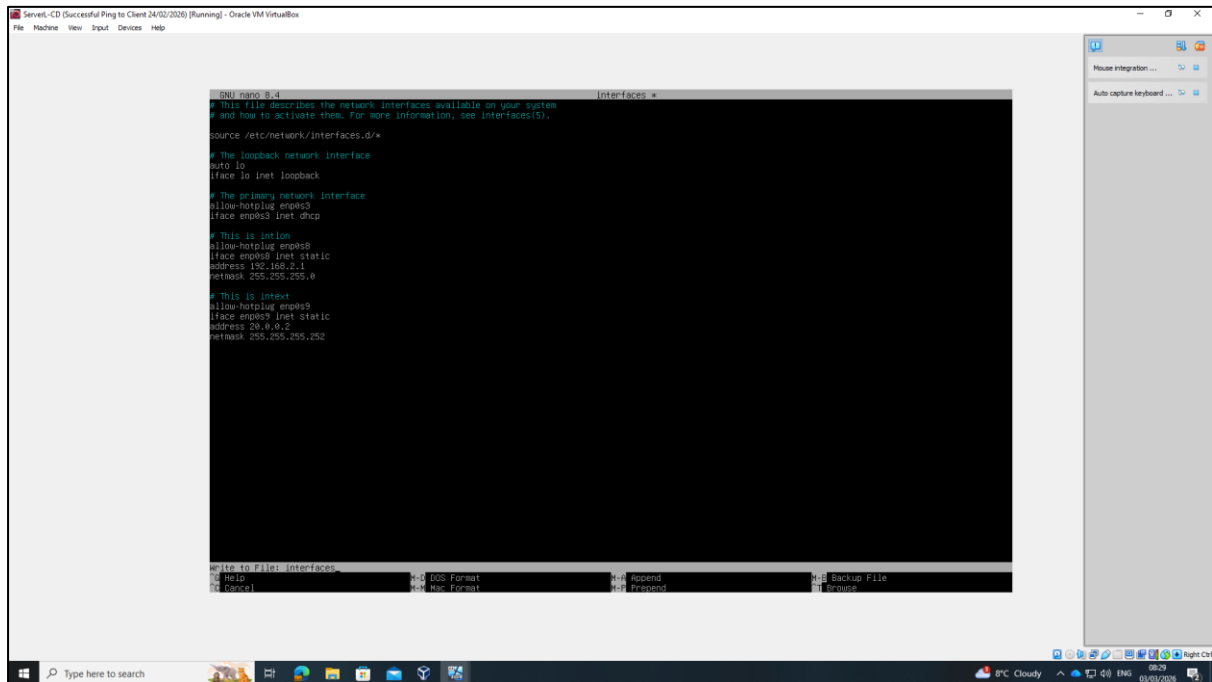
(Figure 2.2.2.10 – the external adapter on the Debian server)

The internal adapter on the Swansea server had to be configured within the ‘Network Connections’ settings:

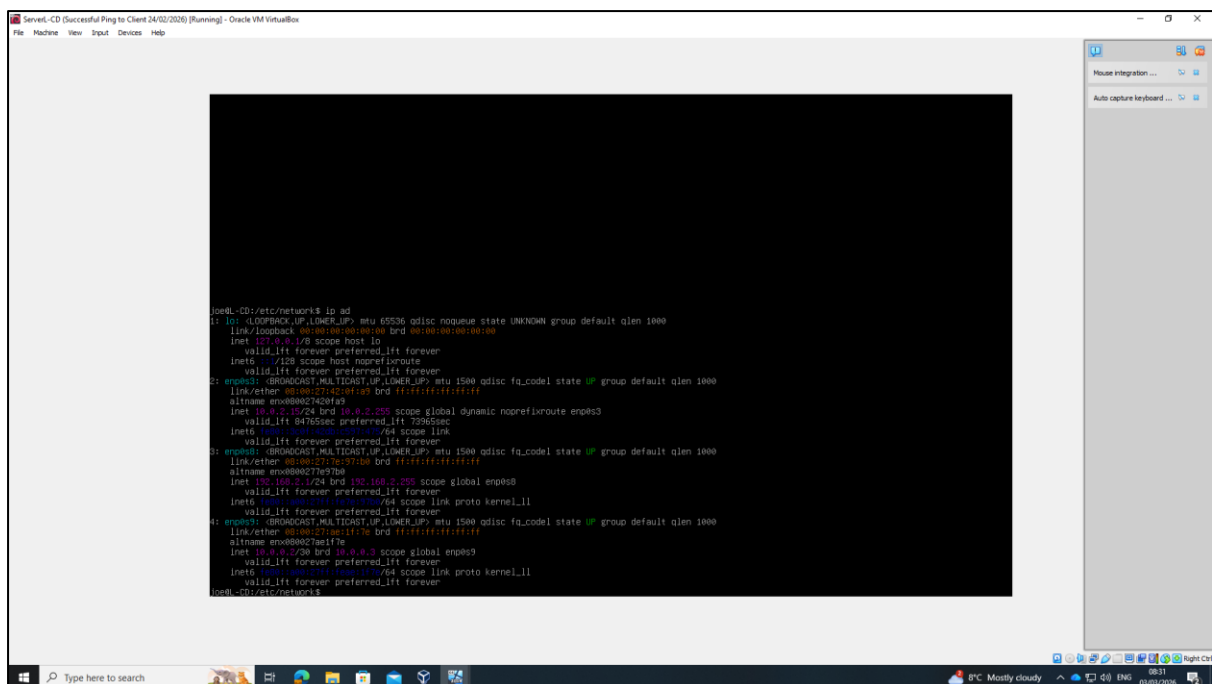


(Figure 2.2.2.11 – the configuration of ‘intext’ on the Microsoft server)

The internal adapter on the London server had to be configured by adding its data to the ‘interfaces’ text file, which then added it to the configurations:



(Figure 2.2.2.12 – Inserting ‘intext’ into the ‘interfaces’ file)



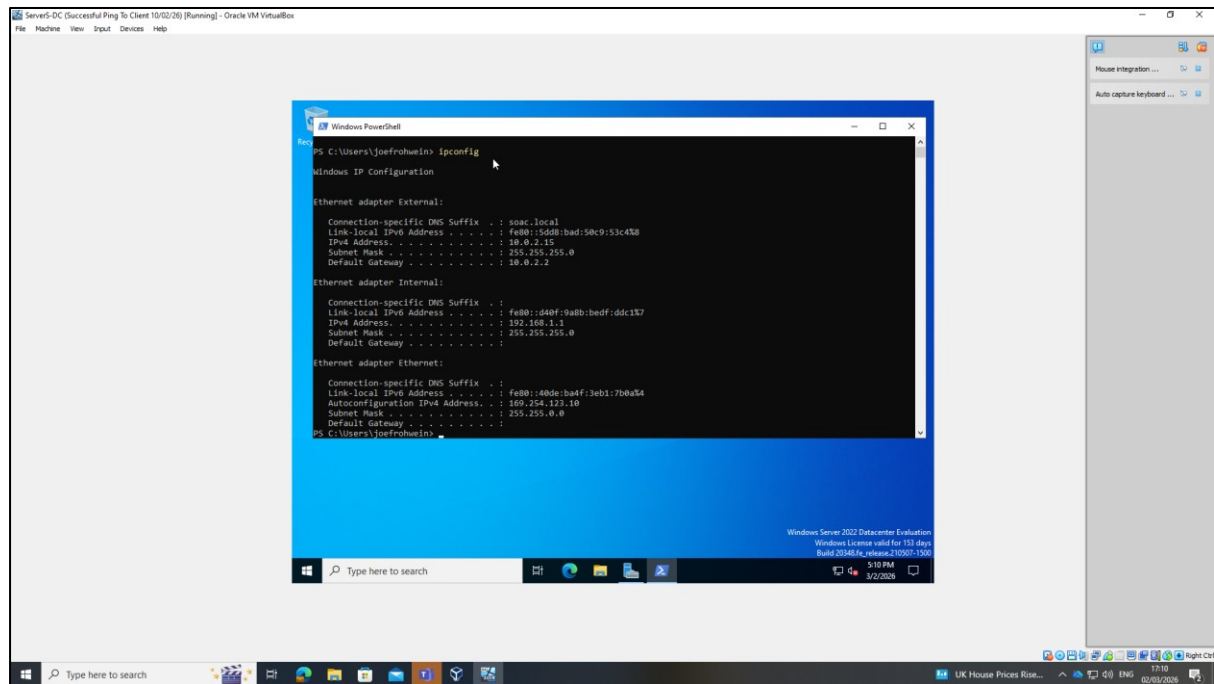
(Figure 2.2.2.13 – Displaying the IP information with the added external adapter)

2.3. Configure IP Addressing

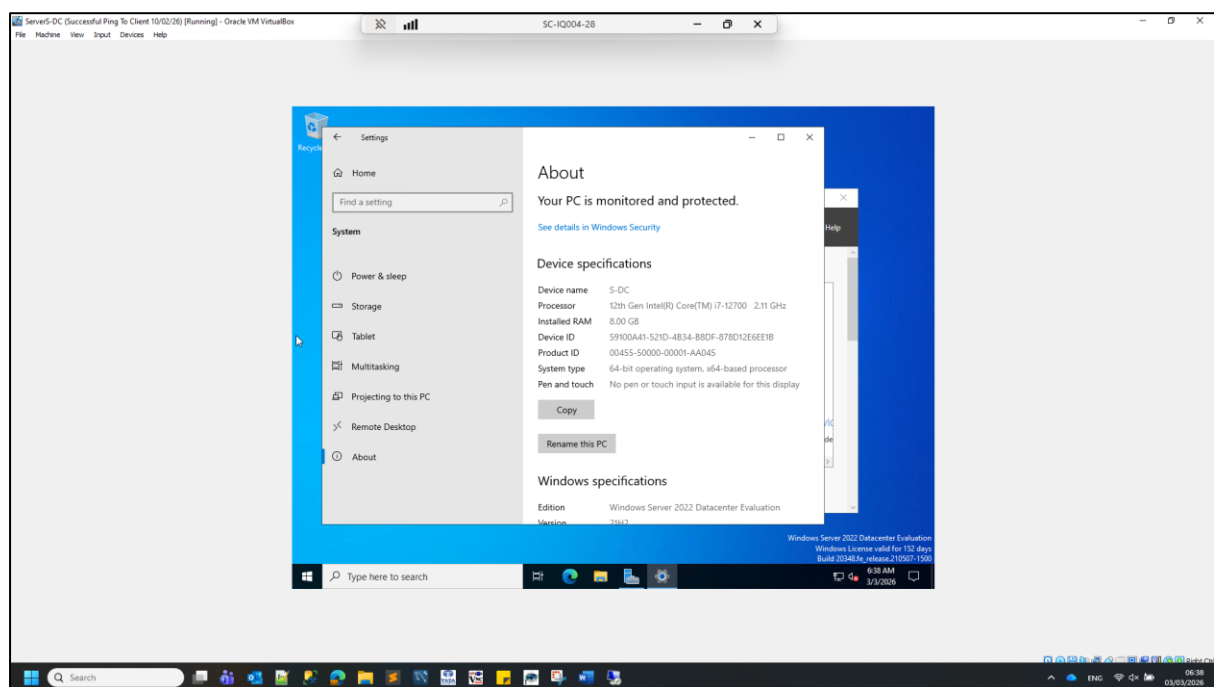
2.3.1. Appropriate IP Addressing

The IP addressing and naming conventions of the network were applied as per the specified network topology, with all IP addresses and machine names matching accordingly.

The Swansea server was assigned 192.168.1.1 and named 'S-DC':

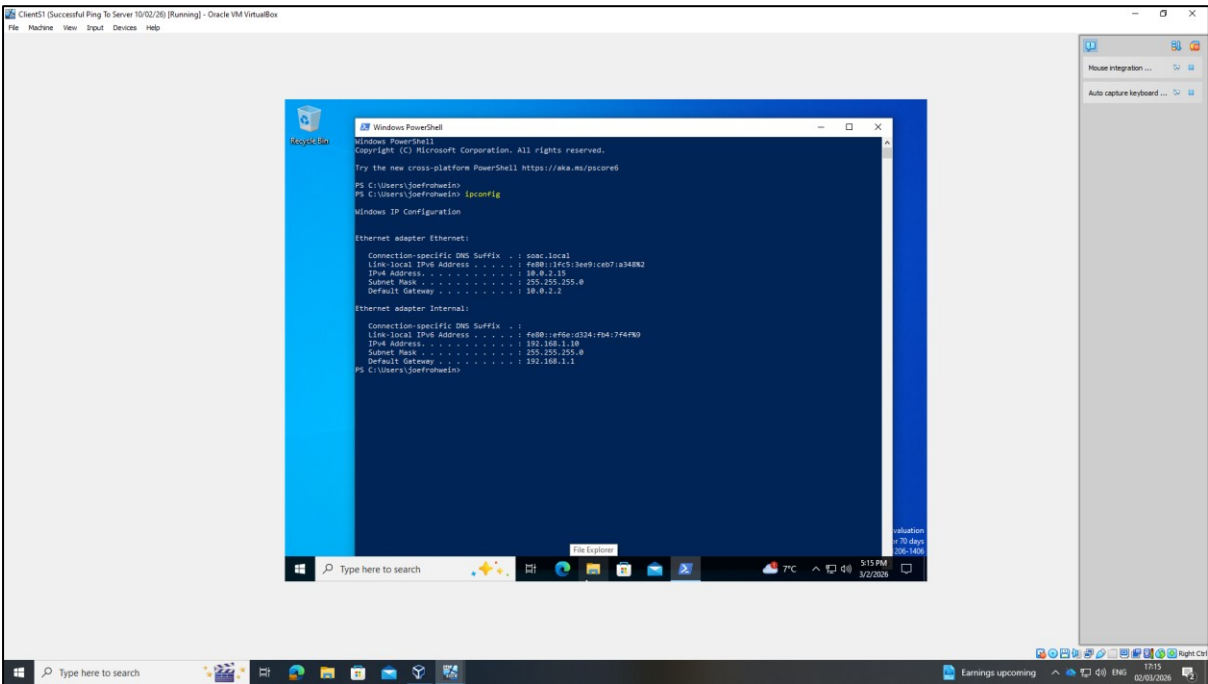


(Figure 2.3.1.1 – The IP address of the Microsoft server)

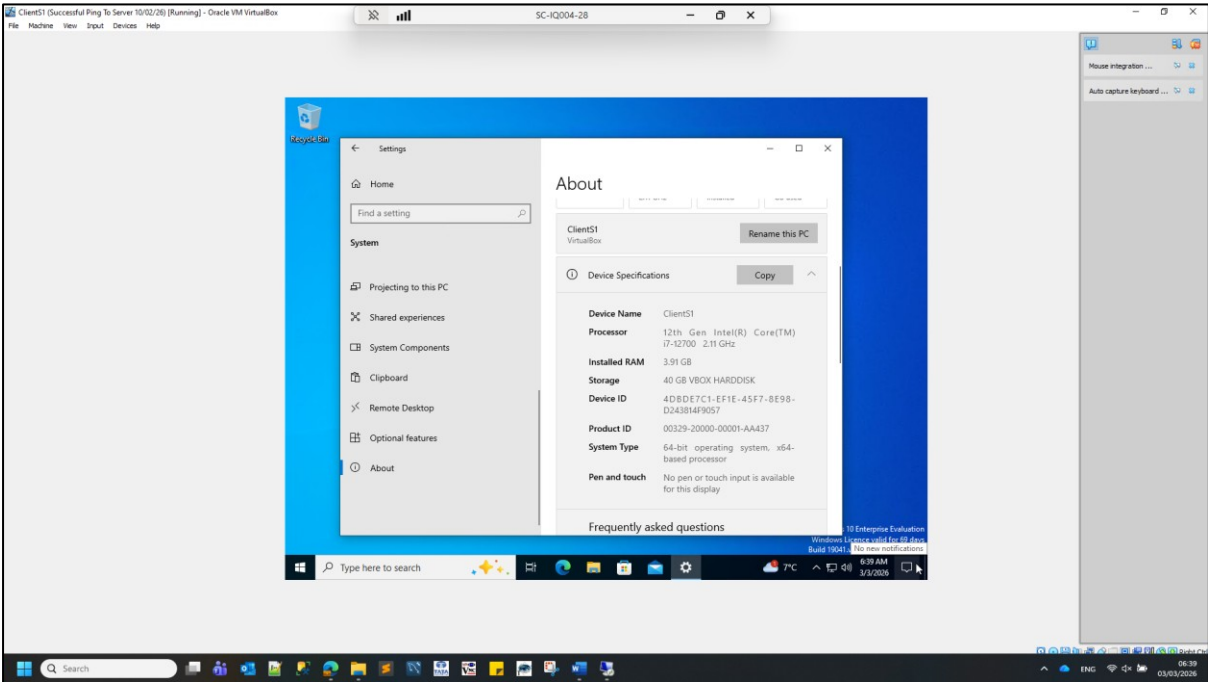


(Figure 2.3.1.2 – The device name of the Microsoft server)

The Swansea client was assigned 192.168.1.10 and named 'ClientS1':

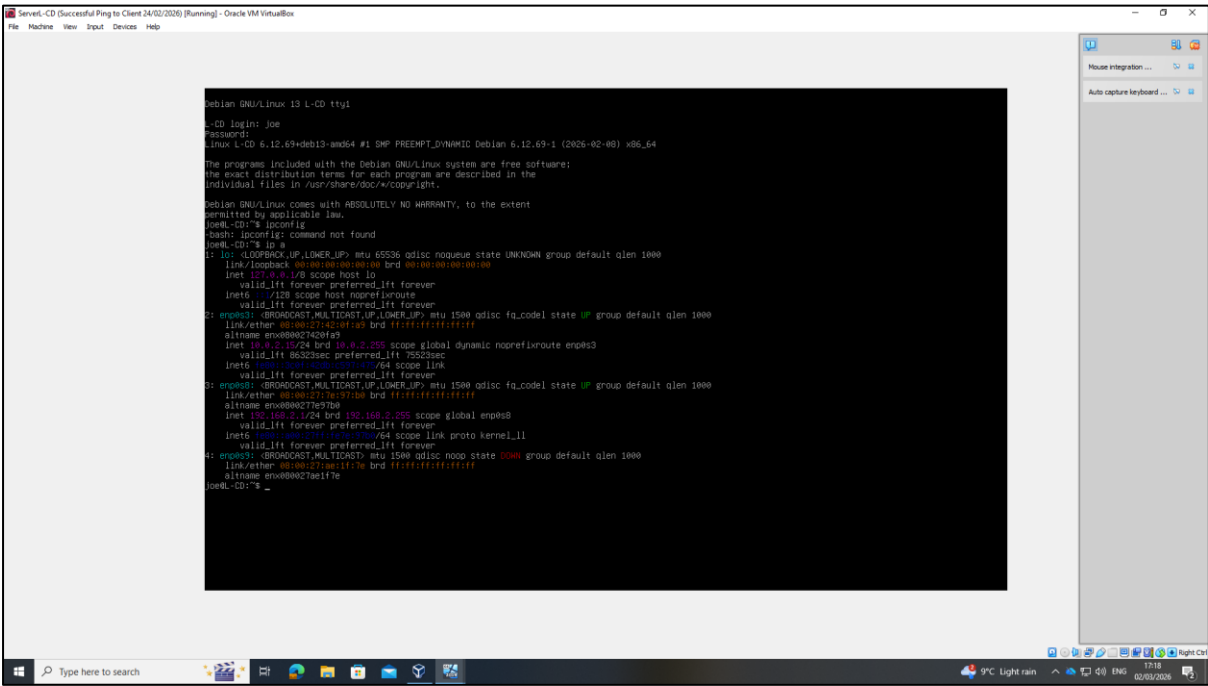


(Figure 2.3.1.3 – The IP address of the Microsoft client)

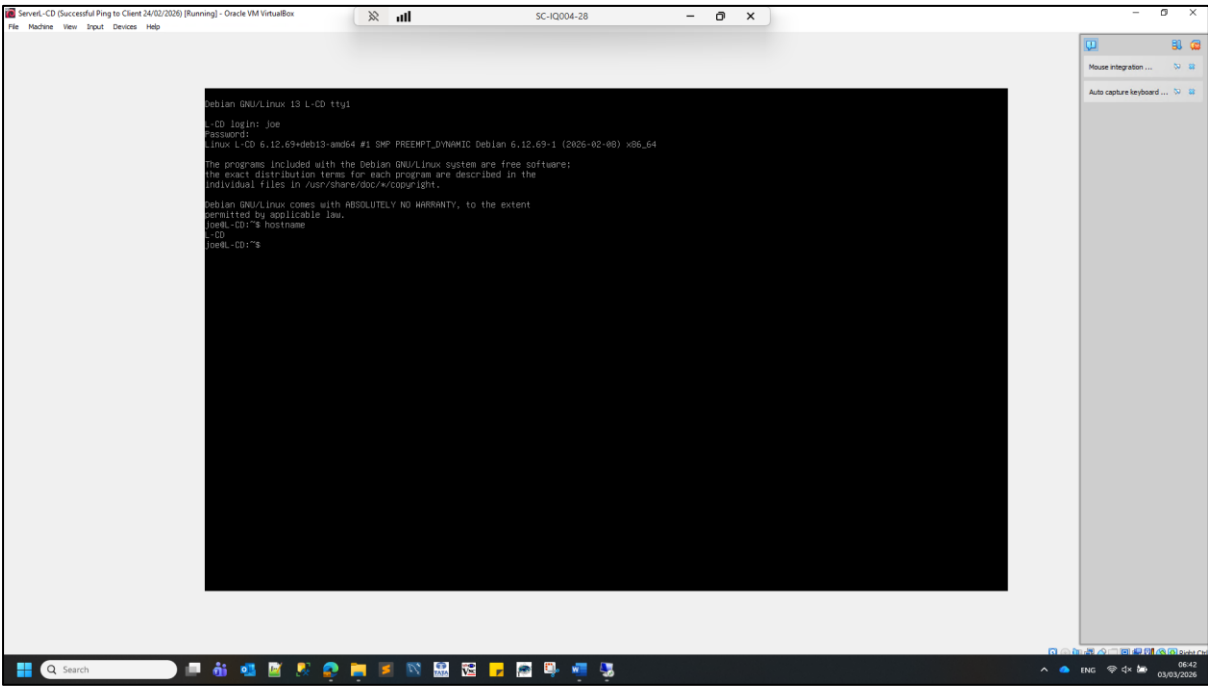


(Figure 2.3.1.4 – The device name of the Microsoft server)

The London server was assigned 192.168.2.1 and named ‘L-CD’:

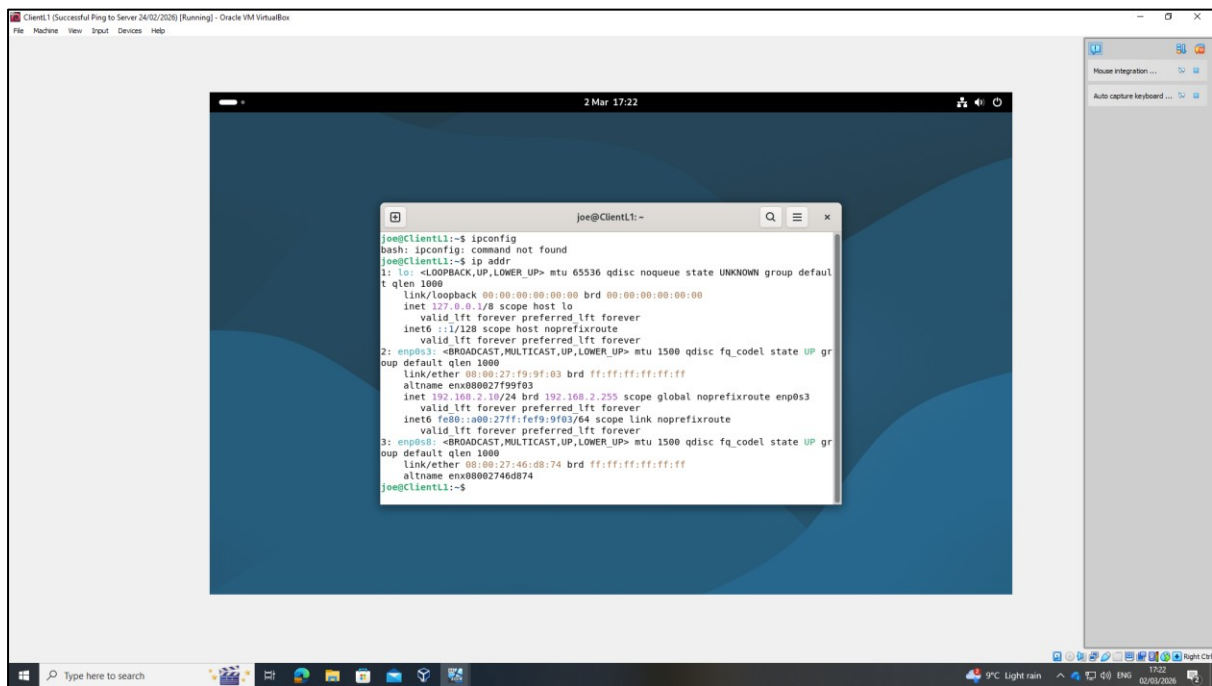


(Figure 2.3.1.5 – The IP address of the Debian server)

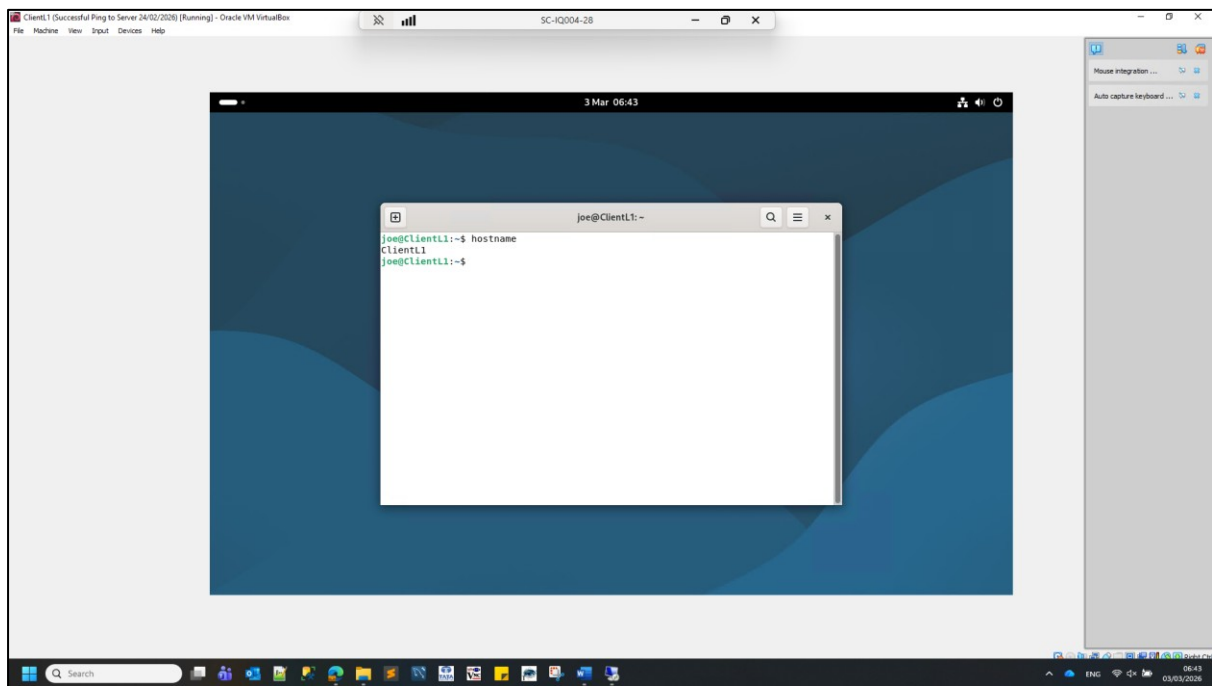


(Figure 2.3.1.6 – The device name of the Debian server)

The London client was assigned 192.168.2.10 and named 'ClientL1':



(Figure 2.3.1.7 – The IP address of the Debian client)

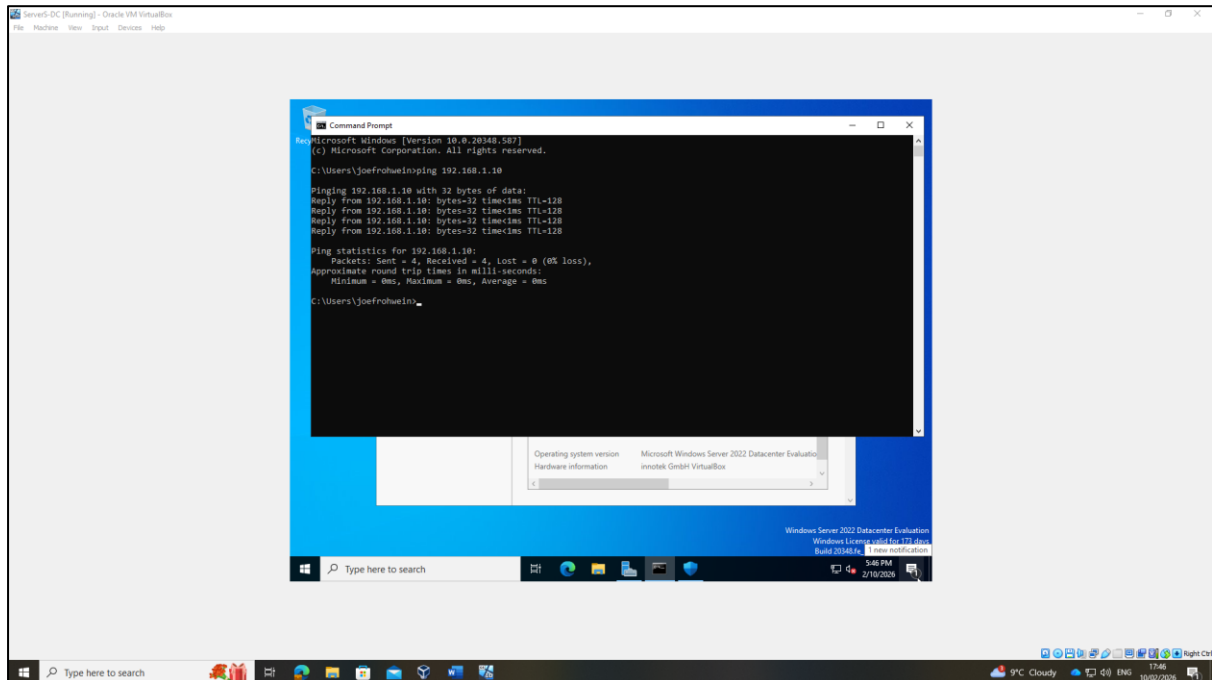


(Figure 2.3.1.8 – The device name of the Debian client)

2.4. Test and Troubleshoot

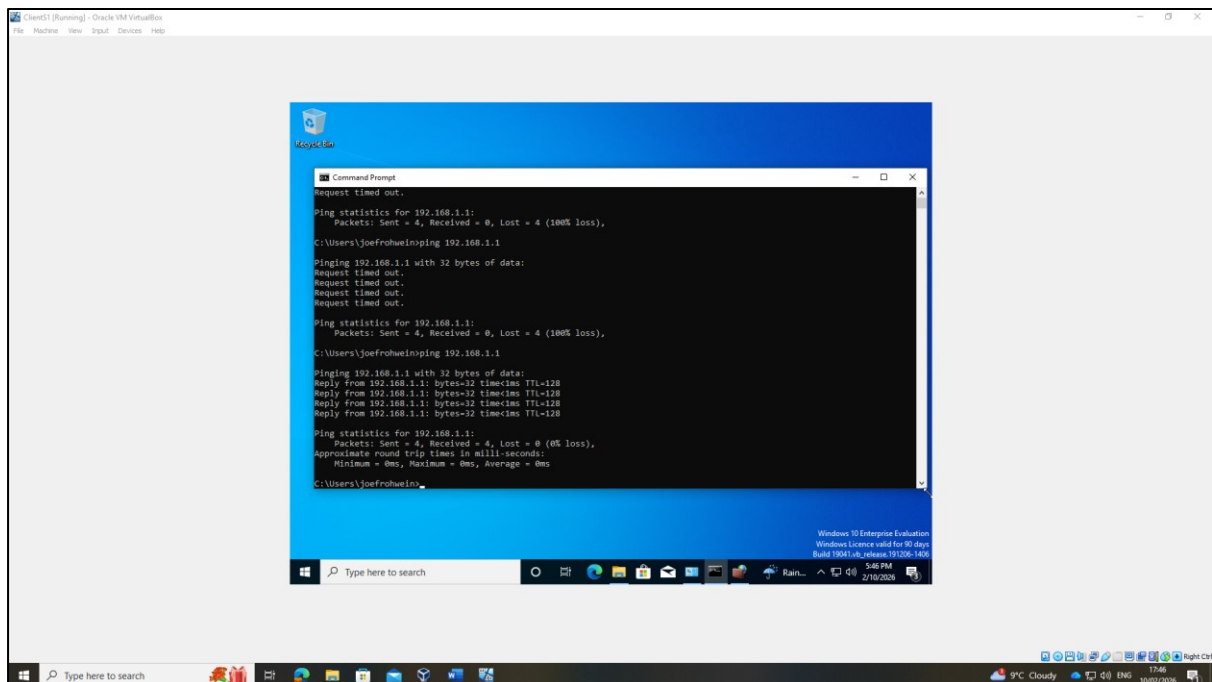
2.4.1. Perform Connectivity tests

The ping from Microsoft server to client was successful:



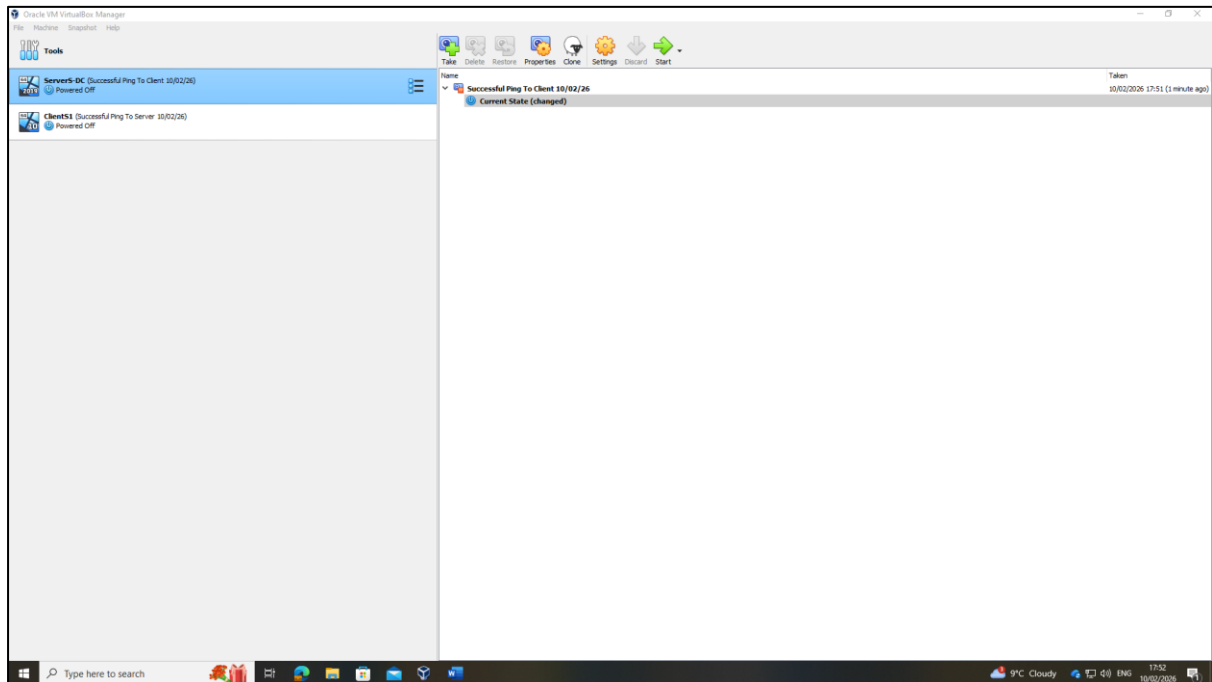
(Figure 2.4.1.1 – A successful ping from Microsoft server to client)

The ping from Microsoft client to server was also successful:



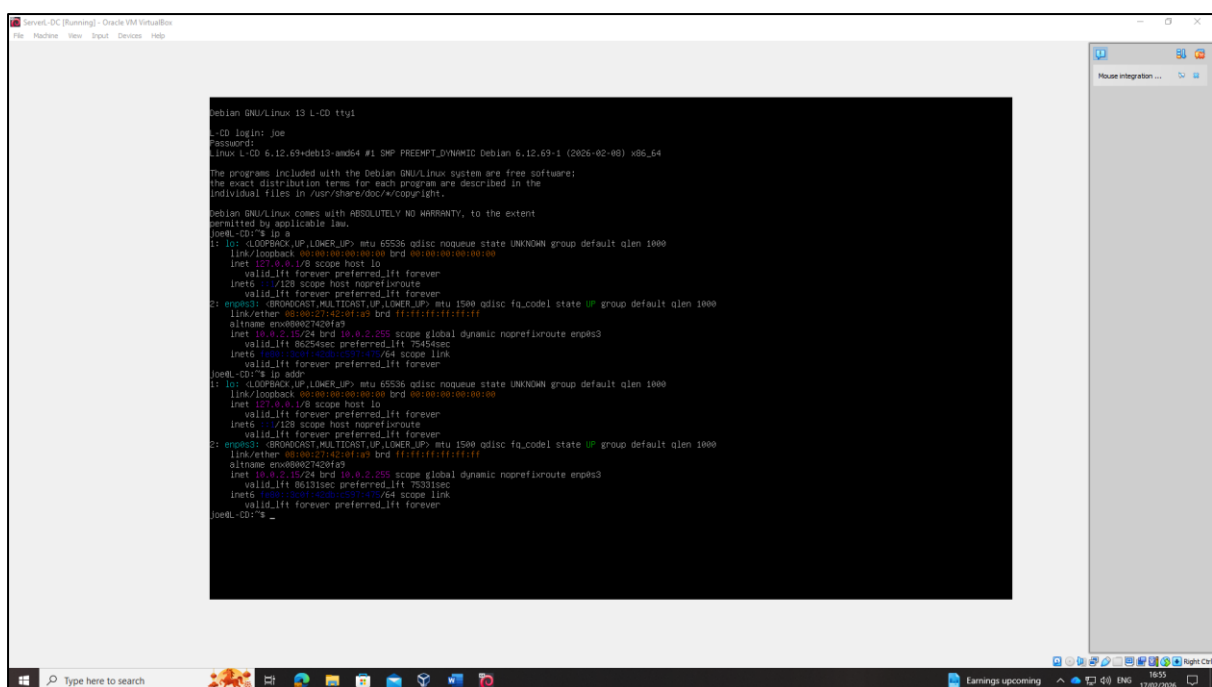
(Figure 2.4.1.2 – A successful ping from Microsoft client to server)

Snapshots were taken of the correctly configured Swansea network after both successful pings to save a copy of each machine:

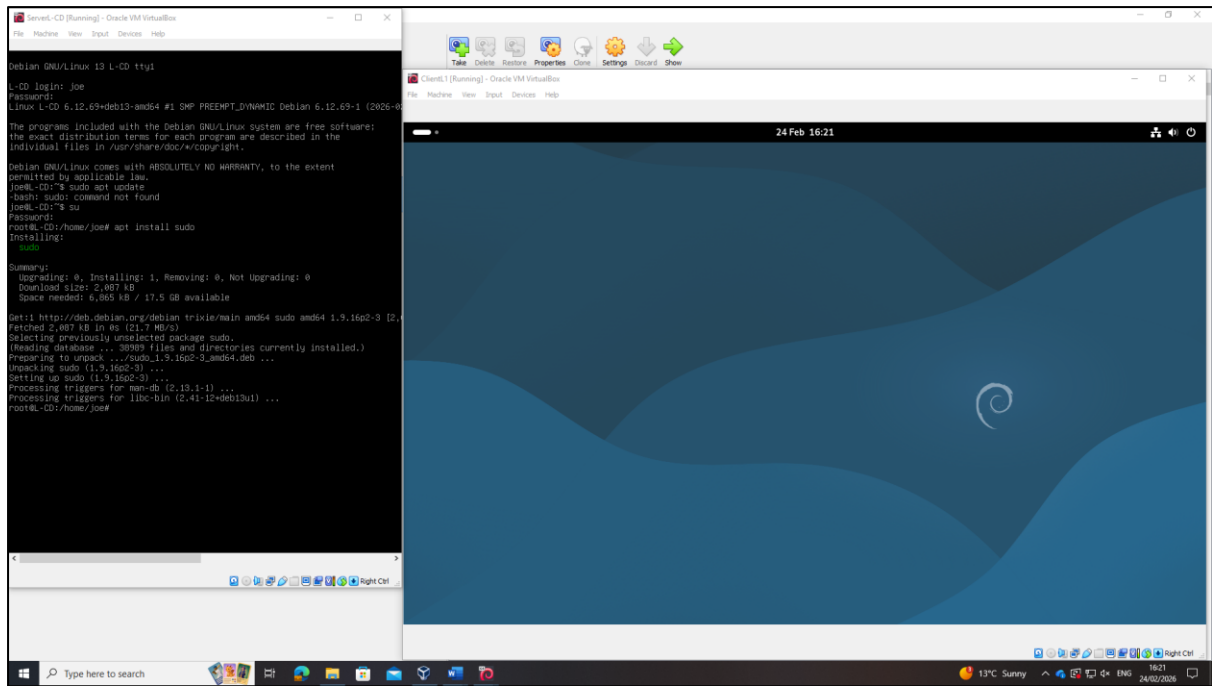


(Figure 2.4.1.3 – Snapshots taken of the successfully configured Microsoft network)

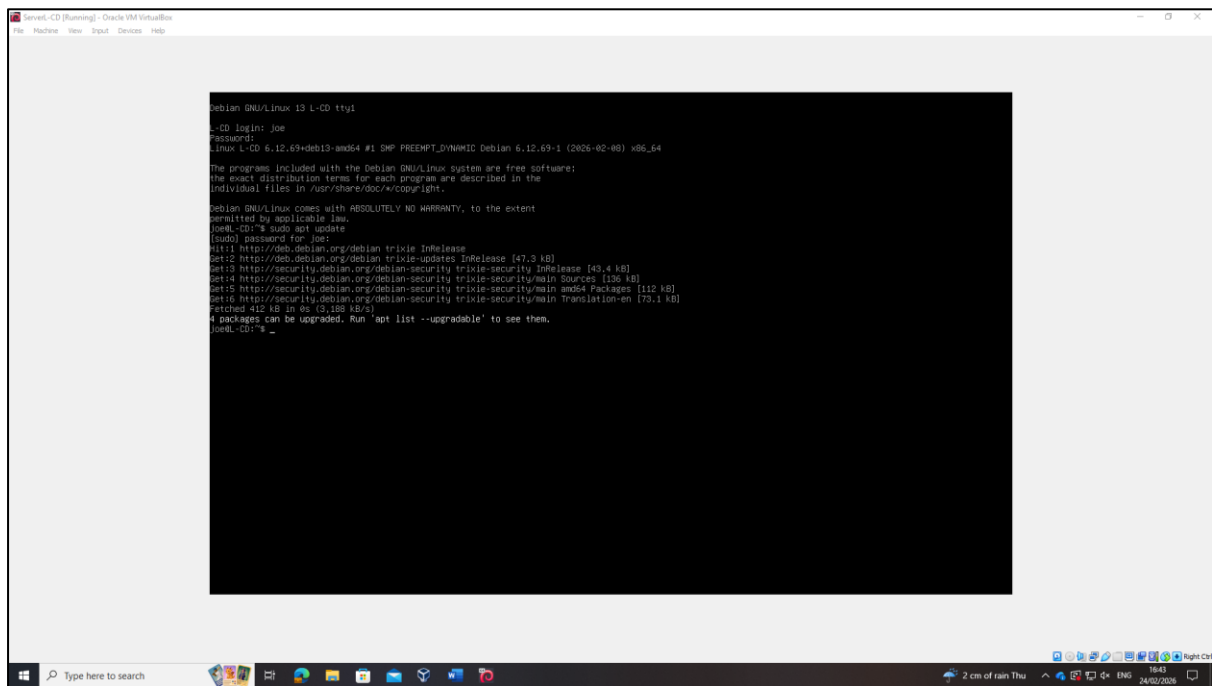
To perform a connectivity test on the London network, sudo had to be installed and updated. This was done by displaying the IP configuration, logging into the administrator (root), installing sudo, assigning the required use to the sudoers list, and updating the server:



(Figure 2.4.1.4 – Displaying the IP configuration of the Debian server)

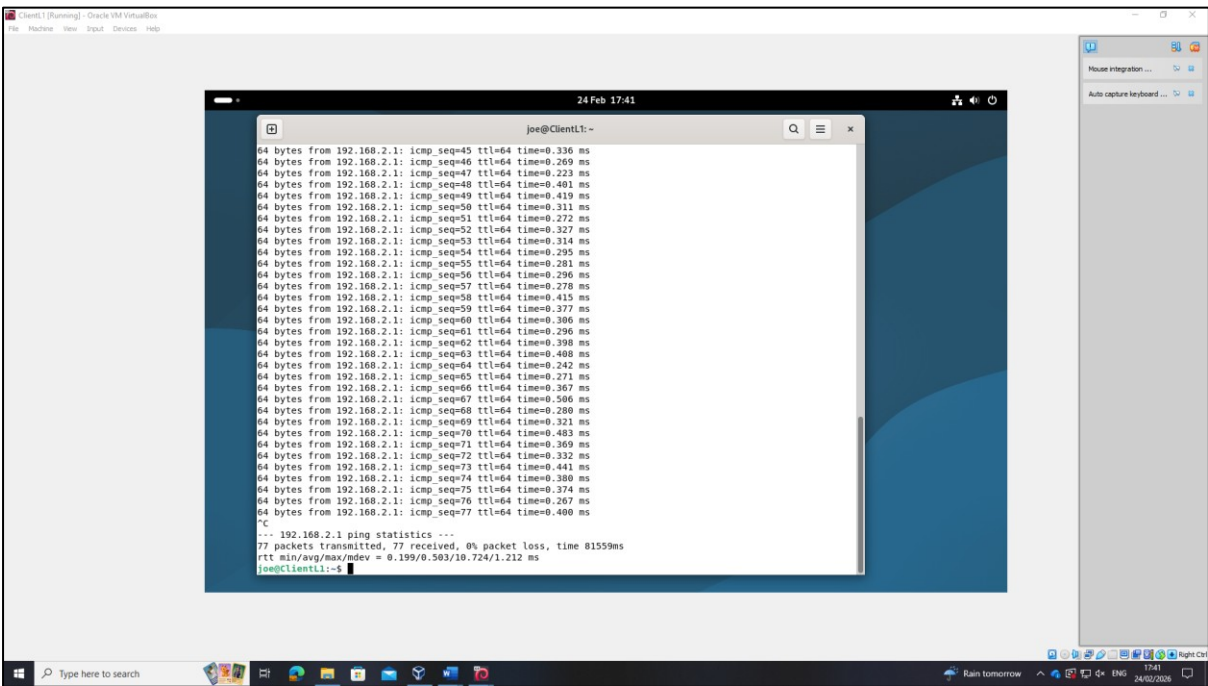


(Figure 2.4.1.5 – Installing ‘sudo’)



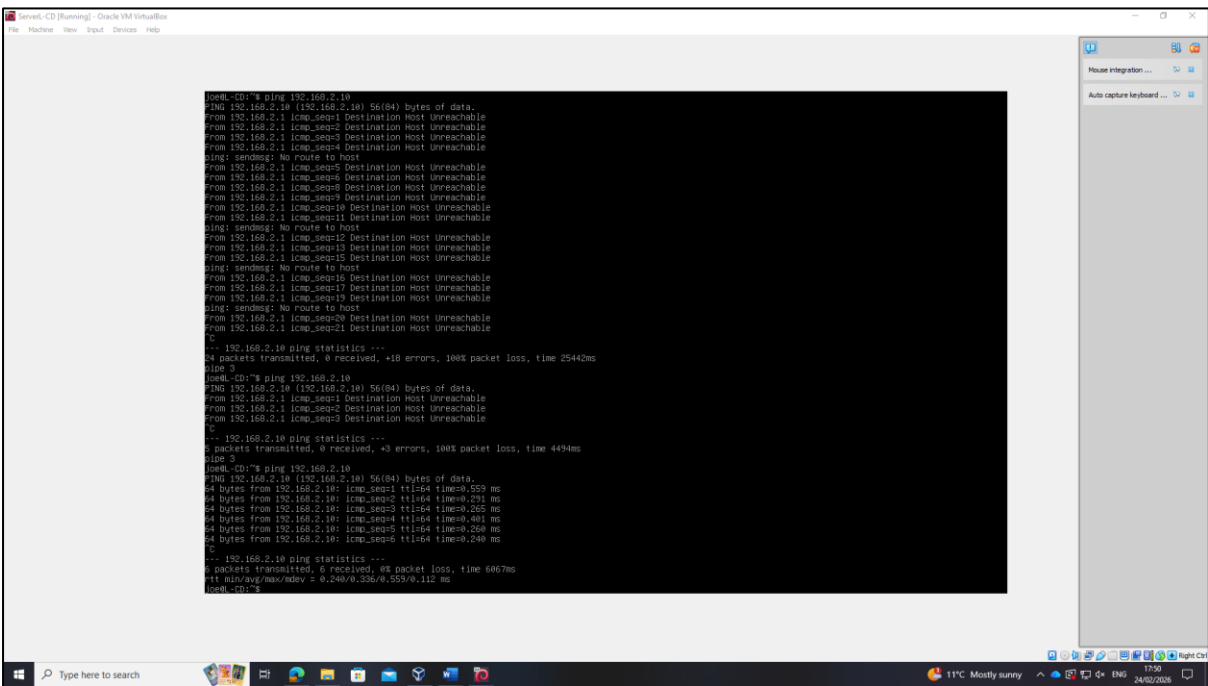
(Figure 2.4.1.5 – Running ‘apt update’)

The ping from Debian client to server was successful:



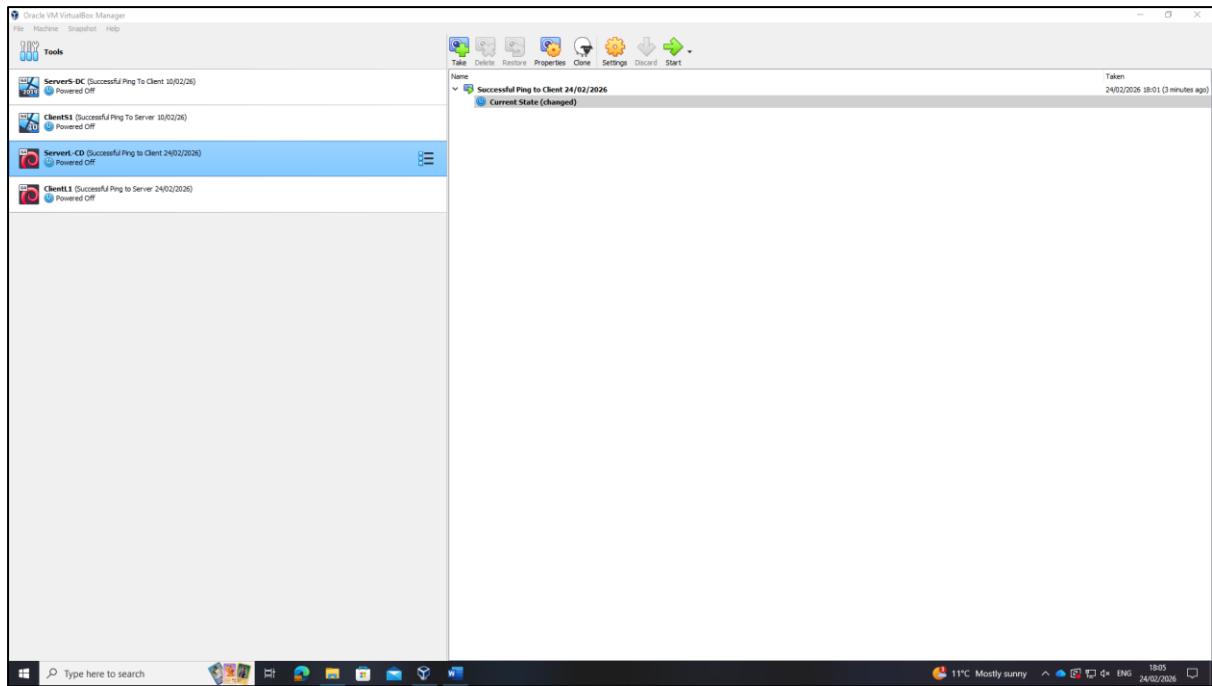
(Figure 2.4.1.6 – A successful ping from Debian client)

The ping from Debian server to client was also successful:



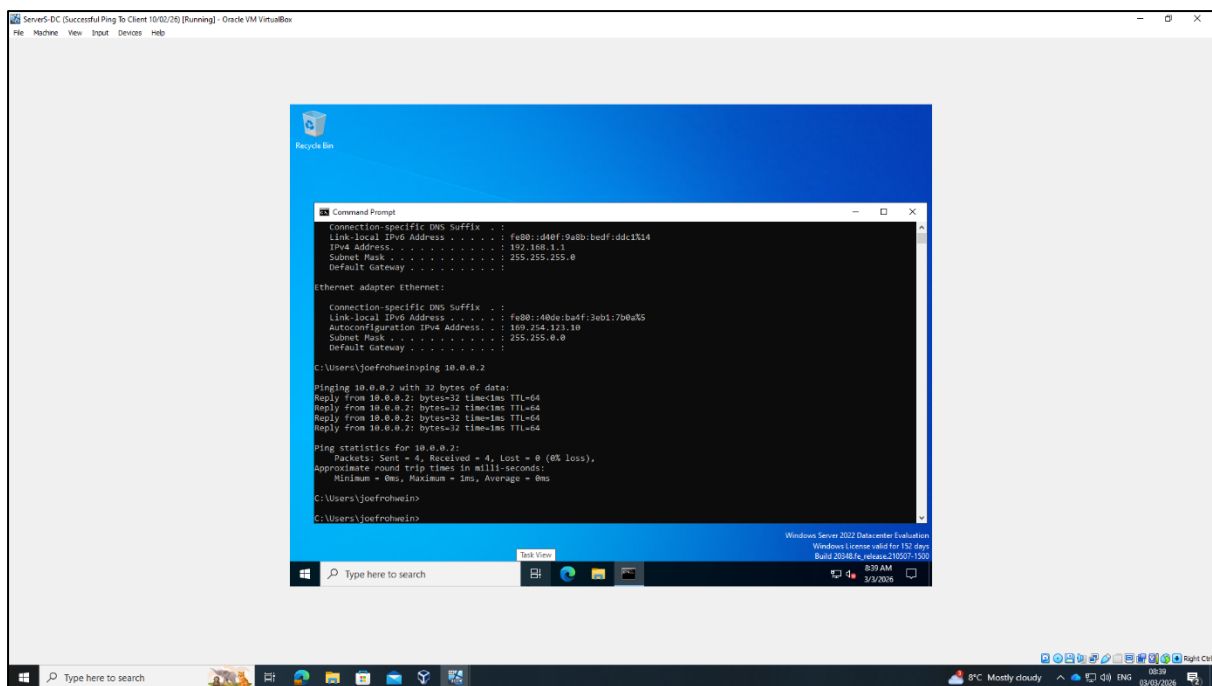
(Figure 2.4.1.7 – A successful ping from Debian server to client)

Snapshots were taken of the correctly configured London network after both successful pings to save a copy of each machine:



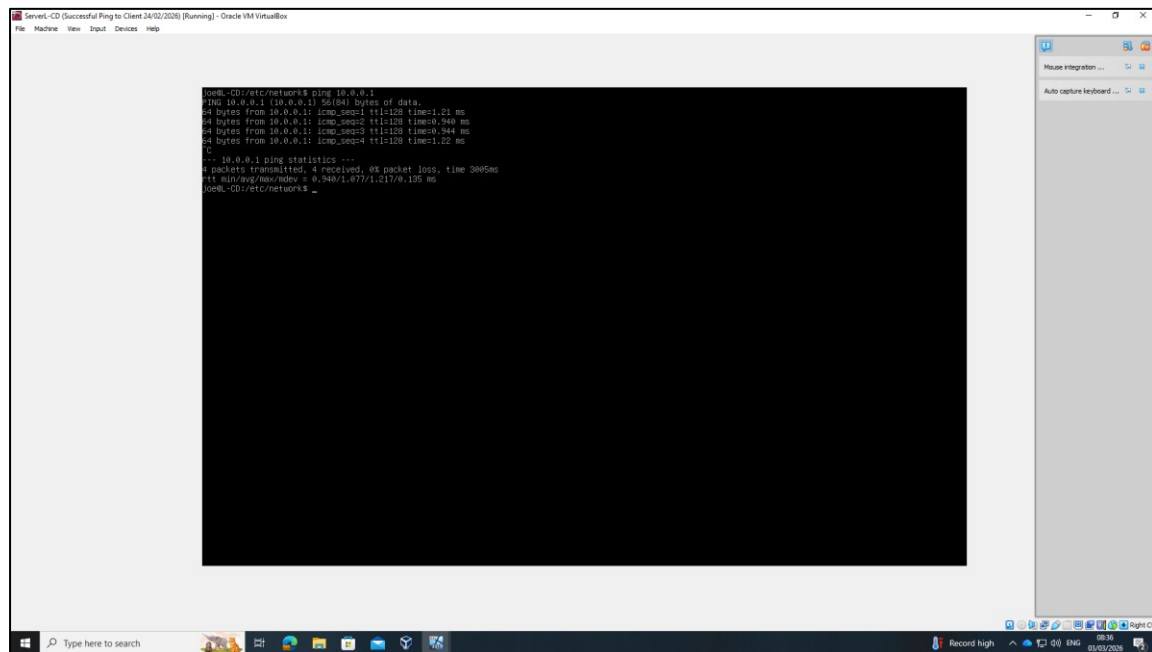
(Figure 2.4.1.8 – Snapshots taken of the successfully configured Microsoft network)

The ping from Swansea server to London server was successful, which also demonstrates the IP addressing of the external adapter:



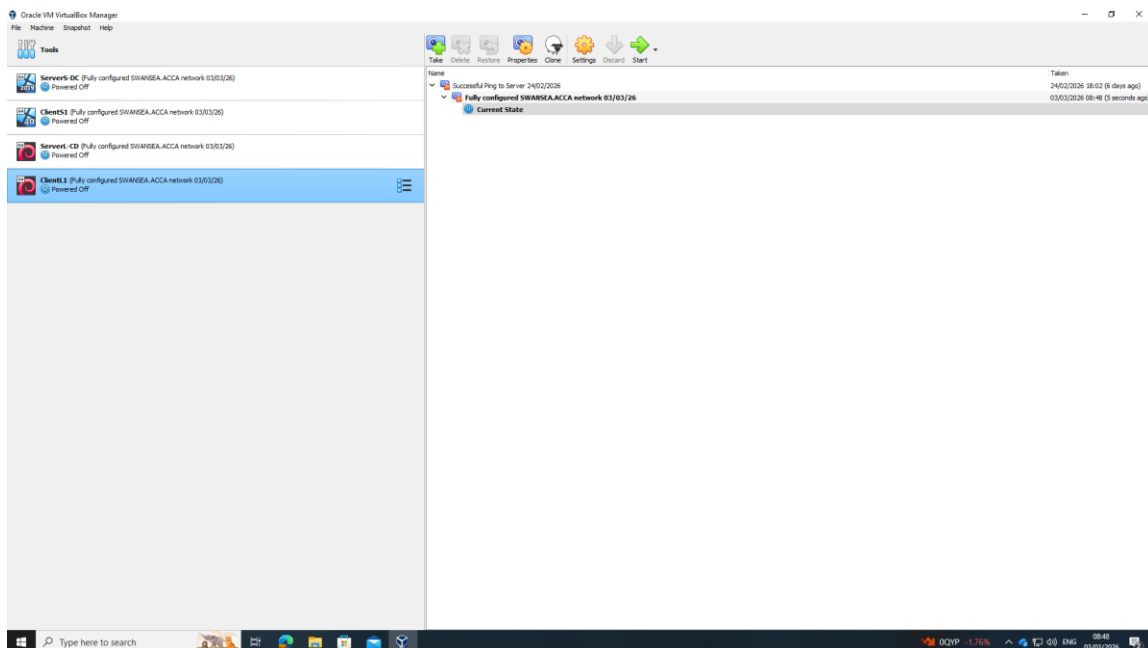
(Figure 2.4.1.9 – A successful ping from Microsoft server to Debian server)

The ping from London server to Swansea server was also successful, which also demonstrates the IP addressing of the external adapter:



(Figure 2.4.1.10 – A successful ping from Debian server to Microsoft server)

As the network was correctly configured and fully functional, having successful connection between each server and its client, alongside successful connection between the two servers, snapshots were taken of the entire network to save a total backup:



(Figure 2.4.1.11 – Snapshots taken of the successfully configured SWANSEA.ACCA network)

3. Reflection

3.1.1. Write a Technical reflection covering network deployment and testing

Throughout the deployment of this network, some complications were faced. The first came when trying to communicate between the servers and clients on both internal networks, which was initially blocked by the default firewalls on the VMs. This prevented the network connection from being tested. To solve this, the firewalls had to be disabled through the Firewall settings menus on the Windows VMs, or through the command window on the Debian VMs. For this specific deployment, it was acceptable to leave the firewalls disabled, though for future work it is best practice to enable them after testing to ensure network security.

Another issue faced was managing administrative changes on the Debian server. Configuration changes, such as installing 'sudo' and assigning users to the 'sudoers' list, required switching between the regular user account and the 'root' administrator account. High-level modifications should be done using the 'root' account, while routine tasks should use non-administrative accounts to minimise the risk.

3.1.2. Write your Personal Reflection

Completing this network deployment helped me to develop my technical skills and knowledge in network operating systems and services. Working with both Windows and Debian VMs, configuring IP addresses, managing administrative changes and testing connectivity provided practical experience, reinforcing my understanding of networking architecture. Challenges such as firewalls and administrative complications allowed me to improve my troubleshooting ability and demonstrated the need to plan carefully. This task has made me aware of the best practices to apply and what to anticipate in the subsequent coursework, which is an extension of this network, allowing for a smooth, efficient deployment of the enhanced topology.

4. References

- [1] “What is a hypervisor?,” vmware, [Online]. Available: <https://www.vmware.com/topics/hypervisor>. [Accessed 27 01 2026].
- [2] A. U. Rehman, R. Aguiar and J. Barraca, Network Functions Virtualization: The Long Road to Commercial Deployments, 2019.
- [3] “What’s the Difference Between Type 1 and Type 2 Hypervisors?,” Amazon Web Services, [Online]. Available: <https://aws.amazon.com/compare/the-difference-between-type-1-and-type-2-hypervisors/>. [Accessed 03 02 2026].
- [4] M. Kumar, “Choose Best Hypervisor Type-1 & Type-2: Complete Guide,” HyperHCI, 10 10 2025. [Online]. Available: <https://hyperhci.com/best-hypervisors-type-1-and-type-2/>. [Accessed 27 01 2026].
- [5] M. Ellis, “Understanding Hypervisors: Type-1 vs Type-2 Explained Simply,” Host Advice, 28 01 2026. [Online]. Available: <https://hostadvice.com/blog/web-hosting/vps/type-1-vs-type-2-hypervisor/>. [Accessed 03 02 2026].
- [6] H. T. C. Ltd, Data Communications and Network Technologies, Springer, 2023.
- [7] “What is a Switch vs a Router?,” Cisco, [Online]. Available: <https://www.cisco.com/site/us/en/learn/topics/small-business/network-switch-vs-router.html>. [Accessed 27 02 2026].
- [8] “What Is An IP Address? How Does It Work?,” Fortinet, [Online]. Available: <https://www.fortinet.com/uk/resources/cyberglossary/what-is-ip-address>. [Accessed 27 02 2026].
- [9] “IP Addressing,” Mosse Cyber Security Institute, [Online]. Available: https://library.mosse-institute.com/articles/2023/08/ip-addressing.html?utm_source=chatgpt.com. [Accessed 27 02 2026].

- [10] "What is Internet Protocol Version 4 (Pv4)," Geeks For Geeks, 04 10 2025. [Online]. Available: <https://www.geeksforgeeks.org/computer-networks/what-is-ipv4/>. [Accessed 27 02 2026].
- [11] S. Lee, "Mastering IPv4 Networking Essentials," Number Analytics, 10 06 2025. [Online]. Available: https://www.numberanalytics.com/blog/ultimate-guide-to-ipv4-in-networking?utm_source=chatgpt.com. [Accessed 27 02 2026].
- [12] "What is IPv6?," Geeks For Geeks, 31 07 2025. [Online]. Available: <https://www.geeksforgeeks.org/computer-networks/what-is-ipv6/>. [Accessed 27 02 2026].
- [13] "Introduction To Subnetting," Geeks For Geeks, 10 02 2026. [Online]. Available: <https://www.geeksforgeeks.org/computer-networks/introduction-to-subnetting/>. [Accessed 27 02 2026].
- [14] "Routing," Geeks For Geeks, 21 01 2026. [Online]. Available: <https://www.geeksforgeeks.org/computer-networks/what-is-routing/>. [Accessed 24 02 2026].
- [15] L. Agapidis, "Purpose of Routing Protocols," Cisco, [Online]. Available: <https://www.networkstraining.com/the-purpose-of-a-routing-protocol/>. [Accessed 24 02 2026].
- [16] D. Jacobs, "Static vs. dynamic routing: What is the difference?," TechTarget, [Online]. Available: https://www.techtarget.com/searchnetworking/answer/Static-and-dynamic-routing?utm_source=chatgpt.com. [Accessed 24 02 2026].
- [17] M. Bialy, "Where to use static and where to use dynamic routing?," Grandmetric, 25 08 2017. [Online]. Available: <https://www.grandmetric.com/where-to-use-static-and-where-to-use-dynamic-routing/>. [Accessed 26 02 2026].
- [18] "What DHCP is and Types of DHCP Explained," ComputerNetworkingNotes, 11 02 2026. [Online]. Available: <https://www.computernetworkingnotes.com/ccna-study-guide/what-dhcp-is-and-types-of-dhcp-explained.html>. [Accessed 24 02 2026].
- [19] "Dynamic Host Configuration Protocol (DHCP)," Geeks For Geeks, 10 02 2026. [Online]. Available: <https://www.geeksforgeeks.org/computer-networks/dynamic-host-configuration-protocol-dhcp/>. [Accessed 24 02 2026].

- [20] D. Coclin, "What's a CA?: Certificate Authorities for Beginners," Digicert, [Online]. Available: <https://www.digicert.com/blog/what-is-a-certificate-authority>. [Accessed 28 02 2026].
- [21] V. Raj, "Best Practices for Certificate Authority Management," Secure W2, 15 09 2025. [Online]. Available: <https://www.securew2.com/blog/best-practices-certificate-authority-management>. [Accessed 28 02 2026].
- [22] "Best Practices for effective implementation of private Certificate Authorities (CAs)," Sectigo, [Online]. Available: <https://www.sectigo.com/blog/private-ca-implementation-best-practices>. [Accessed 28 02 2026].
- [23] S. Chauhan, "Type 1 vs Type 2 hypervisors – (Key Differences)," Tou Stable, 28 01 2026. [Online]. Available: https://www.youstable.com/blog/type-1-vs-type-2-hypervisors?utm_source=chatgpt.com. [Accessed 27 02 2026].
- [24] "What's the difference between type 1 and type 2 hypervisors?," IONOS, 11 07 2024. [Online]. Available: <https://www.ionos.co.uk/digitalguide/server/know-how/hypervisor-type-1-and-type-2/>. [Accessed 27 02 2026].
- [25] "Virtual Private Networks (VPNs)," National Cyber Security Centre, [Online]. Available: <https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks>. [Accessed 28 02 2026].
- [26] "What is a VPN?," Microsoft Azure, [Online]. Available: <https://azure.microsoft.com/en-gb/resources/cloud-computing-dictionary/what-is-vpn>. [Accessed 02 28 2026].
- [27] "What is DHCP?," Akamai, [Online]. Available: <https://www.akamai.com/glossary/what-is-dhcp>. [Accessed 28 02 2026].
- [28] "What is Dynamic Host Configuration Protocol (DHCP) Server in Windows Server?," Microsoft, [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top>. [Accessed 02 28 2026].
- [29] "Sysadmin's Guide to Network Services," MSP360, [Online]. Available: <https://www.msp360.com/resources/blog/sysadmins-guide-to-network-services/>. [Accessed 28 02 2026].

- [30] “Active Directory Domain Services overview,” Microsoft, [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>. [Accessed 28 02 2026].
- [31] “Best practices for securing Active Directory,” Microsoft, [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>. [Accessed 28 02 2026].
- [32] “What is Active Directory?,” Proofpoint, [Online]. Available: <https://www.proofpoint.com/uk/threat-reference/active-directory#:~:text=User%20authentication.,maintaining%20high%20levels%20of%20security..> [Accessed 28 02 2026].