

Network Operating Systems and Services

ACCA5023



Hashim Hasan
2409446

TASK 1

RESEARCH ON HYPERVISORS

A hypervisor is a virtualization technology that allows multiple operating systems to run concurrently on a single physical machine by abstracting hardware resources. There are two primary hypervisor types:

Type 1 (bare-metal) hypervisors run directly on the hardware, providing high performance, security, and scalability. Type 2 (hosted) hypervisors operate atop an existing operating system, making them easy to install and manage.

While Type 1 hypervisors are often favoured for enterprise and large-scale deployments, Type 2 hypervisors offer several advantages, particularly for smaller-scale or more flexible environments. Type 2 hypervisors, such as VMware Workstation or Oracle VirtualBox, require minimal hardware changes and can be installed like regular software. This makes them cost-effective and accessible, especially for organisations or individuals without dedicated server hardware.

For a topology that hosts both Windows Server 2025 and Debian Server, a Type 2 hypervisor is a suitable option when convenience, compatibility, and ease of use are top priorities. Type 2 hypervisors support a wide array of guest operating systems, making them highly compatible. They are ideal for testing, development, and educational purposes where rapid deployment and flexibility are important.

While they may not offer the highest level of performance or security, their straightforward setup, lower hardware requirements, and ability to run on existing systems make them practical for mixed environments where enterprise-level scalability is not the primary concern.

IP AND ROUTING

INTERNET PROTOCOL

IP addressing is foundational for data transmission on the Internet. When data moves from one computer to another, it is broken into packets, each labeled with source and destination IP addresses. These addresses act like postal codes, ensuring data reaches the right recipient.

Routers and switches play distinct roles in this process. Routers read IP addresses on packets, determining the best path across interconnected networks, while switches operate within local networks, directing packets based on MAC addresses for efficient internal delivery.

IPv4 addresses are 32-bit numbers, typically shown in dotted decimal format (e.g., 192.168.1.1), allowing about 4.3 billion unique addresses. IPv6, introduced to address IPv4 exhaustion, uses 128-bit hexadecimal notation (e.g.,

2001:0db8:85a3:0000:0000:8a2e:0370:7334), vastly expanding address capacity . Subnetting divides a network into smaller segments, boosting security and efficient address allocation. For example, the address 192.168.1.0/24 indicates a network with 256 possible host addresses, simplifying management, and reducing broadcast traffic.

Diagrams can illustrate subnetting, such as:

Network: 192.168.1.0/24

-- Subnet 1: 192.168.1.0/26 (64 hosts)

-- Subnet 2: 192.168.1.64/26 (64 hosts)

In summary, IP addressing structures data delivery, supports network scalability, and underpins Internet functionality.

ROUTING PROTOCOL

Routing protocols are essential for directing data across networks, ensuring packets reach their intended destinations efficiently. Their primary purpose is to determine the best path for data transmission within or between networks. Routing can be managed using either static or dynamic methods.

Static routing involves manually configuring routes on routers or servers. This approach offers predictability and control, making it suitable for small or simple networks where routes rarely change. However, it requires manual intervention to update routes when network changes occur, which can be time-consuming and error-prone.

Dynamic routing, on the other hand, uses protocols like RIP, OSPF, or EIGRP to enable routers to automatically exchange information and adapt to network

changes. This scalability and adaptability make dynamic routing preferable for larger or more complex networks, as it reduces administrative overhead and improves resilience to failures.

Given a topology where a Debian Server acts as a DHCP Relay and a Windows Server requires connectivity, the suitable routing approach depends on network complexity. If the topology is straightforward with minimal route changes (for example, a single path between servers and clients), static routing could be efficient and secure. However, if the network is expected to grow or change frequently, or if there are multiple potential paths between devices, dynamic routing is advantageous to ensure seamless client connectivity and automated route updates. In most educational or small business scenarios, static routing may suffice, but dynamic routing offers greater flexibility for evolving topologies.

VIRTUAL PRIVATE NETWORK

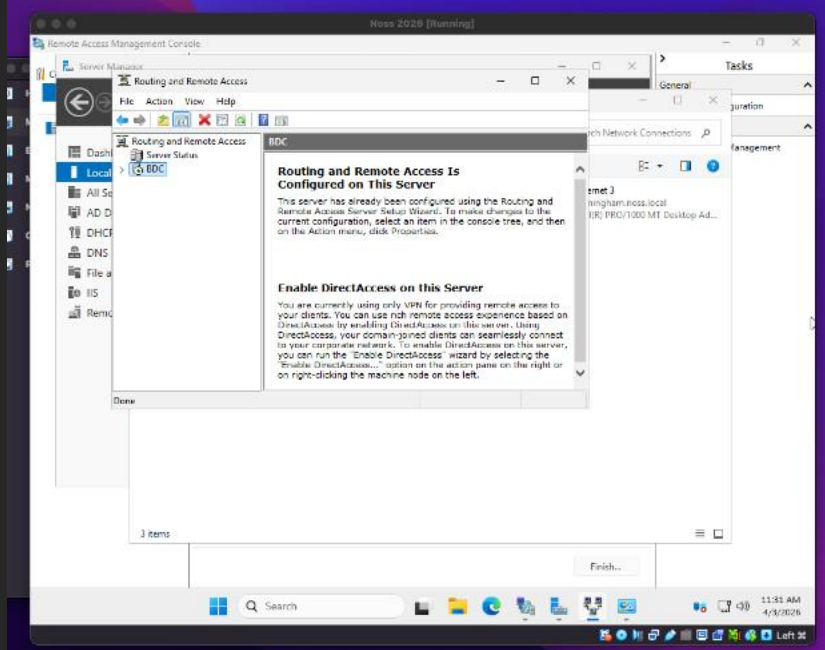
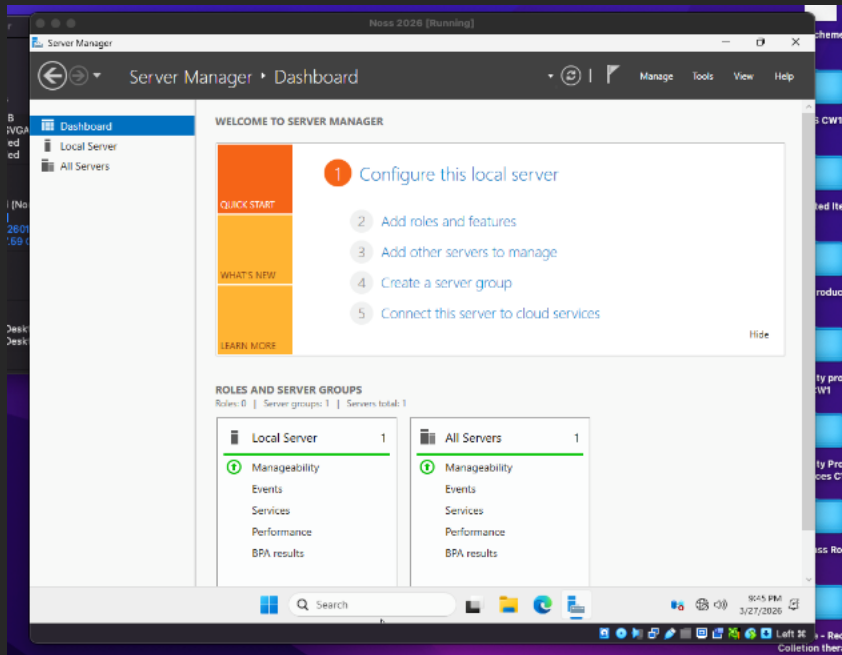
Virtual Private Networks (VPNs) provide secure, encrypted connections over public networks, enabling remote users to access organisational resources as if they were on a local network. Key features include data encryption, authentication, and remote access capabilities. Best practices involve using strong encryption protocols (such as OpenVPN or IPsec), enforcing multi-factor authentication, and regularly updating VPN software to mitigate vulnerabilities.

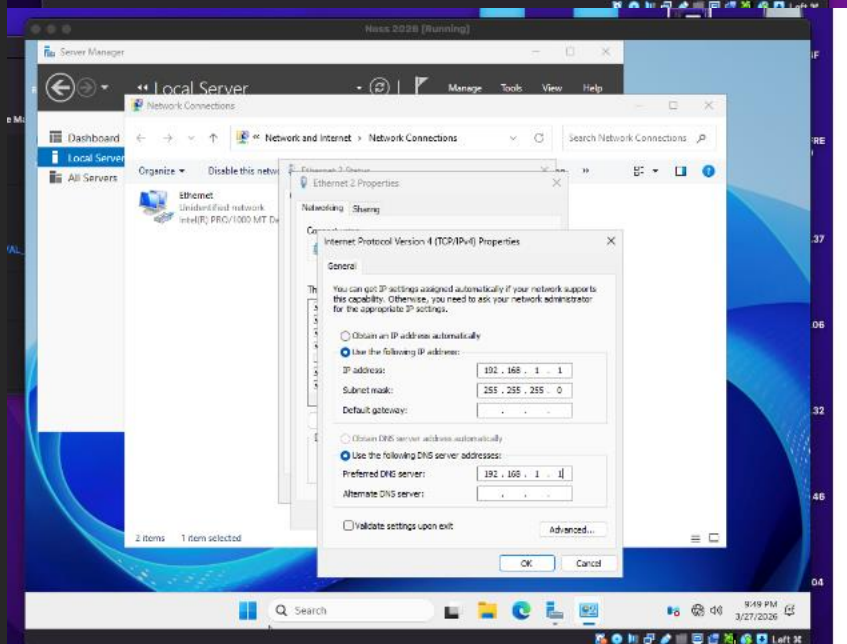
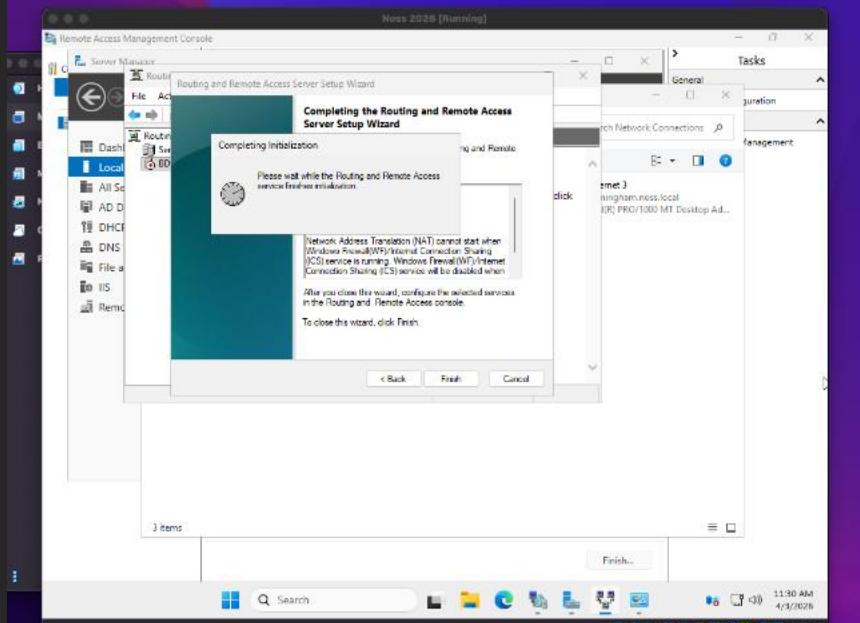
Dynamic Host Configuration Protocol (DHCP) automates the assignment of IP addresses and network configuration to devices on a network, reducing manual errors and administrative workload. Its key features include dynamic IP assignment, lease management, and support for redundant servers. Best practices include using DHCP reservations for critical devices, implementing DHCP failover for high availability, and segmenting DHCP scopes to minimise broadcast traffic. Active Directory Domain Services (AD DS) is Microsoft's directory service that manages user accounts, authentication, and resource access in Windows networks. AD DS features centralised authentication, policy management via Group Policy, and scalability across multiple domains. Best practices encompass implementing strong password policies, regularly reviewing user permissions, and maintaining a robust backup and disaster recovery plan.

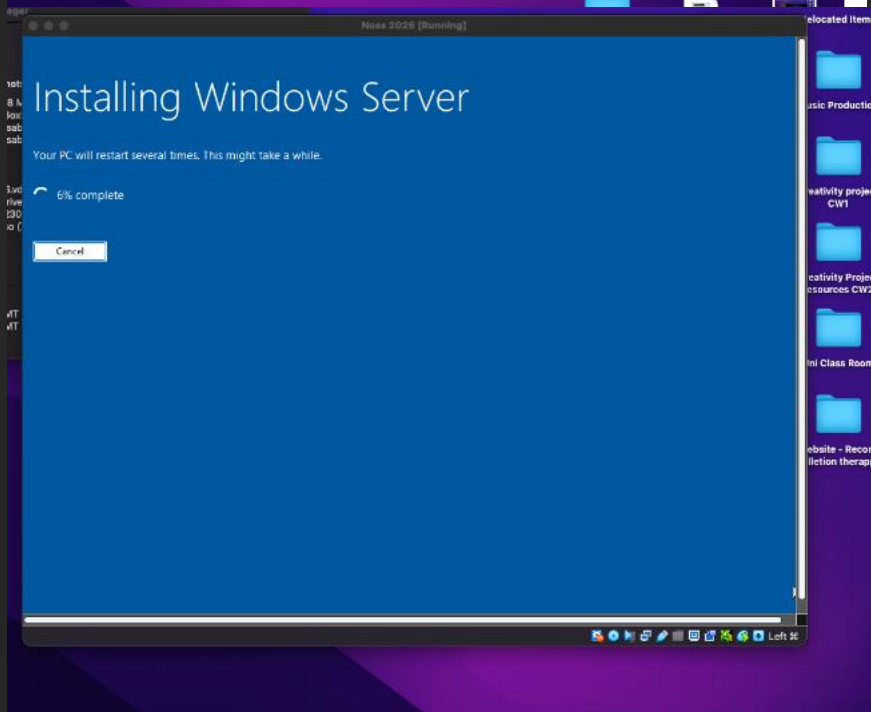
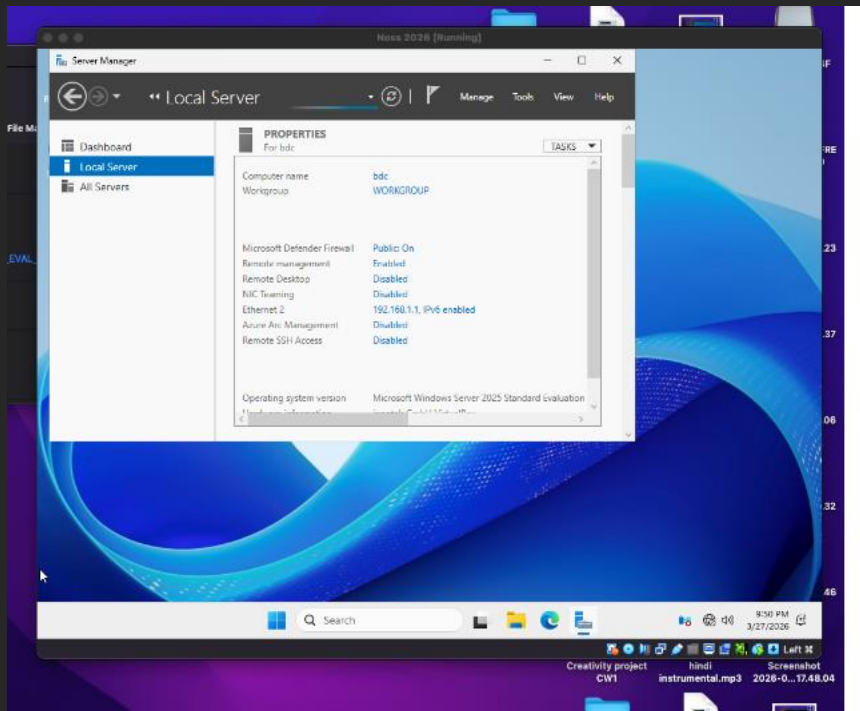
Certificate Authorities (CAs) issue digital certificates that validate the identity of users, devices, or services, enabling secure communication and trust within a network. Key features include certificate issuance, management, and revocation. Best practices include protecting the root CA with strict physical and logical security, deploying subordinate CAs for operational tasks, and routinely auditing certificate usage and

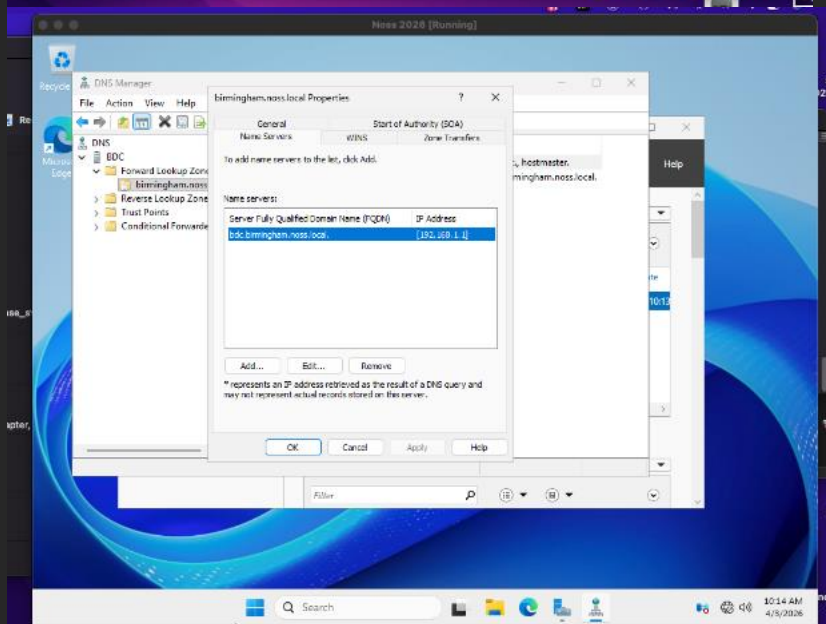
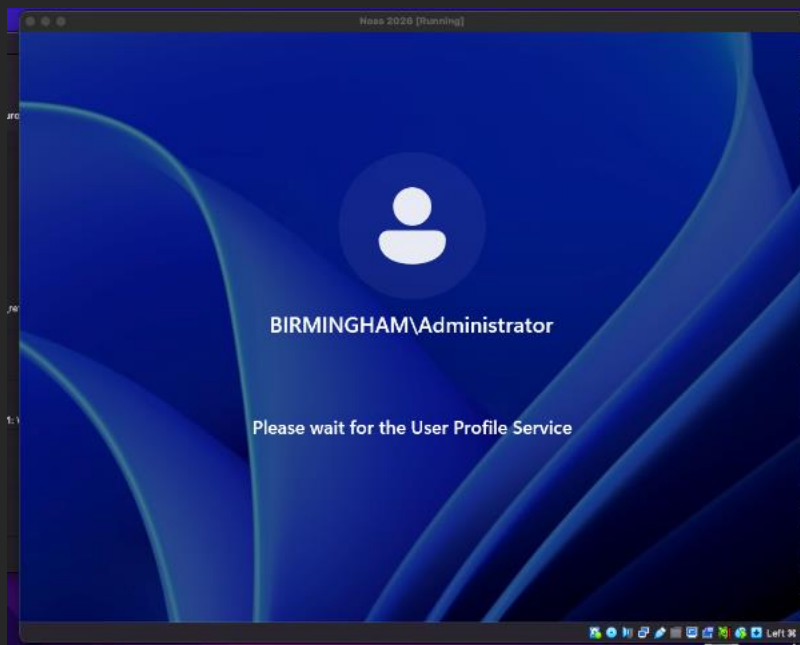
TASK 2

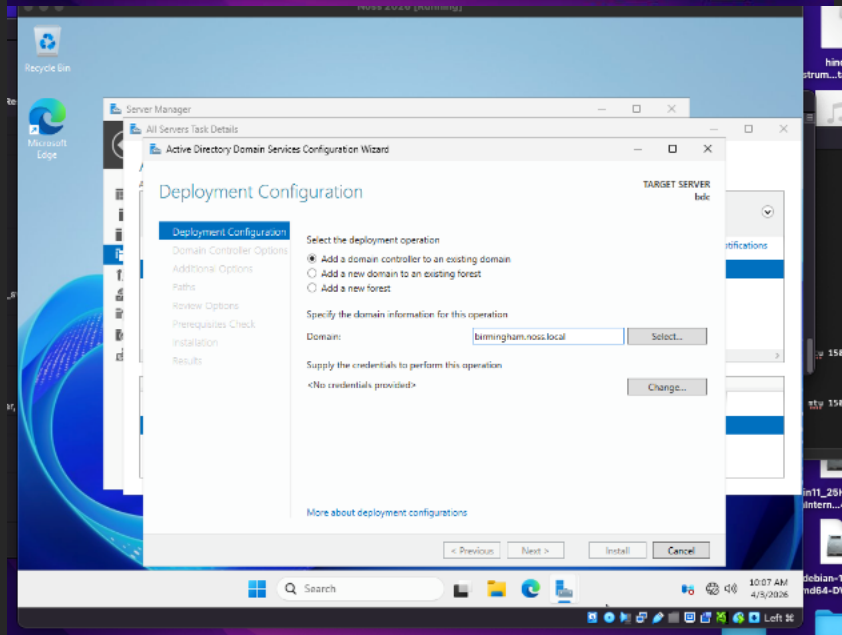
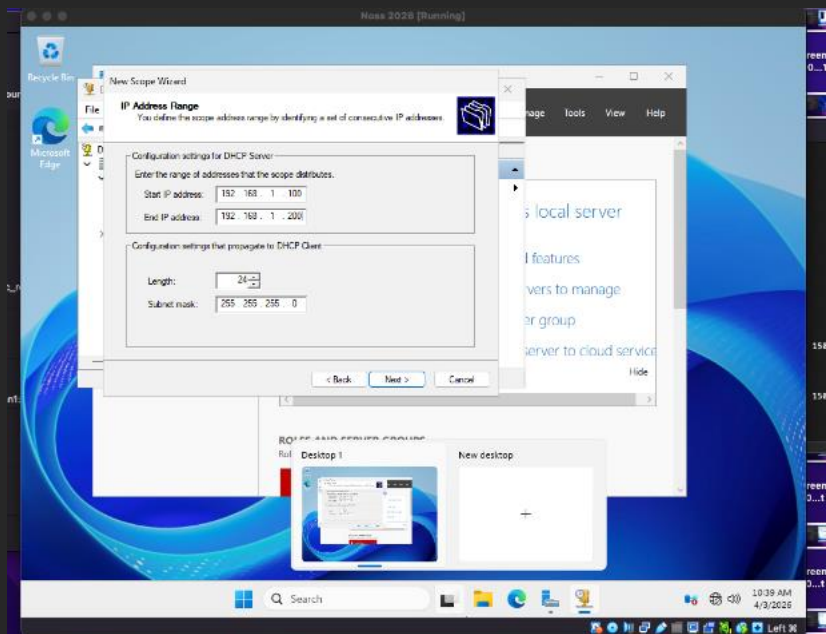
TECHNICAL DOCUMENTATION

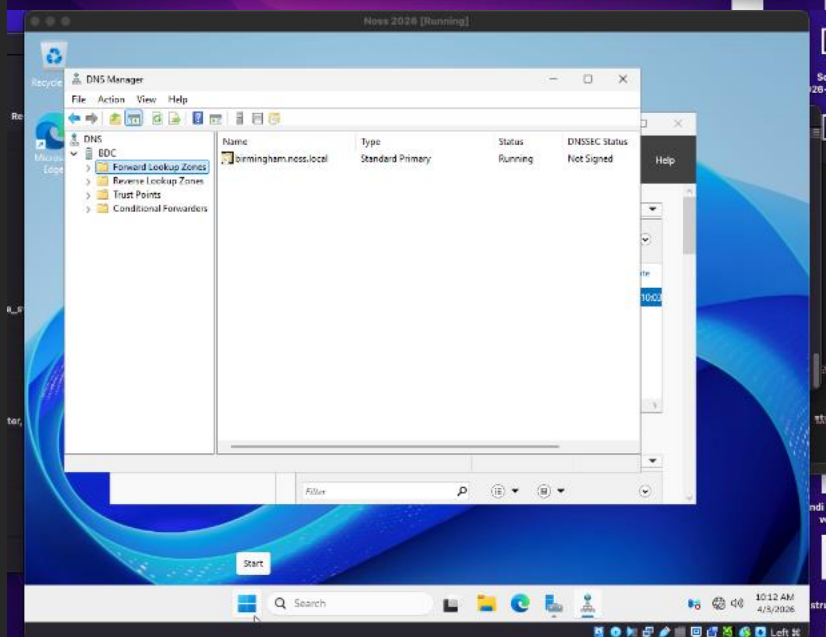
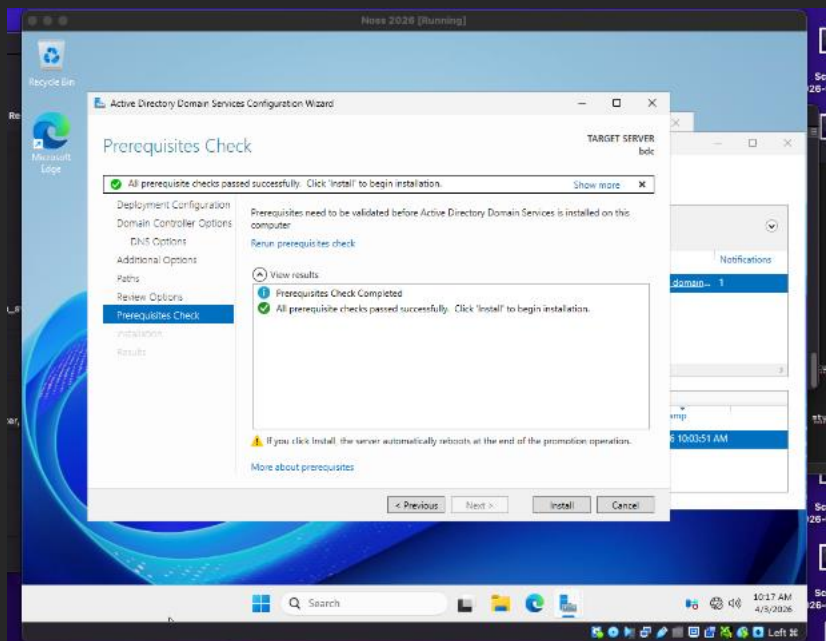


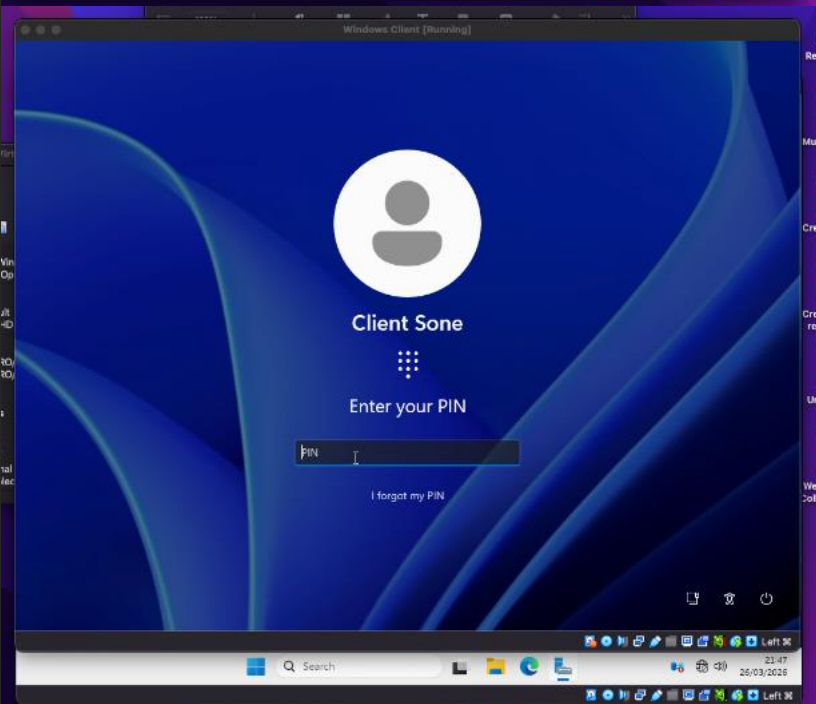
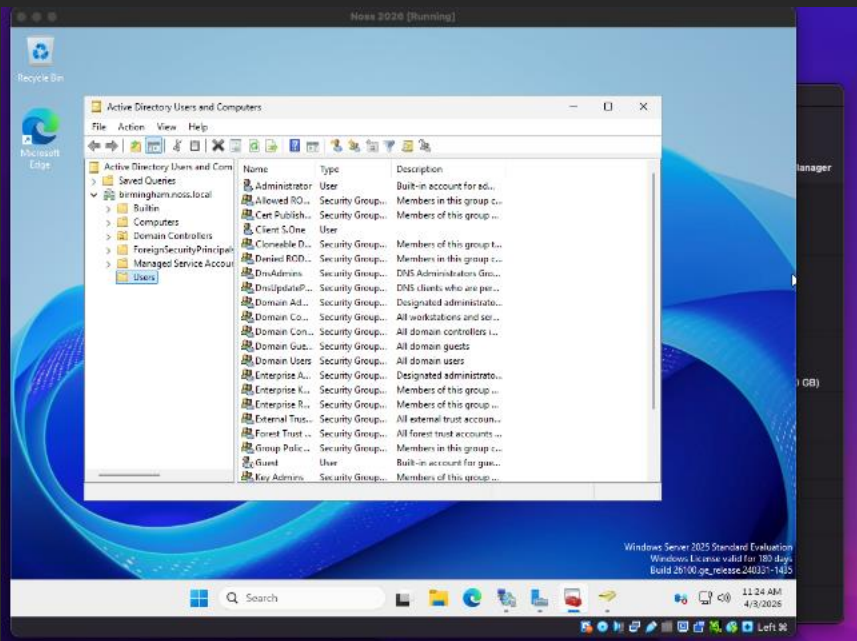


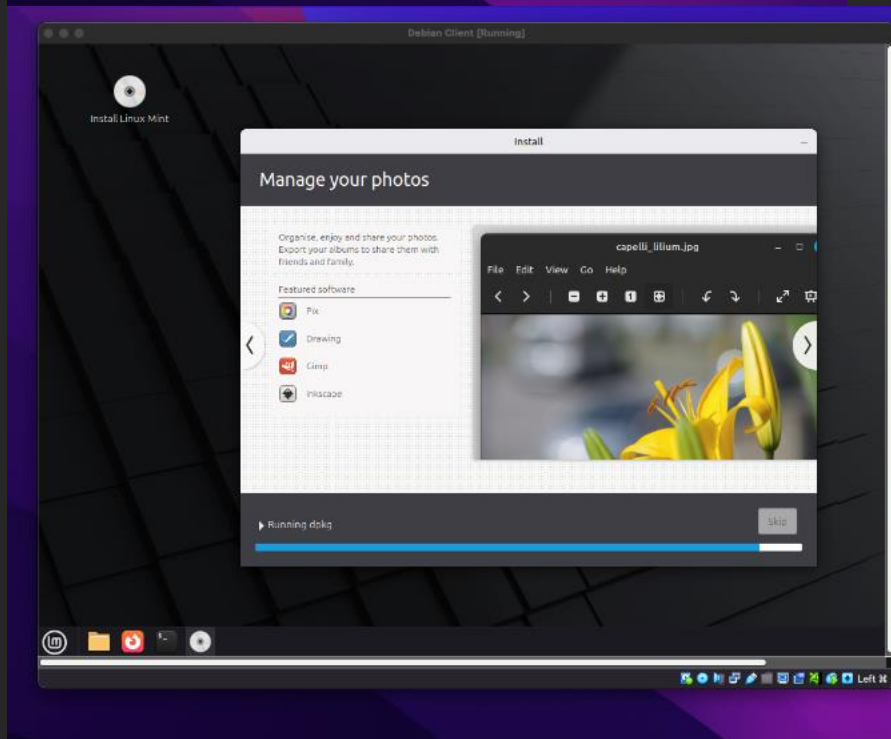
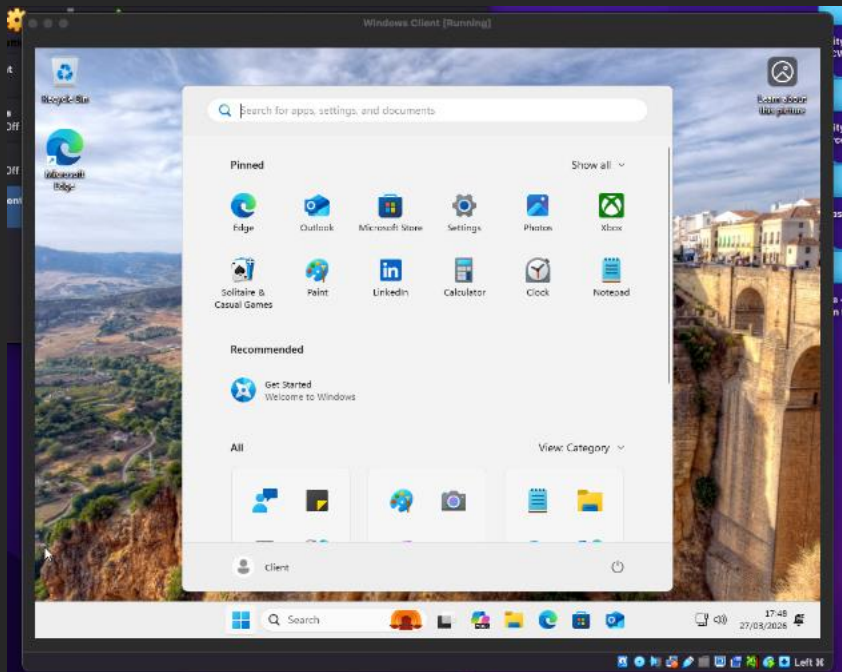


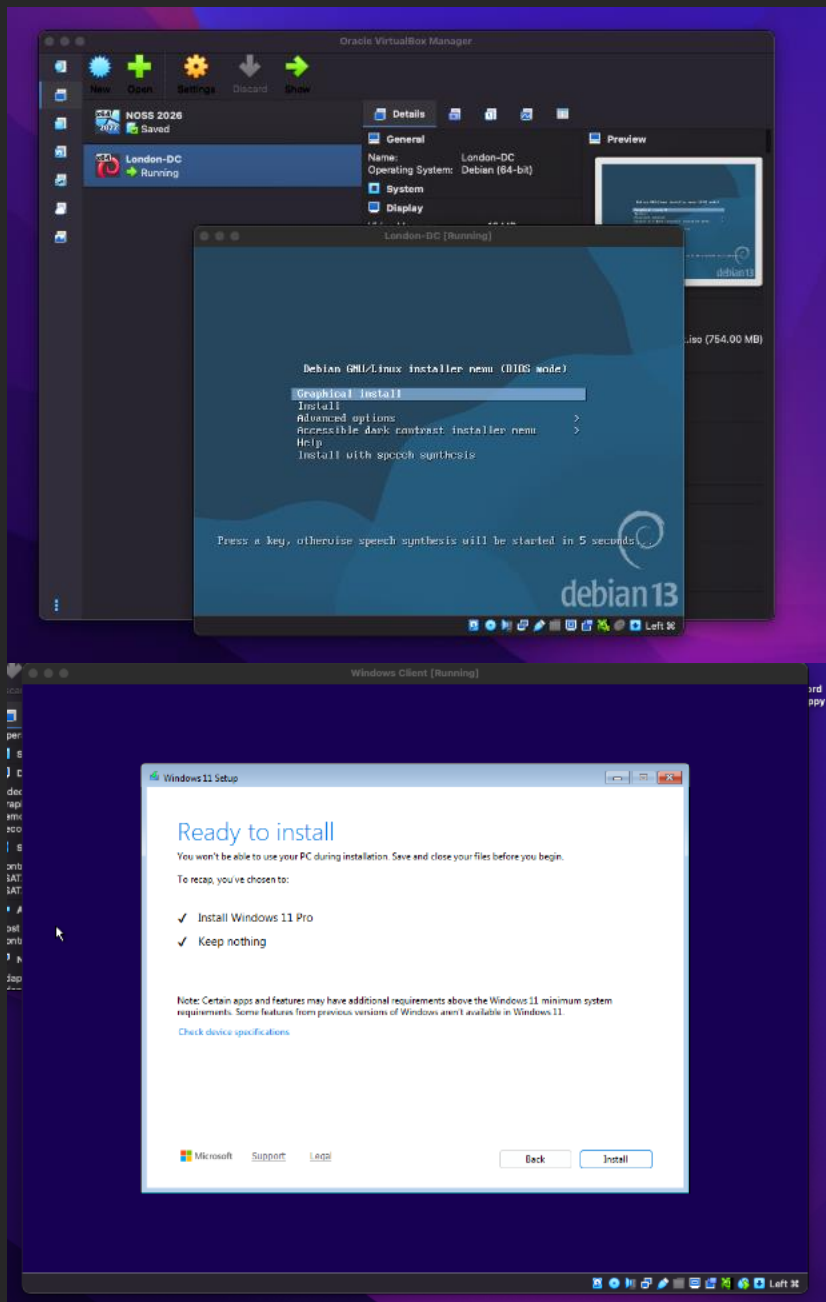


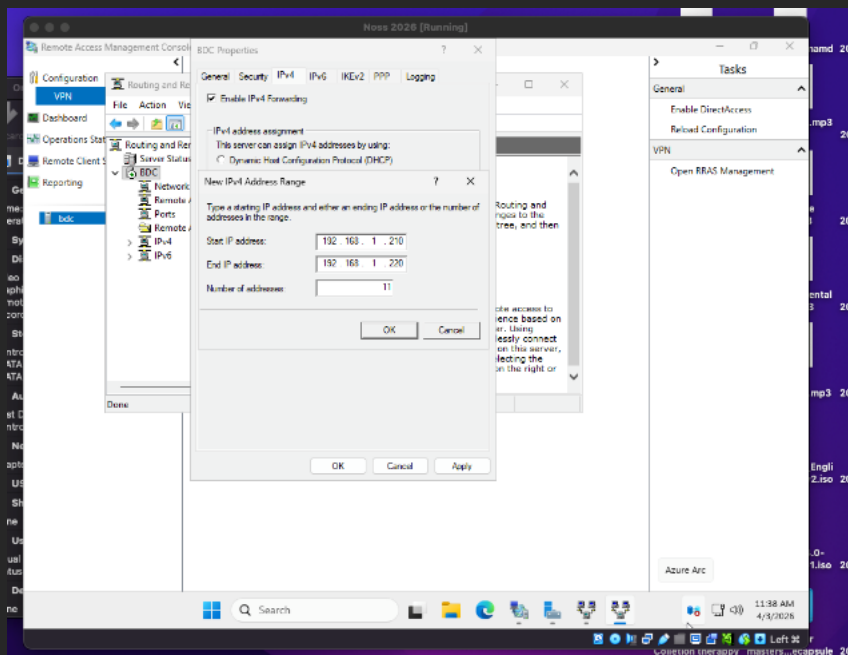












CONCLUSION

In conclusion, this technical documentation is inconclusive due to unresolved technical difficulties experienced while conducting the testing. The primary challenge arose from attempting to run multiple virtual machines simultaneously using Oracle VirtualBox, which was used for all environments, including Windows Server 2025, Debian 13 Server, Windows 11 Pro, and Linux Mint OS.

Due to these difficulties, I was unable to fully test and verify network connectivity between Windows Server 2025 and Windows 11 Pro, as well as between Debian 13 Server and Linux Mint OS. The inability to establish and monitor inter-VM network connections limited the scope of the documentation and prevented definitive findings regarding connectivity and interoperability between the respective server and client operating systems.

As a result, while the documentation outlines the intended procedures and configurations, it does not provide conclusive results or verification of successful connectivity due to the technical constraints encountered with Oracle VirtualBox during the evaluation process.

REFERENCES

W. Stallings, *Operating Systems: Internals and Design Principles*, 9th ed., Pearson, 2018.

“Hypervisors: Types, Benefits, and Use Cases,” VMware, [Online]. Available: <https://www.vmware.com/topics/glossary/content/hypervisor>

R. Perlman, D. Green, and M. Kaufman, *Network Security: Private Communication in a Public World*, 3rd ed., Prentice Hall, 2010.

A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th ed., Pearson, 2011.

“Internet Protocol Version 6 (IPv6) Overview,” Internet Engineering Task Force (IETF), RFC 8200, July 2017. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc8200>

T. A. Lammle, *CCNA Certification Study Guide*, 9th ed., Wiley, 2020.

“Routing Basics,” Cisco, [Online]. Available: <https://www.cisco.com/c/en/us/td/docs/internetworking/technology/handbook/route.pdf>

“VPN Overview,” Microsoft Learn, [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/remote/remote-access/vpn/vpn-overview>

“Dynamic Host Configuration Protocol (DHCP),” Internet Engineering Task Force (IETF), RFC 2131, March 1997. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc2131>

“Active Directory Domain Services Overview,” Microsoft Learn, [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

“Certificate Authority Guidance,” National Institute of Standards and Technology (NIST), Special Publication 800-32, [Online]. Available: <https://csrc.nist.gov/publications/detail/sp/800-32/final>