

TASK 1

1. Hypervisor

Virtualisation enables multiple operating systems to run concurrently on a single physical host through hardware abstraction and resource sharing mechanisms [1]. Hypervisors are categorised into Type 1 (bare-metal) and Type 2 (hosted) architectures, each differing in performance, scalability, and security exposure [2].

Type 1 hypervisors operate directly on physical hardware, eliminating dependency on a host operating system and thereby reducing latency and improving isolation [3]. This architectural design minimises the attack surface and is commonly deployed within enterprise data centres. In contrast, Type 2 hypervisors operate above a host operating system, introducing an additional abstraction layer but offering ease of installation, hardware compatibility, and simplified configuration [4].

From a security standpoint, hosted hypervisors inherit certain vulnerabilities from the underlying host operating system, potentially increasing exposure to privilege escalation or malware threats [5]. However, within a controlled academic laboratory environment such as the NOSS2026 topology, these risks are significantly reduced due to limited external connectivity and moderate scalability demands.

The SWANSEA.ACCA domain environment required simultaneous deployment of Windows Server and Debian Server systems. A Type 2 hypervisor provided sufficient compatibility and flexibility to support both operating systems while remaining aligned with hardware constraints and time limitations [6]. Although a production multinational corporation would likely favour a Type 1 solution for enhanced resilience and scalability, the selected architecture remains technically justified within this coursework context.

Nevertheless, the architectural limitations of Type 2 hypervisors highlight the trade-off between enterprise-grade performance and academic deployment practicality.

2. IP Addressing

IP addressing underpins logical communication across networks by uniquely identifying devices and enabling packet forwarding between interconnected systems [7]. When data is transmitted across the Internet, it is segmented into packets containing source and destination IP addresses, sequencing information, and error detection data. Routers interpret the destination IP address to determine the most efficient forwarding path [8].

IPv4 utilises a 32-bit addressing structure expressed in dotted decimal notation, which supports approximately 4.3 billion unique addresses but has experienced exhaustion due to global Internet expansion [9]. IPv6 addresses this limitation through a 128-bit hexadecimal structure, significantly expanding address capacity and enabling improved hierarchical routing aggregation [10]. The structural differences between IPv4 and IPv6 reflect evolving scalability and efficiency requirements in modern networking environments.

Subnetting divides a larger network into smaller logical segments by manipulating subnet masks to define network and host portions [11]. Variable Length Subnet Masking (VLSM) improves efficient address allocation by tailoring subnet sizes to specific host requirements rather than applying uniform mask lengths [12].

Within the NOSS2026 topology, logical separation between Swansea and London LANs demonstrates how subnetting enhances broadcast control, security segmentation, and structured routing. Efficient IP allocation directly contributes to simplified troubleshooting and stable communication. Poor addressing design may result in overlapping subnets or routing ambiguity, reinforcing the importance of structured planning in enterprise environments [13].

3. Routing

Routing facilitates packet delivery between distinct IP networks by maintaining routing tables that determine next-hop forwarding decisions [14]. Static routing requires manual configuration and offers administrative control and predictable traffic flow but lacks scalability in complex or rapidly changing topologies [15]. Because routes must be configured individually, administrative overhead increases as networks expand.

Dynamic routing protocols such as OSPF and RIP automatically exchange routing information between routers, enabling adaptive path selection and automatic convergence when topology changes occur [16]. These protocols improve fault tolerance and scalability, particularly within distributed enterprise environments. However, dynamic routing introduces additional protocol overhead, computational processing, and configuration complexity, which may be unnecessary in small deployments [17].

In the NOSS2026 topology, only two LANs and a single point-to-point interconnection were required. Under these conditions, static routing provides sufficient functionality without introducing unnecessary protocol overhead [18]. The simplicity of static configuration also improves troubleshooting clarity, as routing paths remain explicitly defined.

Nevertheless, in a real multinational corporate infrastructure with multiple branches and redundant inter-site links, dynamic routing would provide improved resilience, automated failover, and scalable network growth. This comparison demonstrates that routing strategy is context-dependent and must align with organisational scale, administrative capability, and long-term infrastructure objectives rather than adopting a universal solution.

4. Network Services

Enterprise network infrastructures rely on integrated services including Active Directory Domain Services (AD DS), DHCP, VPN technologies, and Certificate Authorities to ensure structured management, authentication, and secure communication [19]. Rather than operating independently, these services form an interconnected framework that supports enterprise governance and trust models.

Active Directory Domain Services centralises authentication and identity management, enabling policy enforcement, user access control, and structured resource management within domain environments such as SWANSEA.ACCA [20]. This centralisation enhances administrative efficiency while reducing inconsistent security practices. DHCP automates IP address allocation, minimising configuration errors and improving scalability across segmented subnets [21]. When combined with subnetting strategies such as VLSM, DHCP enhances efficient address utilisation and simplifies network administration.

VPN technologies provide encrypted communication across public networks, ensuring confidentiality and integrity of inter-site traffic between geographically dispersed locations

[22]. Certificate Authorities underpin Public Key Infrastructure (PKI) models by issuing and validating digital certificates that establish trusted communication channels between systems and services [23].

However, improper configuration, weak authentication policies, or inadequate certificate lifecycle management may introduce vulnerabilities such as unauthorised access, address conflicts, or trust exploitation [24]. Therefore, effective integration, secure configuration, and ongoing management of these services directly determine the resilience, scalability, and trustworthiness of enterprise infrastructures such as NOSS2026.

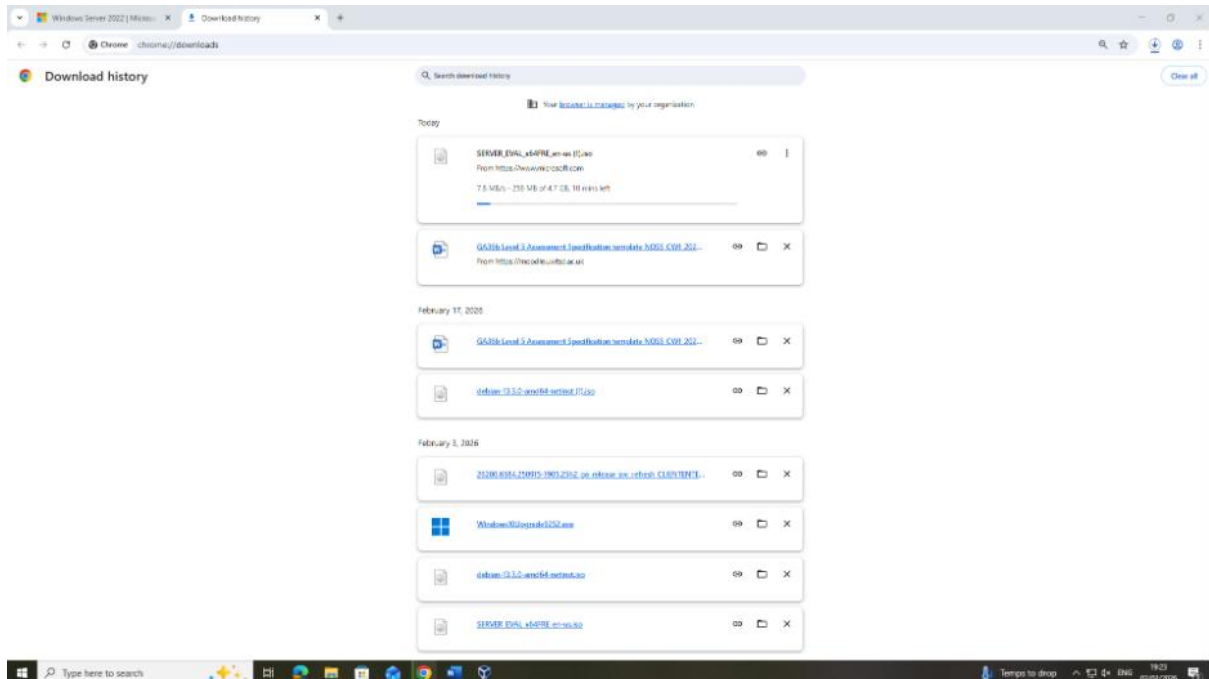
TASK 2

The virtual network was deployed using a selected hypervisor platform to host Windows Server and Debian Server environments. The implementation followed the topology requirements of the NOSS2026 scenario, ensuring logical connectivity between virtual machines. The deployment process involved configuring IP addressing, establishing network adapters, and performing connectivity testing to verify communication within the virtualised environment.

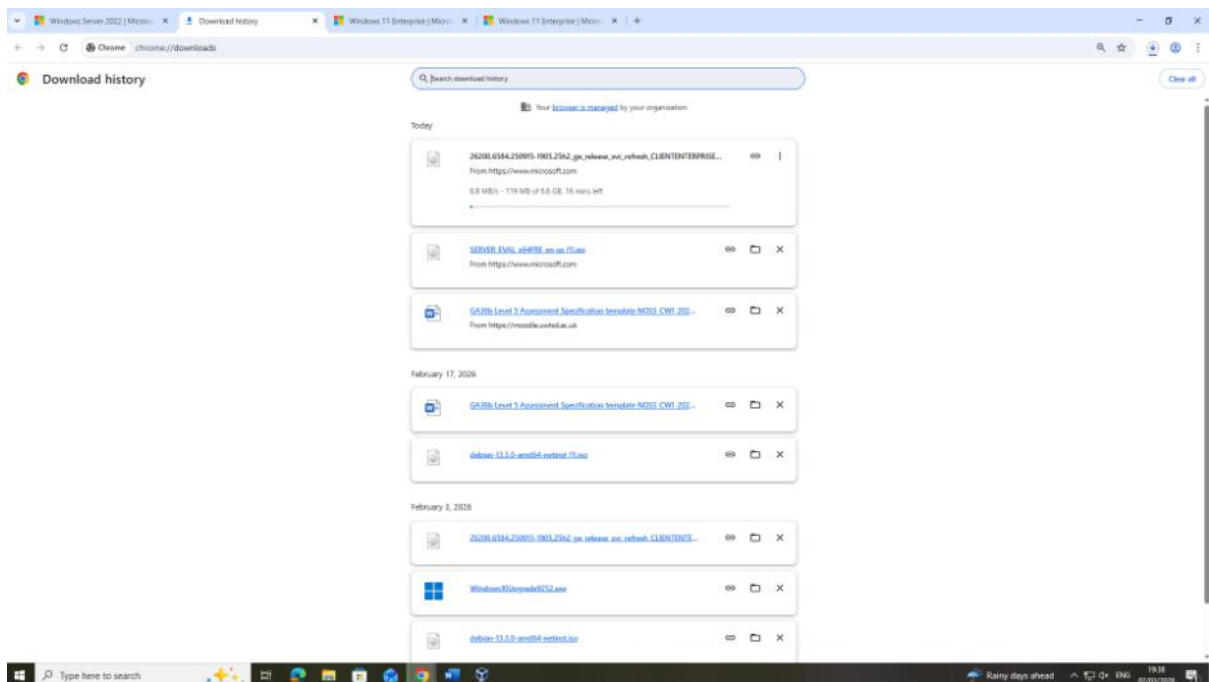
A Type 2 hypervisor was selected due to its accessibility, ease of installation, and compatibility with the available hardware resources. Although Type 1 hypervisors provide better performance in large enterprise environments, the Type 2 architecture was sufficient for this academic deployment scenario. The choice supports simultaneous hosting of Windows and Debian servers while maintaining practical implementation simplicity.

Screenshots

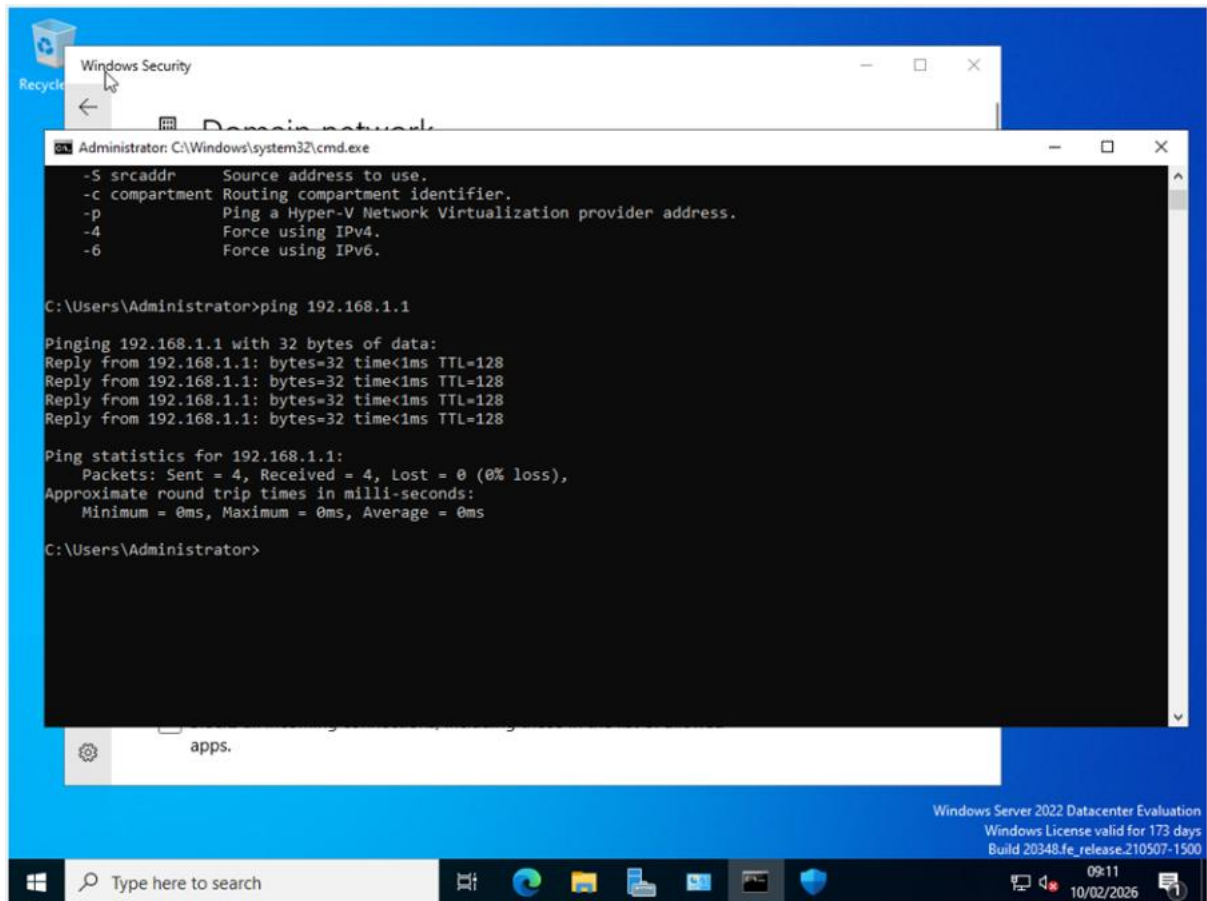
Windows server download



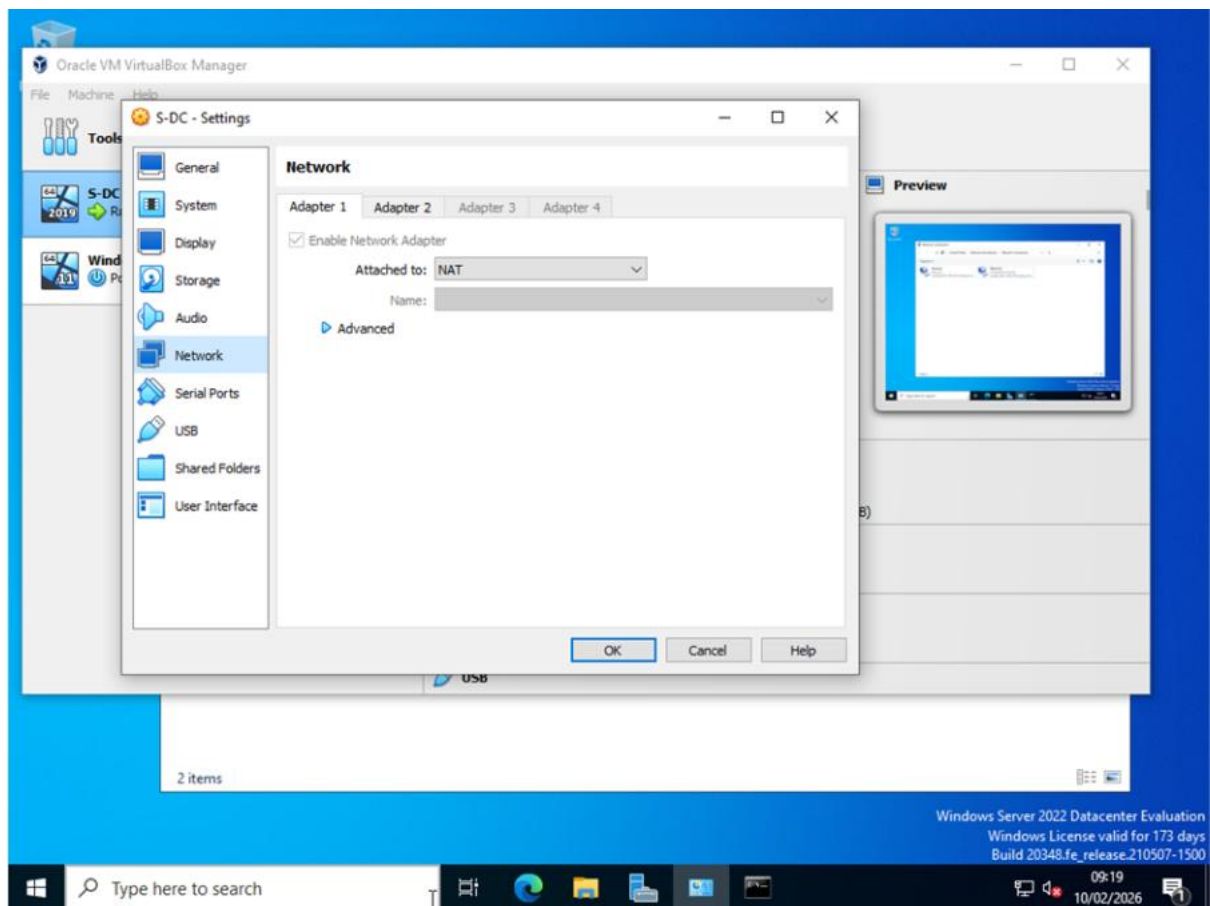
Windows 11 Enterprise download



Successful ping

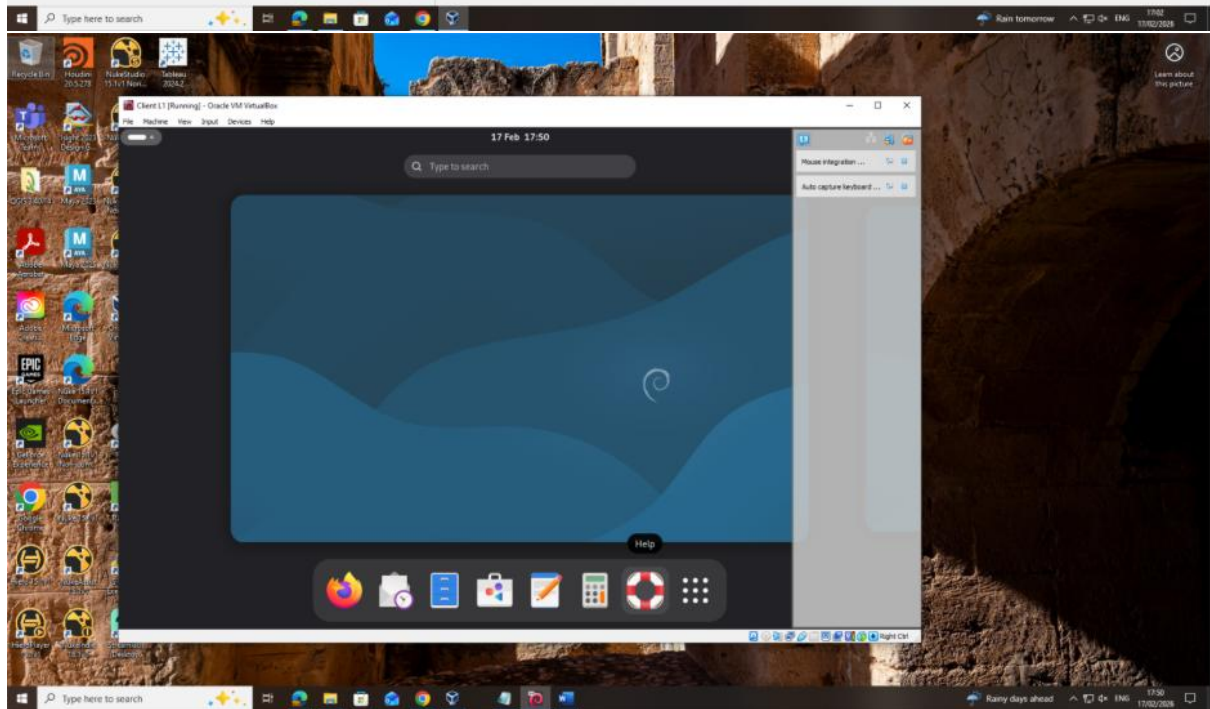
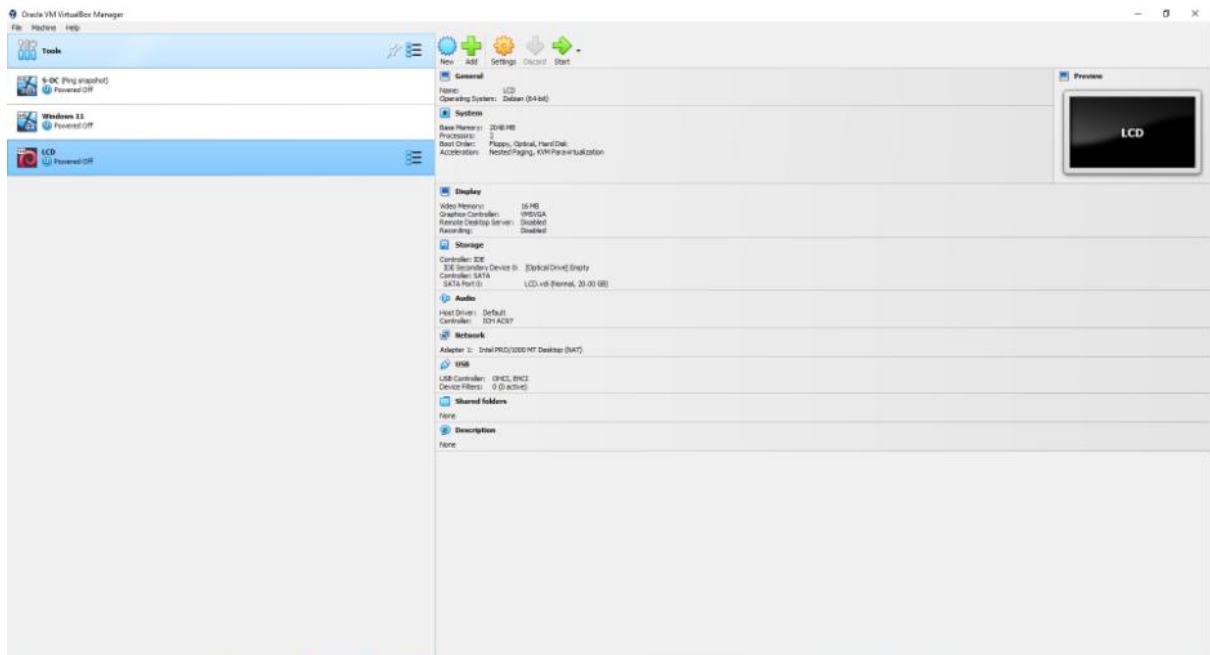


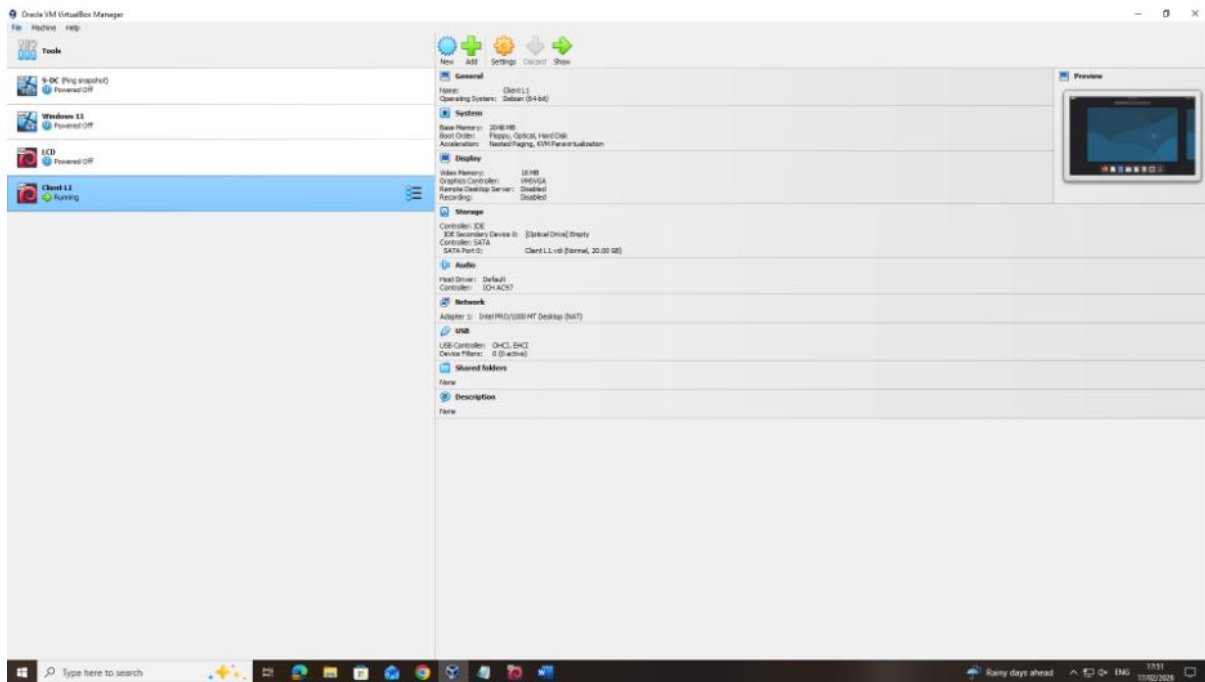
Network Adapter 1



Network Adapter 2

[illegible]





TASK 3

Although I encountered some difficulty fully mastering every technical detail of the deployment process, the exercise allowed me to gain a basic operational understanding of virtual network configuration and testing procedures. The assignment provided practical exposure to setting up virtualised networking environments, which helped me better appreciate how theoretical networking concepts are applied in real implementations.

During the deployment process, I learned the importance of accurate IP configuration and systematic connectivity testing. I attempted to verify communication between virtual machines using network diagnostic tools.

In future network deployment tasks, I would aim to improve my technical knowledge of subnet design, routing configuration, and service integration within virtual infrastructures. Overall, this assignment helped me develop foundational practical skills in network deployment and troubleshooting while reinforcing my understanding of virtualised enterprise networking concepts.

References

- [1] M. Pearce, S. Zeadally, and R. Hunt, "Virtualization: Issues, security threats, and solutions," *ACM Computing Surveys*, vol. 45, no. 2, pp. 1–39, Feb. 2013.
- [2] J. Brodtkin, "A look at bare-metal hypervisor basics," *Network World*, vol. 27, no. 14, pp. 1, 11, Jul. 26, 2010.
- [3] M. Moore and A. Zenla, "Goldilocks Isolation: High Performance VMs with Edera," Jan. 2025.
- [4] J. Brodtkin, "A look at bare-metal hypervisor basics," *Network World*, vol. 27, no. 14, pp. 1, 11, Jul. 26, 2010.
- [5] Z. Aalam, V. Kumar, and S. Gour, "A review paper on hypervisor and virtual machine security," *Journal of Physics: Conference Series*, vol. 1950, no. 1, Aug. 2021, doi: 10.1088/1742-6596/1950/1/012027.
- [6] R. Langmann and S. Arts, "Application virtualization in virtual learning labs," in *Proc. 9th Int. Conf. Remote Engineering and Virtual Instrumentation*, 2012.
- [7] *IP Addressing and Subnetting Including IPv6*. Syngress, Elsevier Science & Technology Books, 2000.
- [8] K. M. M. Fathima, "A survey on multiprotocol label switching in virtual private networks," in *Proc. 2nd Int. Conf. I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, 2018, pp. 737–740.
- [9] J. Beeharry and B. Nowbutsing, "Forecasting IPv4 exhaustion and IPv6 migration," in *Proc. IEEE Int. Conf. Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*, 2016, pp. 336–340.
- [10] Y. Muni, "Understanding the evolution of internet protocols: An in-depth review of IPv4 and IPv6," *International Journal of Advanced Research in Computer Science*, vol. 16, no. 4, pp. 109–117, Aug. 2025, doi: 10.26483/ijarcs.v16i4.7307.
- [11] S. N. Sisat, P. S. Bhopale, and V. K. Barbudhe, "IP subnetting," *International Journal of Electronics, Communication and Soft Computing Science & Engineering*, vol. 2, no. 5, pp. 5–9, 2012.
- [12] H. A.-R. Lafta and A. O. Hoori, "Design and implementation of a VLSM simulator," *Journal of Engineering*, vol. 18, no. 9, pp. 1030–1041, Jul. 2023.
- [13] H. Singh, *Implementing Cisco Networking Solutions: Configure, Implement, and Manage Complex Network Designs*. Packt Publishing, 2017.
- [14] Q. Li, Y. Wu, J. Duan, J. Yang, and Y. Jiang, "Weighted NSFIB aggregation with generalized next hop of strict partial order," *IEEE Transactions on Network and Service Management*, vol. 19, no. 2, pp. 890–904, Jun. 2022.
- [15] M. Amin, D. Kurnia, and K. Mikli, "Design of three class internet protocol routing model based on Linux command line interface," *Journal of Applied Engineering and Technological Science*, vol. 3, no. 2, pp. 133–138, Jun. 2022.

- [16] P. Singh and T. Sood, "A comparative analytical survey on RIP, EIGRP and OSPF," in *Proc. 2nd IEEE Delhi Section Flagship Conf. (DELCON)*, 2023, pp. 1–6.
- [17] R. Rakheja, S. Khera, N. Turk, and S. Kamboj, "Parametric analysis of dynamic routing protocol for wireless sensor networks," *Multimedia Tools and Applications*, vol. 82, no. 25, pp. 39035–39055, Oct. 2023.
- [18] I. Nikolaevskiy, "Scalability and resiliency of static routing," ProQuest Dissertations & Theses, 2016.
- [19] O. Afolalu and M. S. Tsoeu, "Enterprise networking optimization: A review of challenges, solutions, and technological interventions," *Future Internet*, vol. 17, no. 4, p. 133, Apr. 2025.
- [20] D. Francis, *Mastering Active Directory: Deploy and Secure Infrastructures with Windows Server 2016 and PowerShell*, 2nd ed. Birmingham: Packt Publishing, 2019.
- [21] R. S. Priya, R. Ramprasad, J. Narayanan, D. Balaji, and S. Kishor, "A DHCP based approach to IP address management and allocation in a network using VLSM," in *Proc. Int. Conf. Advanced Computing and Communication Systems*, vol. 1, 2023, pp. 882–887.
- [22] A. Hasani and M. Niklekaj, "Security of VPNs in high-surveillance environments: A comparative study of VPN alternatives," *Ingenious*, vol. 5, no. 1, pp. 108–116, Feb. 2025.
- [23] P. A. Kadam et al., "ValidCertify: An effective blockchain-based domain certificate authentication and verification scheme," *Peer-to-Peer Networking and Applications*, vol. 18, no. 4, Art. no. 177, Aug. 2025.
- [24] M. Smine, D. Espes, N. Cuppens-Boulahia, and F. Cuppens, "Network functions virtualization access control as a service," in *Lecture Notes in Computer Science*, vol. 12122, 2020, pp. 100–117.