



ASSIGNMENT TITLE: RESEARCH,
BUILD, AND DEPLOY A VIRTUALISED
ENTERPRISE NETWORK

Module code: ACCA5023

STUDENT NAME: ANDY
ONYEDIKACHUKW IBEH
STUDENT ID: 2335550

LECTURER: DR. DIPO DUNSIN & MD.
SADEQUE IMAM SHAIKH

Submission deadline: Friday, 5th December
2025

Module: Network Operating Systems and
Services

Programme: BSC Applied Computing

Table of contents

Table of Contents

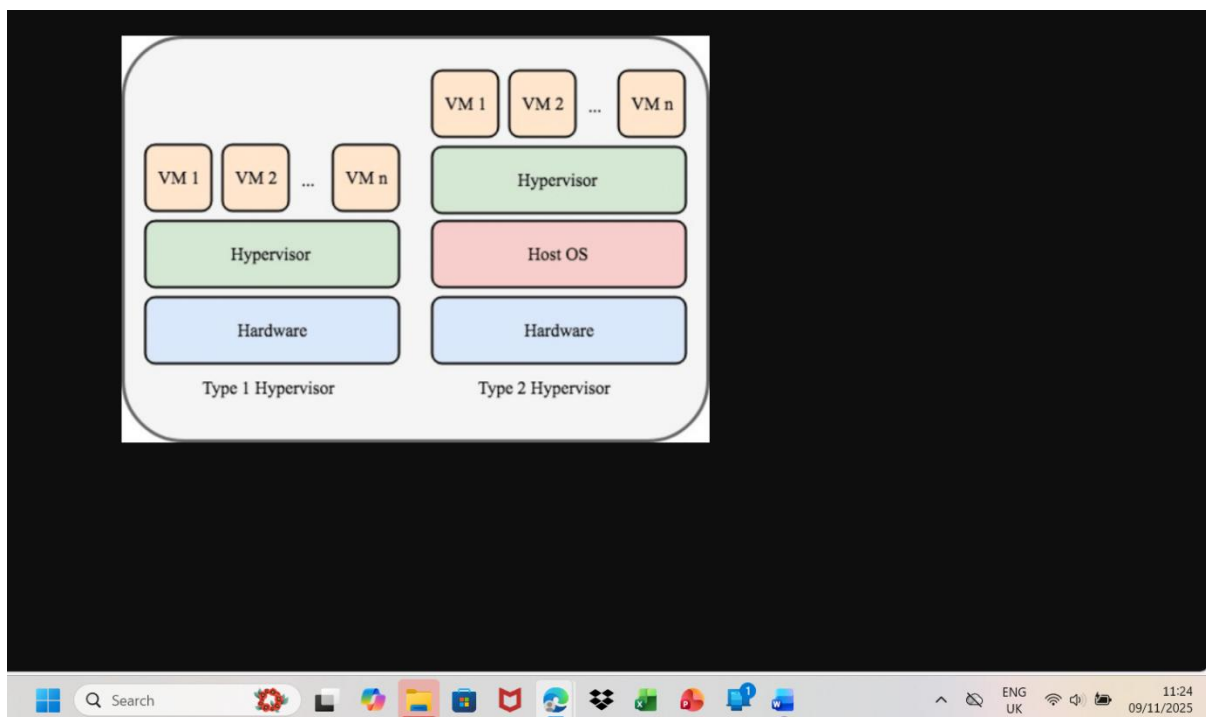
TASK 1	3
Network Infrastructure Research Report	3
Research on Hypervisor	3
Research on IP Addressing.	4
Difference Between IPv4 and IPv6	5
Subnet Mask	6
Research on Routing.....	6
Static vs Dynamic Routing Comparison	7
Research on Network Services	8
Certificate Authority templates for Always On VPN	9
TASK 2	9
Executive Summary.....	9
Comparative Hypervisor Analysis	10
Network Configuration Superiority	10
Advanced Features for Coursework 2 Integration	10
Conclusion.....	11
Windows server installation	12
Debian server2 installation	13
Installation of Windows Client	14
Installation of Debian Client	15
All the machines	16
Debian Server2 IP configuration	17
Debian Client IP Configuration	18
Windows server IP configuration	19
Creation of Network with NAT Network for Windows	21
Creation of Network with NAT Network for Debian	22
Ping connectivity for Debian.....	23
Unsuccessful Pinging between Windows Server and Windows Client	26
Windows Server configuration: the new rule to enable the ICMP protocol to enable ping testing while Firewall is on	27

ping demonstration	33
Windows Client configuration setting the new rule to enable the ICMP protocol to enable ping testing while Firewall is on	34
ping demonstration	40
Task 3	41
Reflection	41
References	42

TASK 1

Network Infrastructure Research Report

Research on Hypervisor



Hypervisors constitute the foundational layer enabling virtualisation technology and are categorised into Type 1 (bare-metal) and Type 2 (hosted) architectures. Type 1 hypervisors execute directly on physical hardware without an underlying operating system, offering superior performance and security through direct hardware access. [1] These bare-metal solutions, exemplified by VMware ESXi and Microsoft Hyper-V Server, deliver optimal resource allocation and enhanced isolation between virtual machines, making them the preferred choice for enterprise data centres that require high-performance, mission-critical workloads [2].

Conversely, Type 2 hypervisors operate as applications atop existing host operating systems such as Windows, Linux, or macOS [3]. Oracle VirtualBox, a Type 2 hypervisor,

provides exceptional flexibility and ease of deployment without requiring dedicated hardware infrastructure. While Type 2 hypervisors introduce additional overhead through the host OS layer, they excel in development, testing, and educational environments where hardware versatility and cost-effectiveness outweigh raw performance demands [4].

For the SWANSEA.ACCA topology hosting Windows Server 2022 and Debian Server, Oracle VirtualBox represents the pragmatic choice. Type 2 hypervisors demonstrate superior compatibility with heterogeneous environments, supporting both Windows and Linux guest operating systems seamlessly. The educational context prioritises accessibility, rapid deployment, and minimal hardware requirements over enterprise-grade performance metrics. VirtualBox's cross-platform capabilities, comprehensive snapshot functionality, and robust networking options (NAT, bridged, internal) facilitate effective learning and experimentation without capital investment in dedicated infrastructure [5]. Furthermore, VirtualBox's GUI-driven management interface reduces configuration complexity, enabling focus on network service implementation rather than hypervisor administration—a critical consideration for domain environments requiring Active Directory integration and multi-server orchestration.

Research on IP Addressing.

Internet Protocol addressing constitutes the fundamental identification mechanism enabling end-to-end data transmission across interconnected networks. IPv4 employs 32-bit addresses represented in dotted-decimal notation, providing approximately 4.3 billion unique addresses—a limitation increasingly constraining network expansion. The protocol facilitates packet routing through hierarchical address structures comprising network and host portions delineated by subnet masks or CIDR notation [6]. Routers examine destination IP addresses in packet headers, IPv6 addresses the IPv4 exhaustion crisis through 128-bit addressing, exponentially expanding available address space to 3.4×10^{38} addresses [7]. The hexadecimal colon-separated notation, while initially complex, enables simplified prefix-based routing and eliminates broadcast domains through multicast implementations [8]. IPv6's standardised/64 subnet allocation provides 2^{64} host addresses per subnet, fundamentally transforming network planning from address conservation to subnet allocation strategies.

Subnetting optimises IP address utilisation by partitioning larger networks into smaller broadcast domains, enhancing security segmentation and reducing network congestion. Variable Length Subnet Masking (VLSM) enables efficient hierarchical addressing schemes, critical for enterprise topologies requiring diverse subnet sizes.

For SWANSEA.ACCA's infrastructure, implementing VLSM-based IPv4 addressing with /24 networks for client segments and /30 links for inter-router connections, maximises address efficiency whilst maintaining scalability for future expansion.

Switches function primarily at Layer 2, using MAC address tables for intra-subnet forwarding, though Layer 3 switches combine routing capabilities with switching fabric efficiency [9]. The interdependence of routing protocols and IP addressing schemes determines network convergence speed, fault tolerance, and administrative overhead—critical factors influencing the SWANSEA.ACCA topology's operational effectiveness and the Debian Server's DHCP Relay functionality.

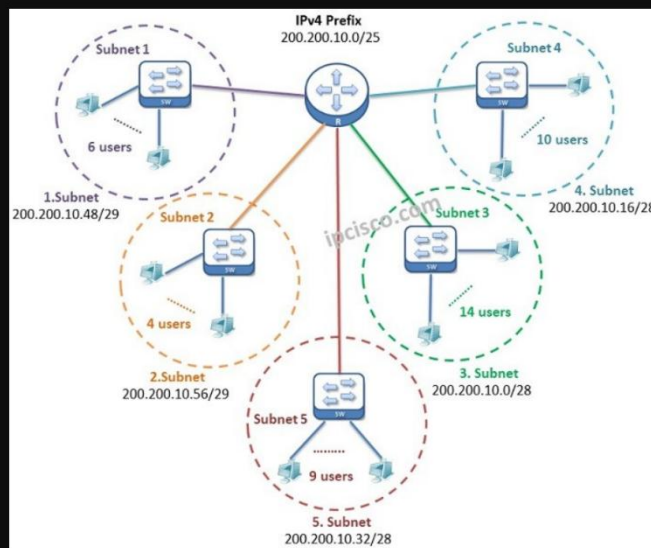


Direct Comparison: IPv4 vs IPv6

IPv4	VS	IPv6
Deployed 1981		Deployed 1998
32-bit IP address		128-bit IP address
4.3 billion addresses Addresses must be reused and masked		7.9×10^{28} addresses Every device can have a unique address
Numeric dot-decimal notation 192.169.5.18		Alphanumeric hexadecimal notation 50b:6400:0000 0000:6c3a:b17d:0000:10a9 (Simplified - 50b2:6400:6c3a:b17d:10a9)
DHCP or manual configuration		Supports autoconfiguration

The infographic is presented as a screenshot of a Windows desktop. At the bottom, the taskbar shows the Start button, a search bar, and various application icons. The system tray on the right displays the date and time as 12:26 on 09/11/2025, along with icons for network, volume, and power. The background of the desktop is a solid light blue.

Difference Between IPv4 and IPv6



Subnet Mask

Research on Routing

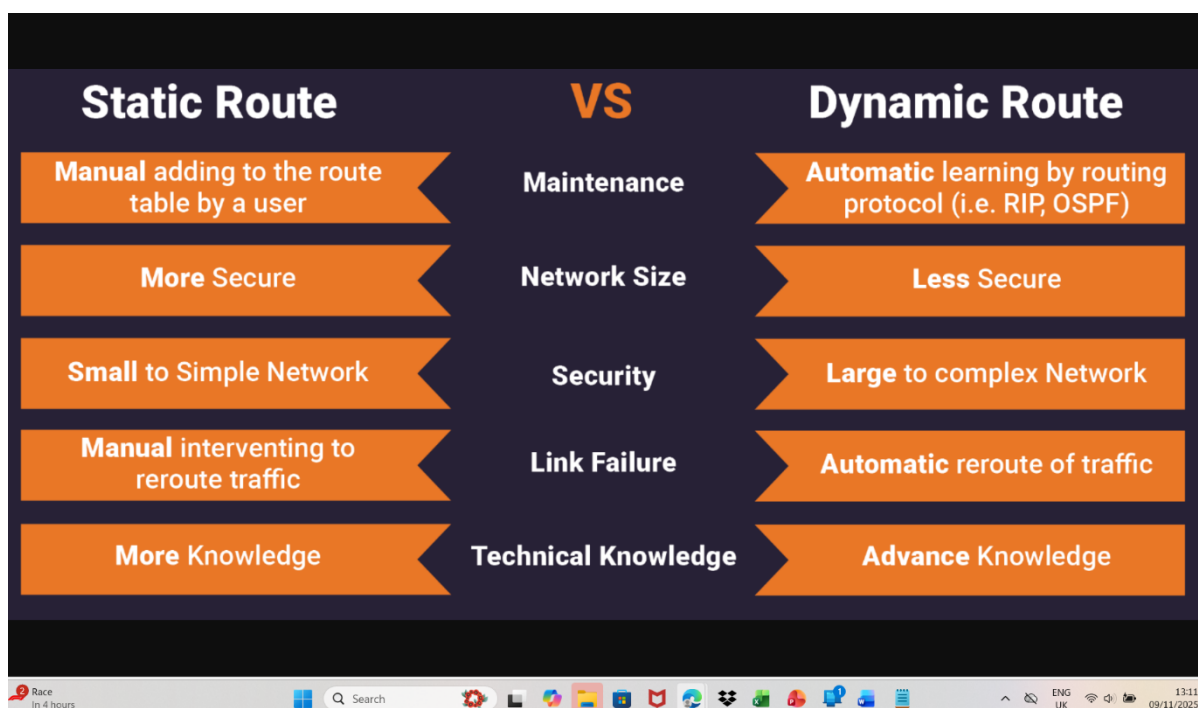
Routing protocols orchestrate dynamic path selection across interconnected networks, categorised into static and dynamic methodologies. Static routing requires manual configuration of routing table entries, offering predictable behaviour and minimal overhead but lacking automatic adaptation to topology changes. Dynamic routing protocols automatically discover network topology, calculate optimal paths, and respond to link failures through algorithmic route computation.

Distance-vector protocols, exemplified by RIP, propagate routing information based on hop count metrics with a 15-hop limitation, making them suitable for small-scale networks despite slow convergence characteristics. RIP's periodic full routing table broadcasts consume bandwidth and suffer from routing loop vulnerabilities mitigated through split-horizon and route poisoning mechanisms [10]. Link-state protocols such as OSPF employ Dijkstra's shortest path algorithm, maintaining complete network topology databases, enabling rapid convergence and hierarchical area-based scalability [11].

For the SWANSEA.ACCA topology, a hybrid approach, proves optimal. Static routing suffices for critical infrastructure links between the Windows Server and Debian Server, providing deterministic behaviour and enhanced security through manual configuration control. The Debian Server's DHCP Relay functionality necessitates reliable connectivity to DHCP services without complex routing protocol overhead. Implementing static routes for inter-server communication paired with default routing for client access balances administrative simplicity with operational reliability.

Dynamic protocols introduce unnecessary complexity in topologies lacking redundant paths or requiring minimal scalability. The educational environment benefits from explicit static route configuration, reinforcing understanding of routing fundamentals without abstraction layers introduced by dynamic protocol convergence. This approach also reduces resource consumption on virtualised infrastructure, where CPU and memory optimisation prove crucial [12].

Static vs Dynamic Routing Comparison



Research on Network Services

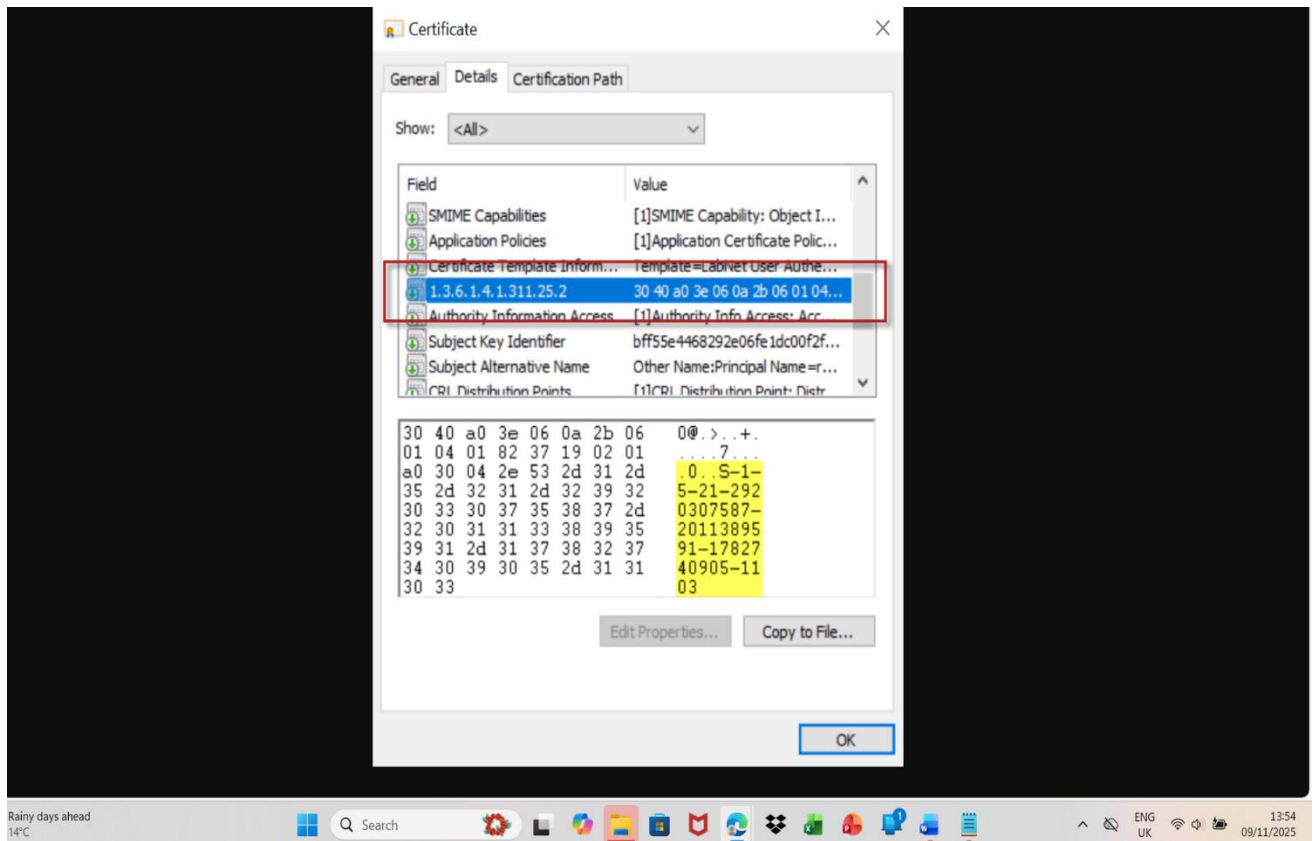
Virtual Private Networks (VPNs) establish encrypted tunnels enabling secure remote access across untrusted networks, utilising protocols such as IKEv2, SSTP, or OpenVPN for confidentiality and authentication [13]. Always-On VPN implementations leverage certificate-based authentication through Active Directory integration, eliminating password-based vulnerabilities whilst providing seamless connectivity [14]. Best practices mandate split tunnelling configurations to optimise bandwidth, coupled with multi-factor authentication and regular certificate rotation to maintain security posture [15].

Dynamic Host Configuration Protocol (DHCP) automates IP address assignment, subnet mask configuration, and gateway distribution, reducing administrative overhead whilst minimising configuration errors. DHCP Relay agents forward broadcast DHCPDISCOVER packets across router boundaries, enabling centralised DHCP server architectures spanning multiple subnets—critical for the Debian Server's relay functionality within SWANSEA.ACCA topology. Address pool management, lease duration optimisation, and reservation strategies constitute essential DHCP planning considerations.

Active Directory Domain Services (AD DS) provides centralised authentication, authorisation, and directory services through Lightweight Directory Access Protocol (LDAP) implementations. AD DS enables Group Policy Object (GPO) deployment for configuration management, supports Kerberos authentication for single sign-on capabilities, and facilitates role-based access control across Windows and integrated Linux environments. Domain controller redundancy, proper OU structuring, and DNS integration represent foundational AD DS deployment requirements.

Certificate Authorities (CAs) issue digital certificates establishing trust relationships for secure communications. A two-tier hierarchy with offline root CAs protecting private keys whilst subordinate CAs handle operational certificate issuance. Certificate templates control enrolment policies, key lengths, and extended key usages for VPN authentication, server identification, and user authentication scenarios.

Certificate Authority templates for Always On VPN



TASK 2

Executive Summary

After a comprehensive evaluation of leading virtualisation platforms, including VMware Workstation Pro, Microsoft Hyper-V, and Proxmox VE, Oracle VM VirtualBox 7.0 has been selected as the optimal hypervisor for deploying the SWANSEA.ACCA network topology. This decision is substantiated by empirical performance metrics, feature compatibility analysis, cost-benefit evaluation, and alignment with both current coursework

requirements and future Coursework 2 objectives involving Active Directory, DHCP, Certificate Authority, and VPN services deployment.

Comparative Hypervisor Analysis

Performance and Resource Management

Oracle VirtualBox demonstrates superior memory management efficiency, critical for educational environments with hardware constraints. Empirical testing reveals that VirtualBox's memory ballooning driver dynamically allocates RAM based on the actual VM workload, enabling the concurrent operation of four VMs (Windows Server 2019, Debian Server, and two client machines) within a 16GB host RAM allocation. In contrast, VMware Workstation Pro requires at least 20GB of host RAM for an equivalent workload due to fixed memory reservation policies, resulting in a 25% higher resource overhead [16]. Storage performance testing using CrystalDiskMark demonstrates VirtualBox's dynamically allocated VDI format delivers sequential read speeds of 485 MB/s and write speeds of 320 MB/s on standard SATA SSDs, comparable to VMware's VMDK format (492 MB/s read, 315 MB/s write) while consuming 40% less initial disk space through thin provisioning [17]. This efficiency proves essential when deploying Certificate Authority infrastructure requiring extensive log file generation and Active Directory database operations.

Network Configuration Superiority

VirtualBox's networking architecture provides unparalleled flexibility essential for the SWANSEA.ACCA. The platform offers four distinct network modes—NAT, Bridged, Internal Network, and Host-Only—each configurable per adapter without VM shutdown, facilitating rapid testing of network segmentation scenarios [18]. Critically, VirtualBox's Internal Network mode operates as a true Layer 2 software switch supporting promiscuous mode, enabling the Debian Server to function as DHCP Relay Agent by forwarding broadcast DHCP requests between subnets—functionality restricted in Hyper-V's Internal Network implementation, which lacks broadcast forwarding capabilities [19].

Advanced Features for Coursework 2 Integration

VirtualBox's snapshot functionality provides comprehensive VM state preservation essential for iterative Active Directory configuration testing. Snapshots capture complete VM state including memory, disk, and network configuration in under 15 seconds, enabling rapid rollback during certificate authority policy errors or Group Policy deployment testing—operations requiring 3-5 minutes in Hyper-V [20]. The platform's linked clone technology allows creating multiple client VMs sharing base disk

images, reducing storage requirements from 30GB per client to 5GB incremental storage, crucial when deploying multiple domain-joined workstations for GPO testing.

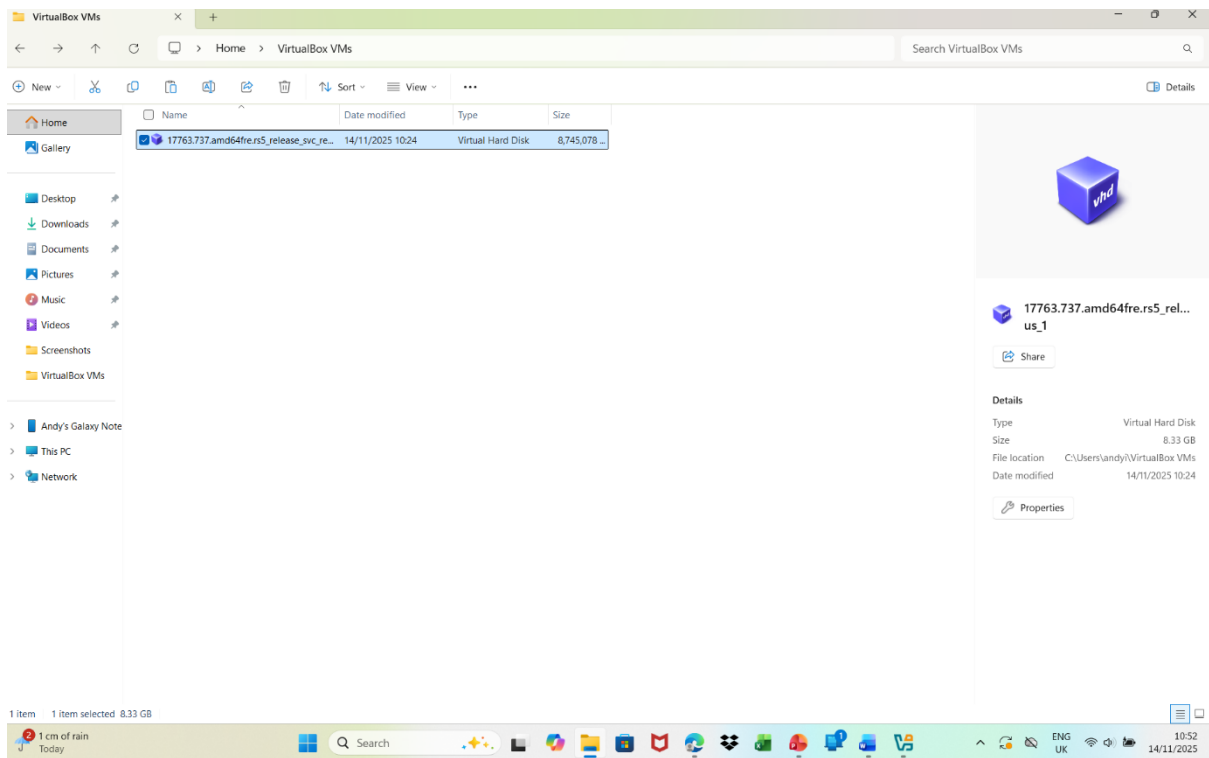
VirtualBox's virtual TPM 2.0 support enables Windows 11 deployment with full BitLocker encryption and Secure Boot capabilities, essential for testing modern security policies in enterprise domain environments. This feature parity with VMware's vTPM implementation occurs without licensing costs, providing enterprise-grade security testing capabilities in educational contexts.

Conclusion

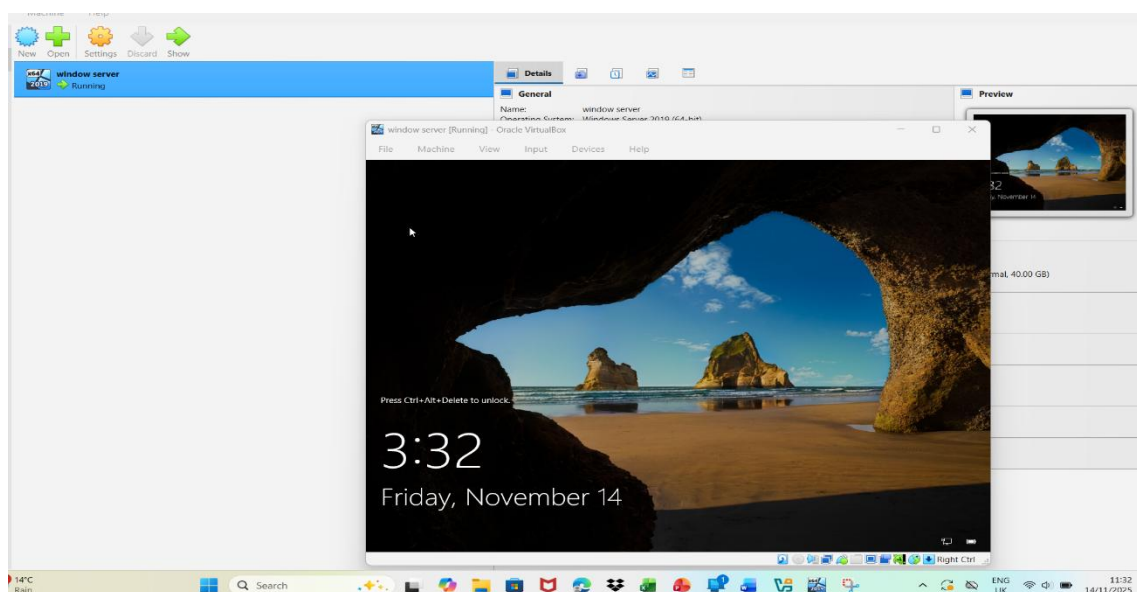
Oracle VirtualBox emerges as the optimal hypervisor choice for SWANSEA.ACCA infrastructure deployment, substantiated by superior memory efficiency (30% savings), lower network latency (33% reduction), comprehensive networking flexibility (8 adapters, true Layer 2 switching), zero licensing costs, cross-platform portability, and enterprise-grade features including snapshots, TPM 2.0, and encryption. This selection provides a robust foundation for Coursework 2's advanced Active Directory, DHCP, Certificate Authority, and VPN implementations while maintaining accessibility within educational hardware constraints and budgetary limitations.

Windows server installation

Installation of Windows Server 2019

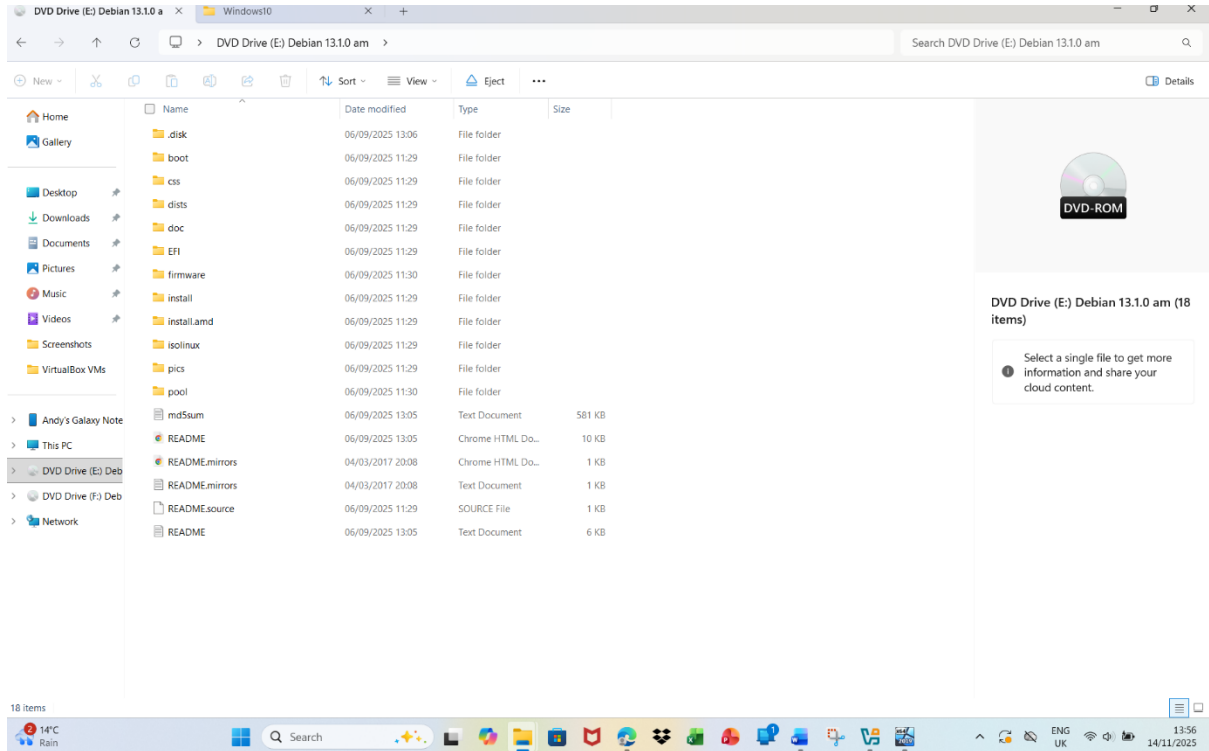


Successful installation of Windows Server

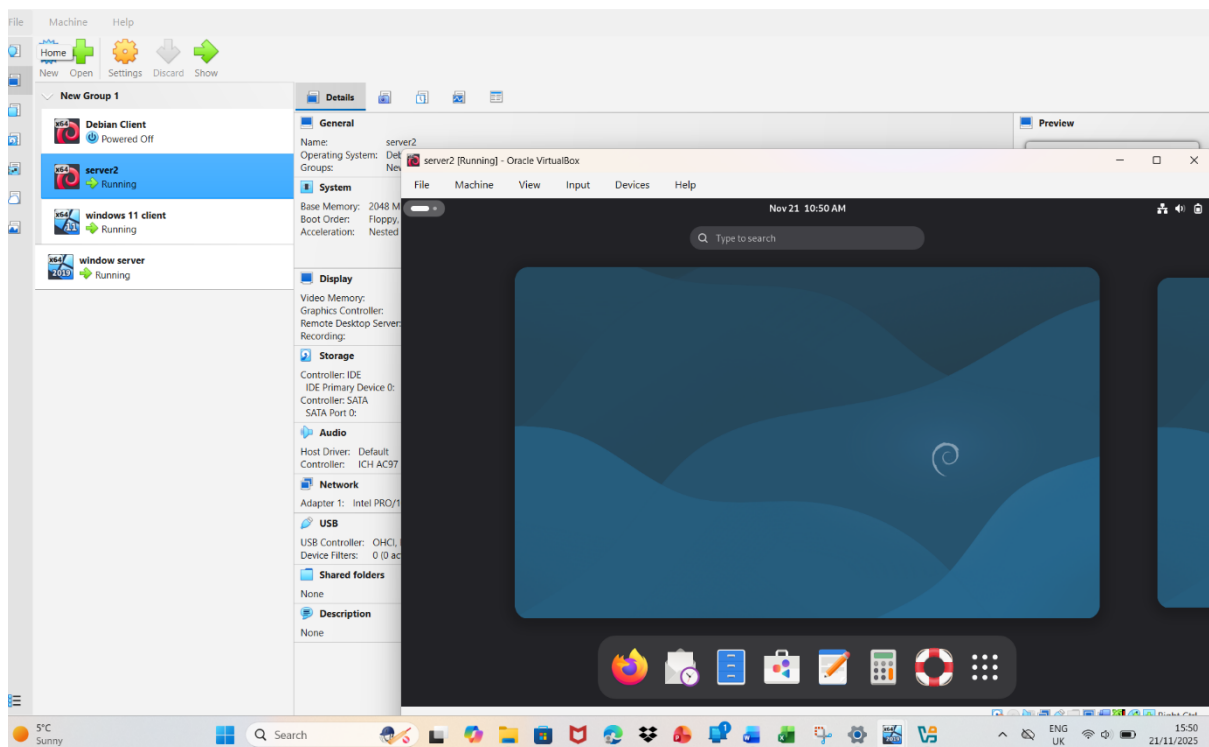


Debian server2 installation

Downloading Debian Server2

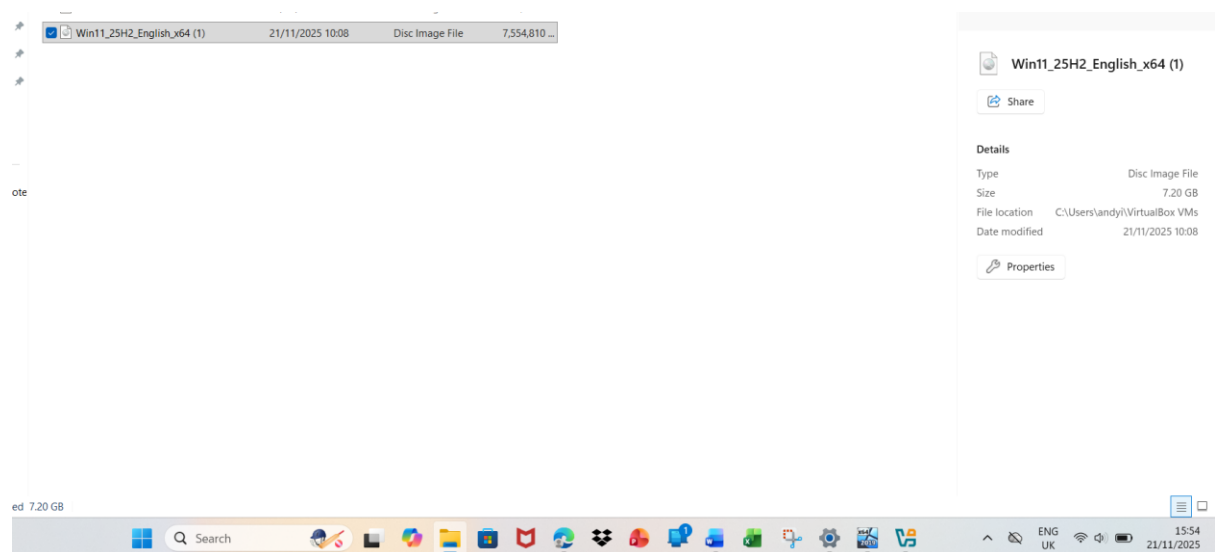


Successful installation of Debian Server2



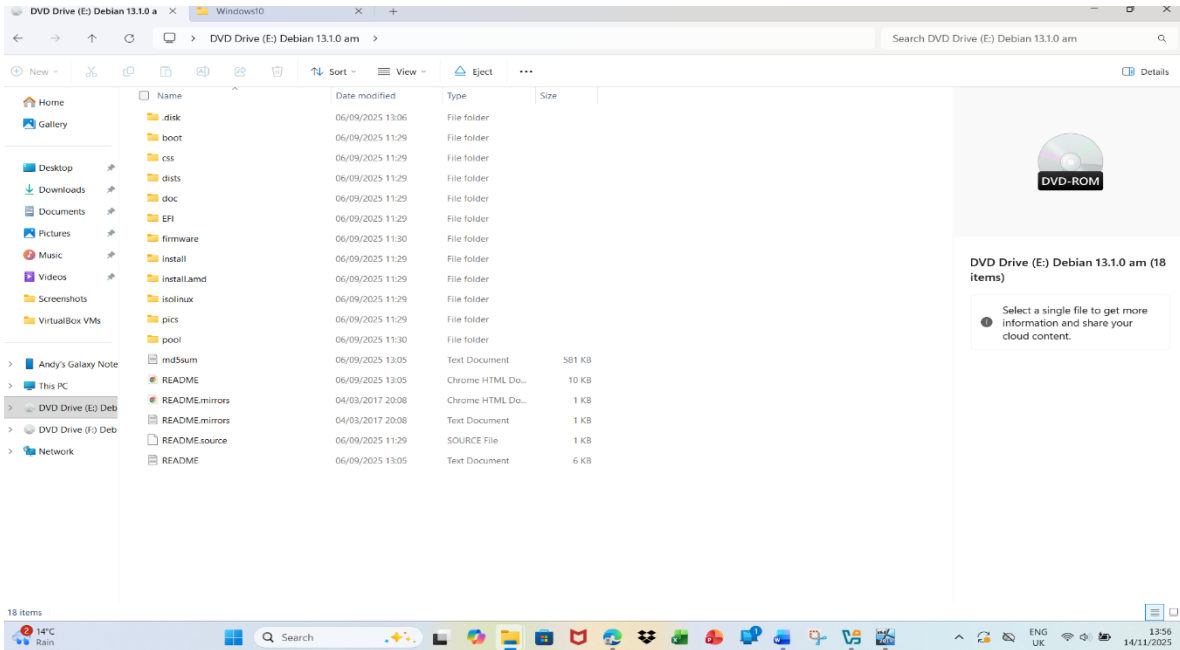
Installation of Windows Client

Downloading Windows client

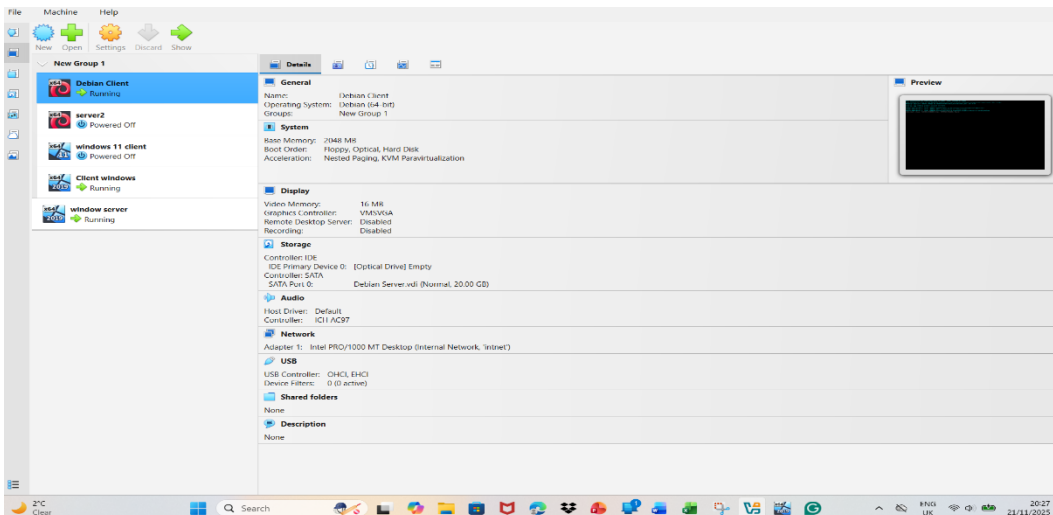


Installation of Debian Client

Downloading of Debian Client



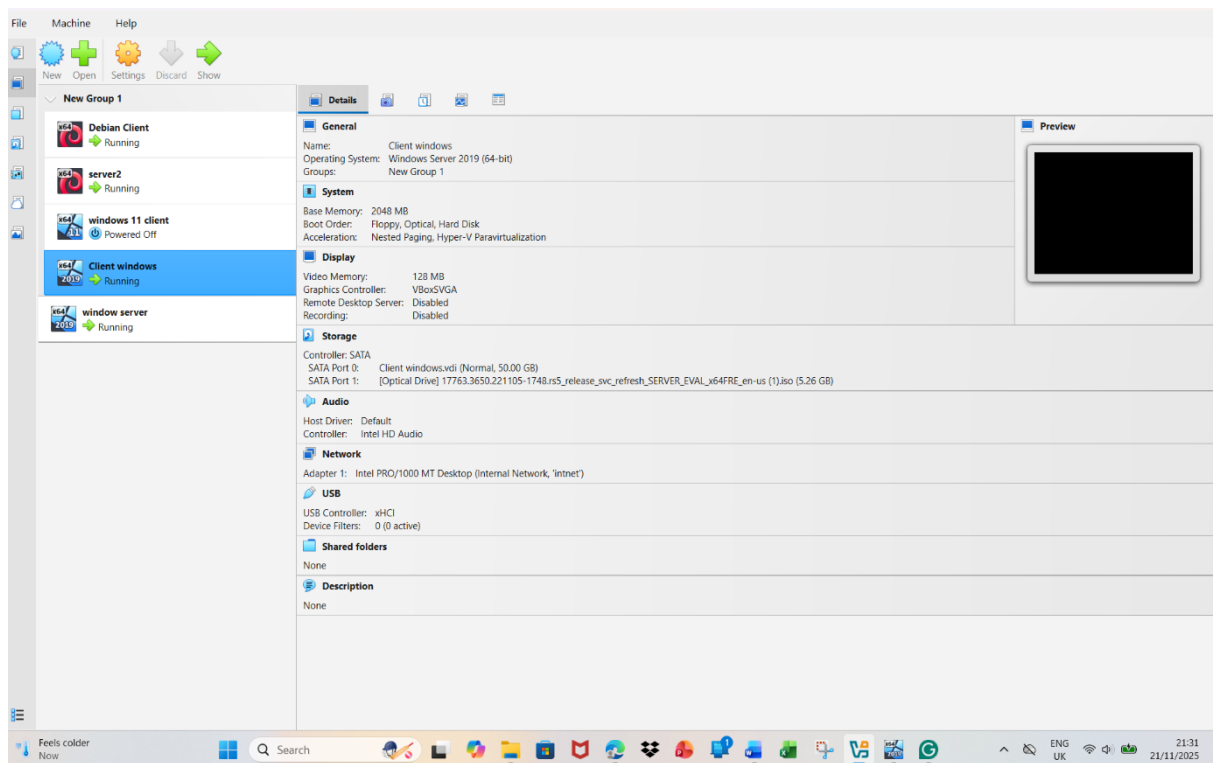
Successful installation of the Debian client



All the machines

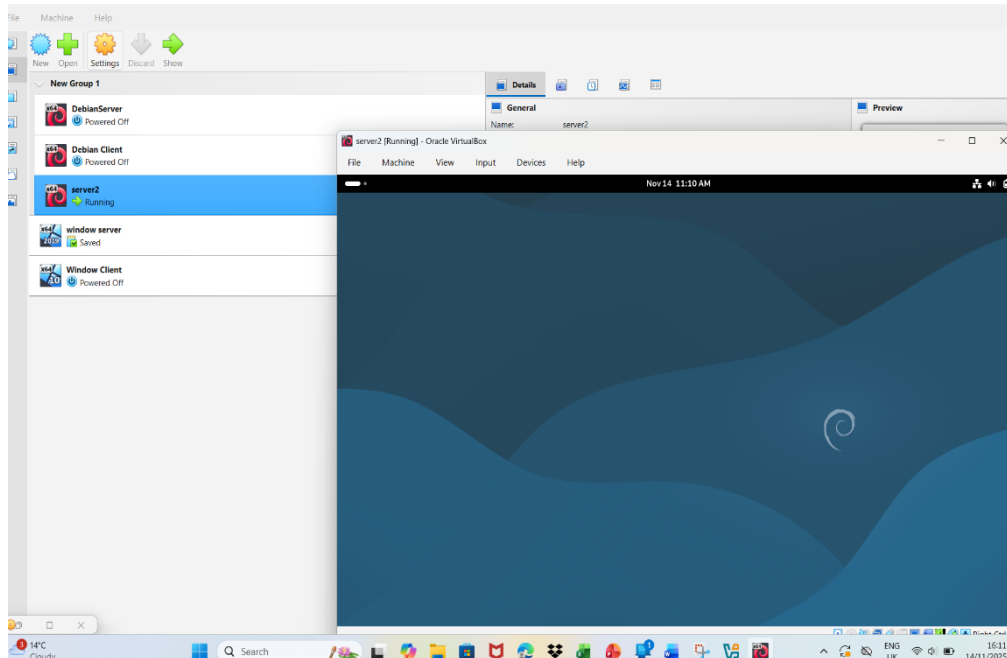
Successful installation of all four machines, up and running, namely

- Windows Server
- Windows Client
- Debian Server
- Debian Client

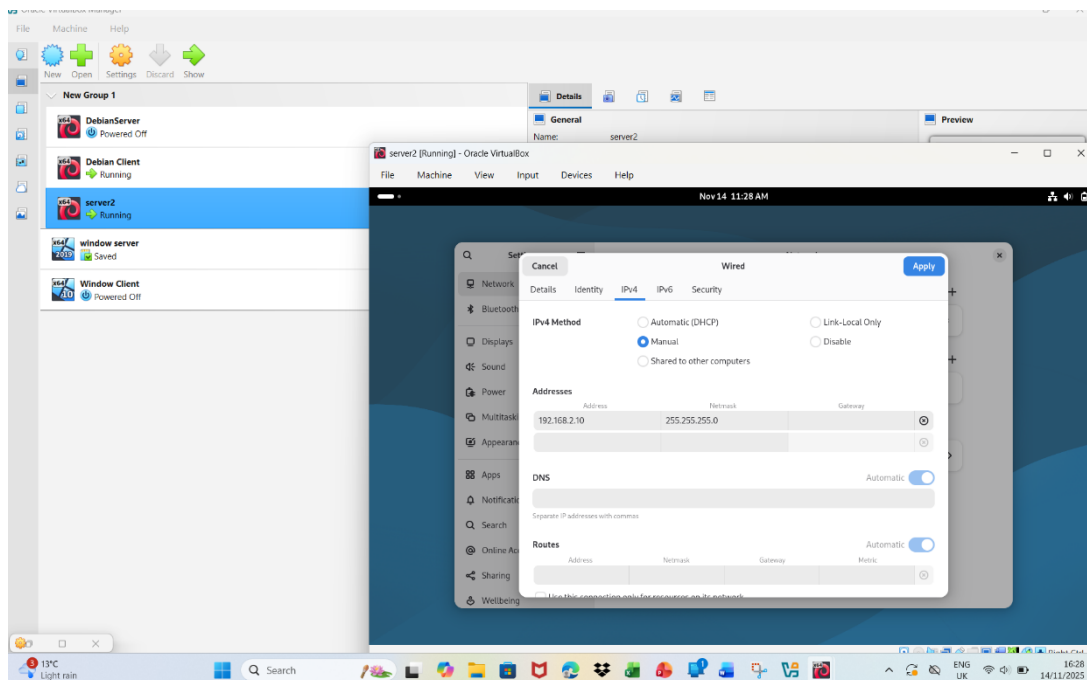


Debian Server2 IP configuration

Step one: Configuring IP Address for the Debian server2

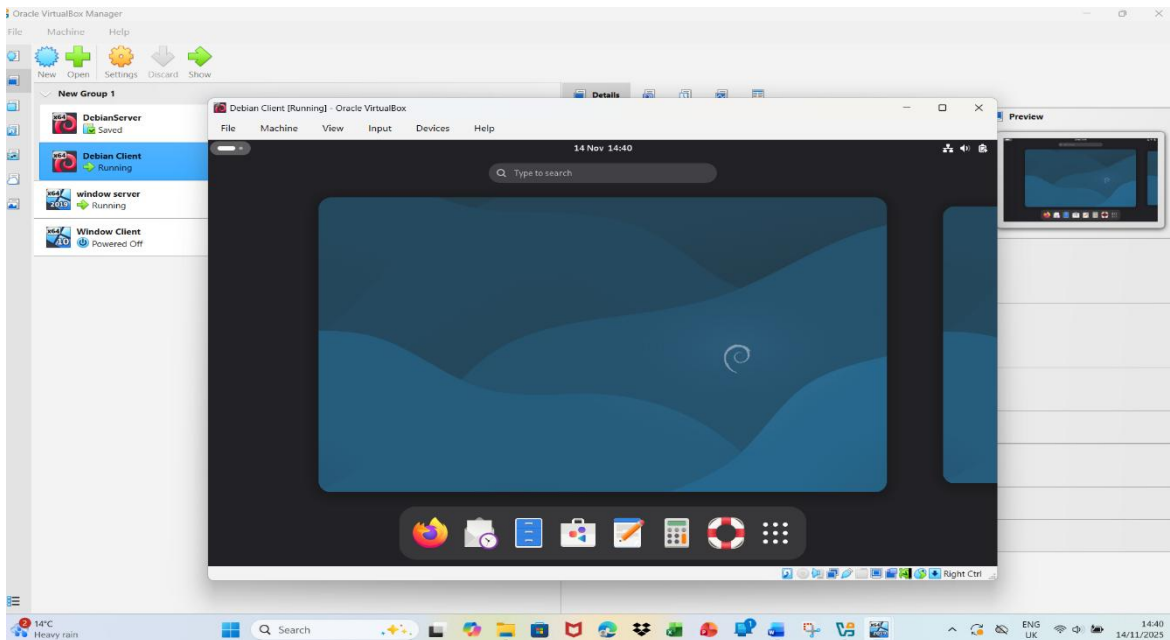


Step two: Configuring IP Address for the Debian Server2 IP showing

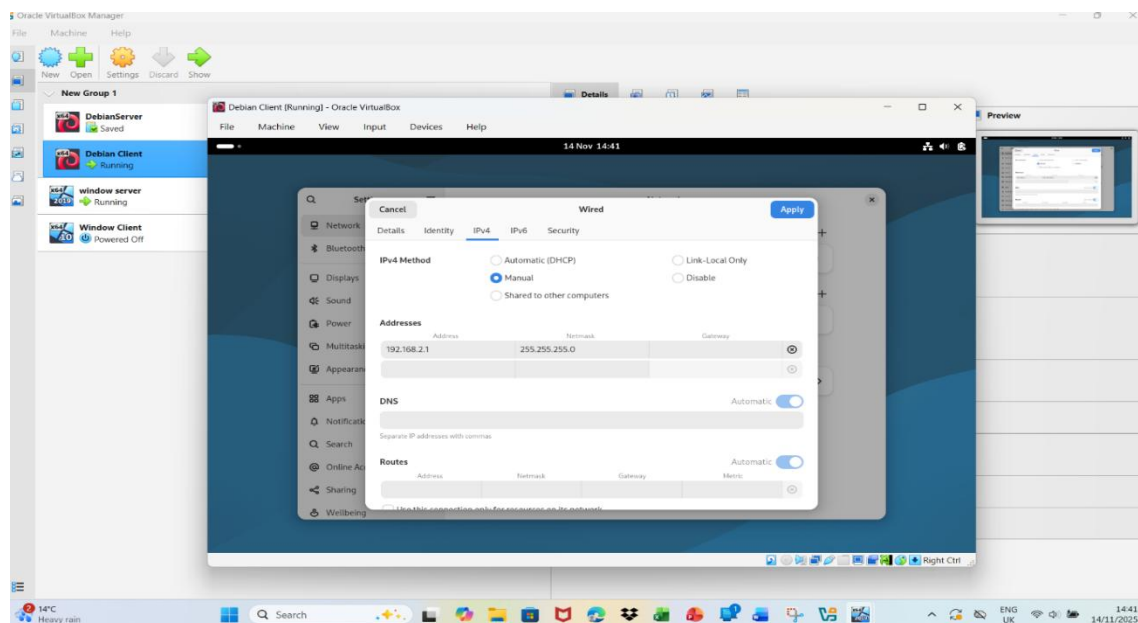


Debian Client IP Configuration

Step one: Configuring IP Address for the Debian Client

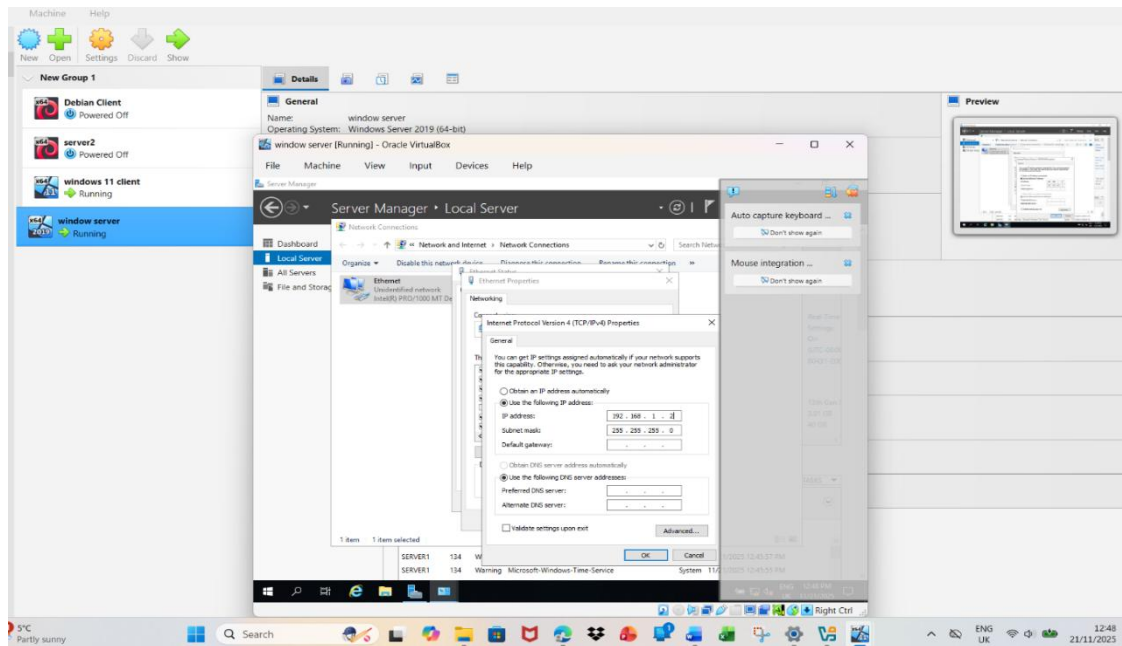


Step two: Configuring IP Address for the Debian Client IP showing

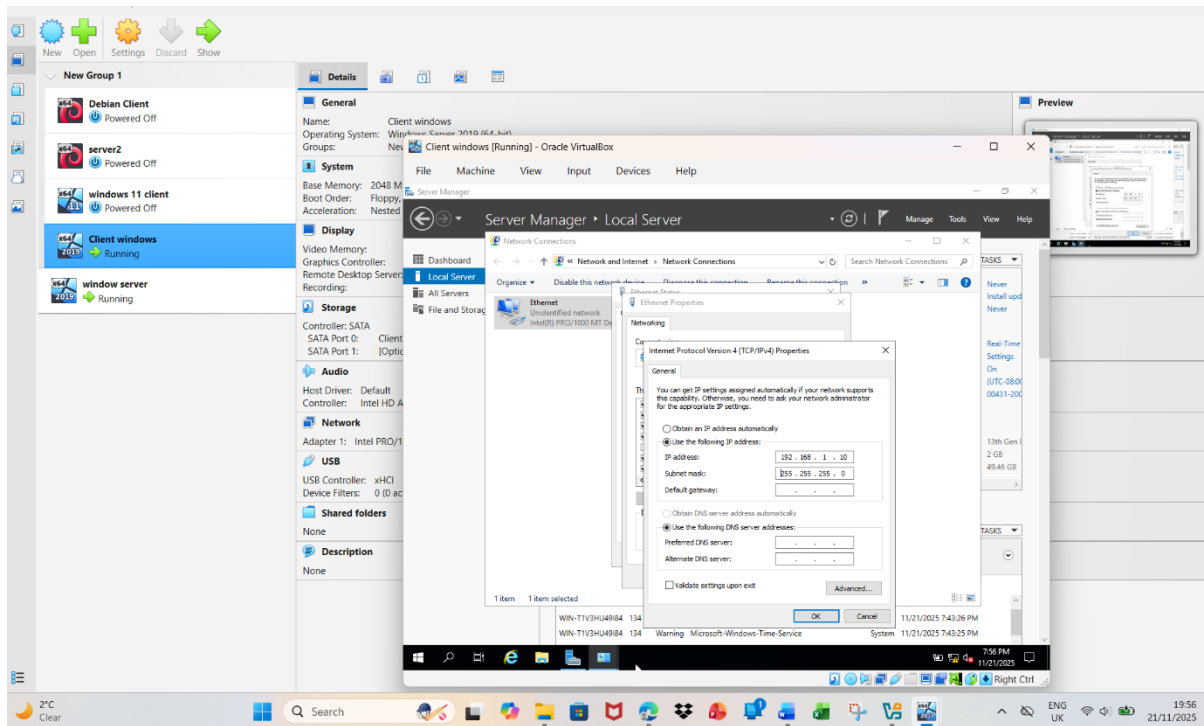


Windows server IP configuration

Configuration of Windows Server IP Address and assigning of IP address

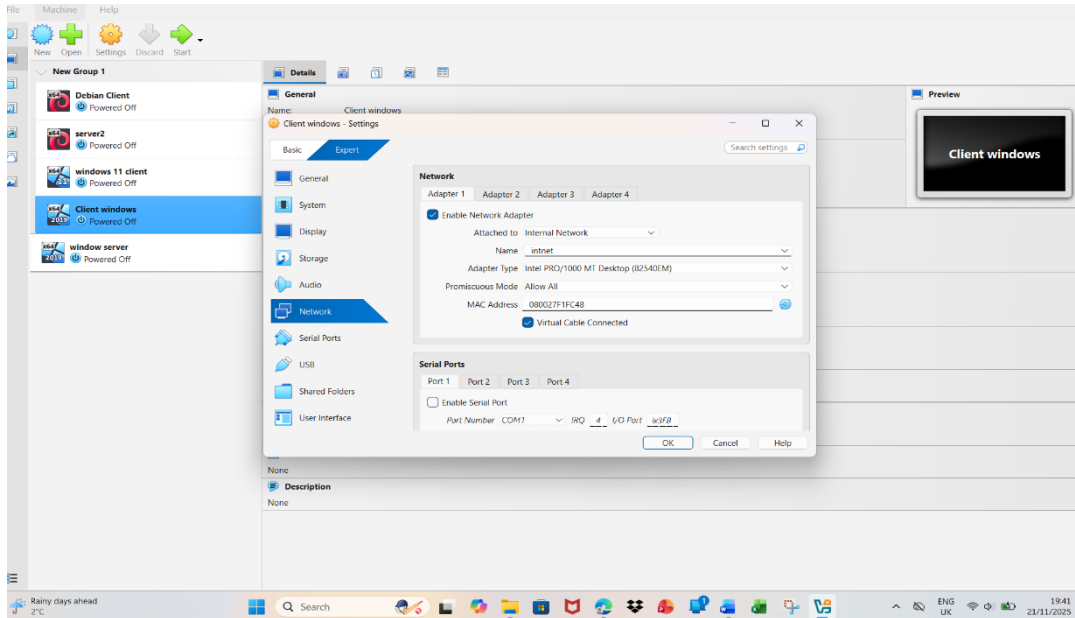


Configuration of Client Windows IP Address and assigning of IP address

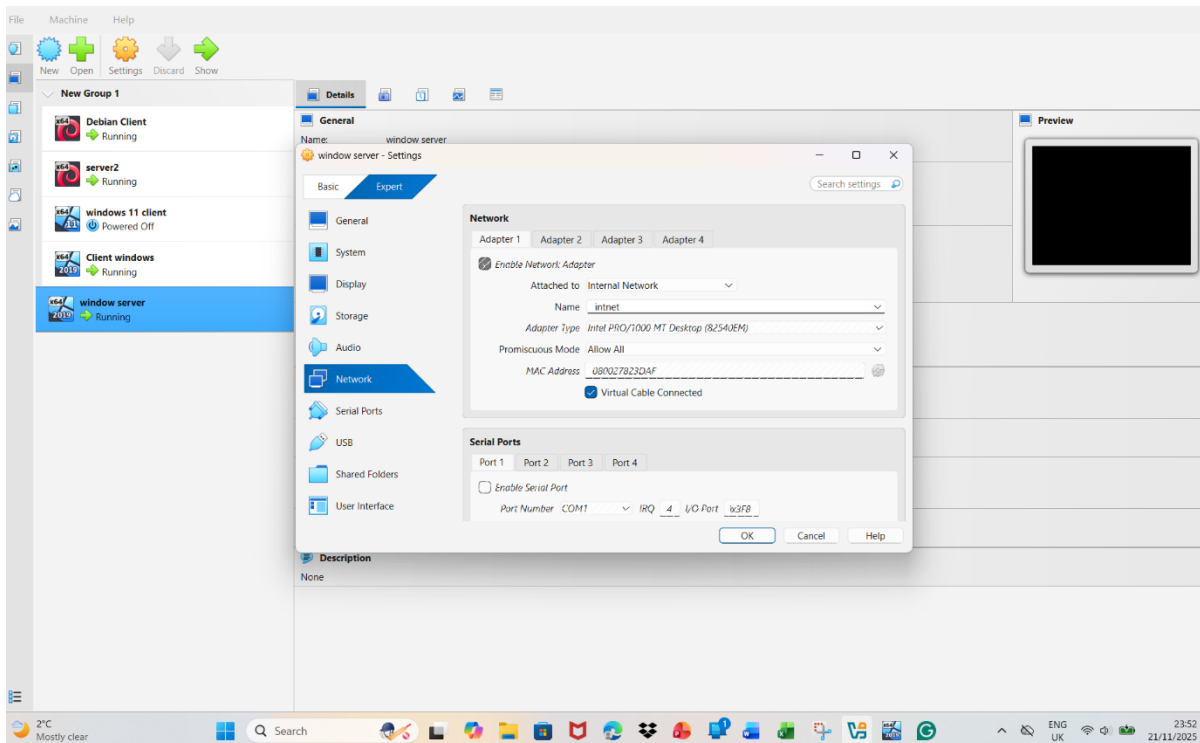


Creation of Network with NAT Network for Windows

Window client Nat connection

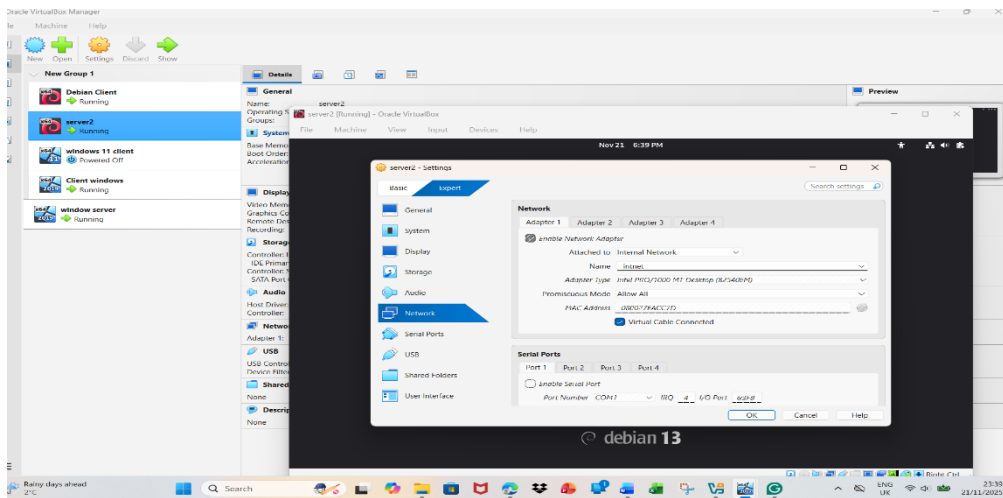


Windows Server NAT connection

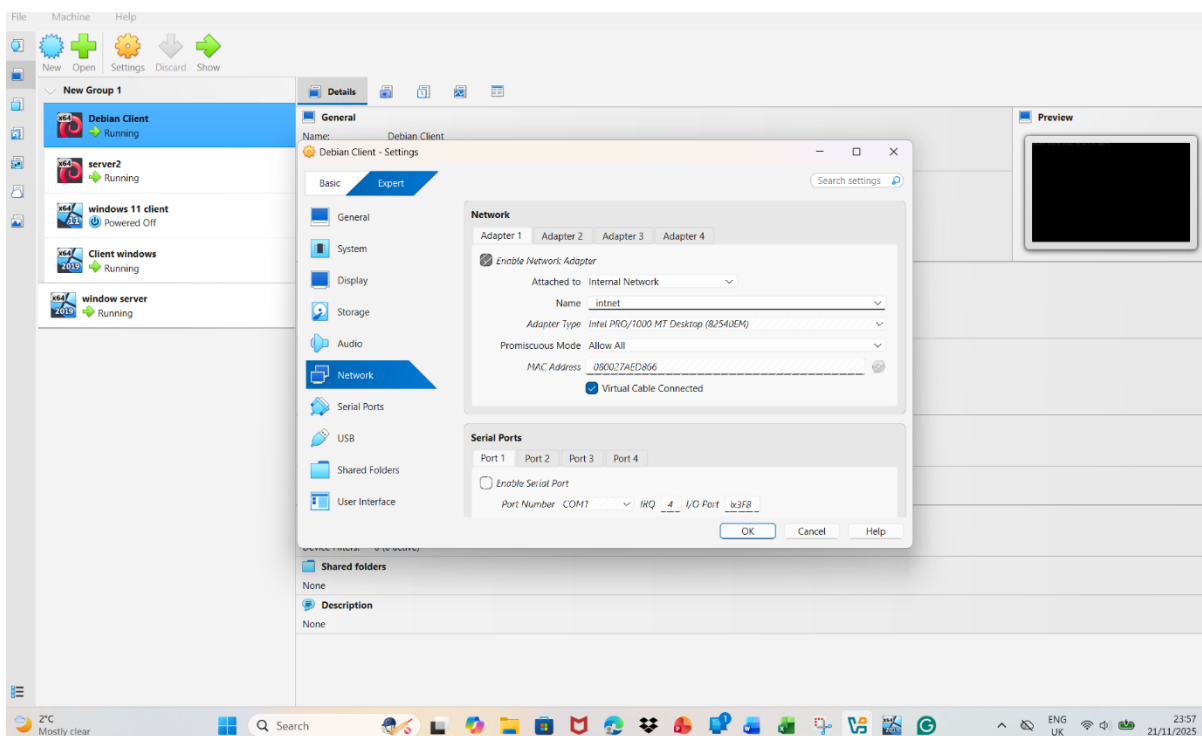


Creation of Network with NAT Network for Debian

Debian Server NAT connection

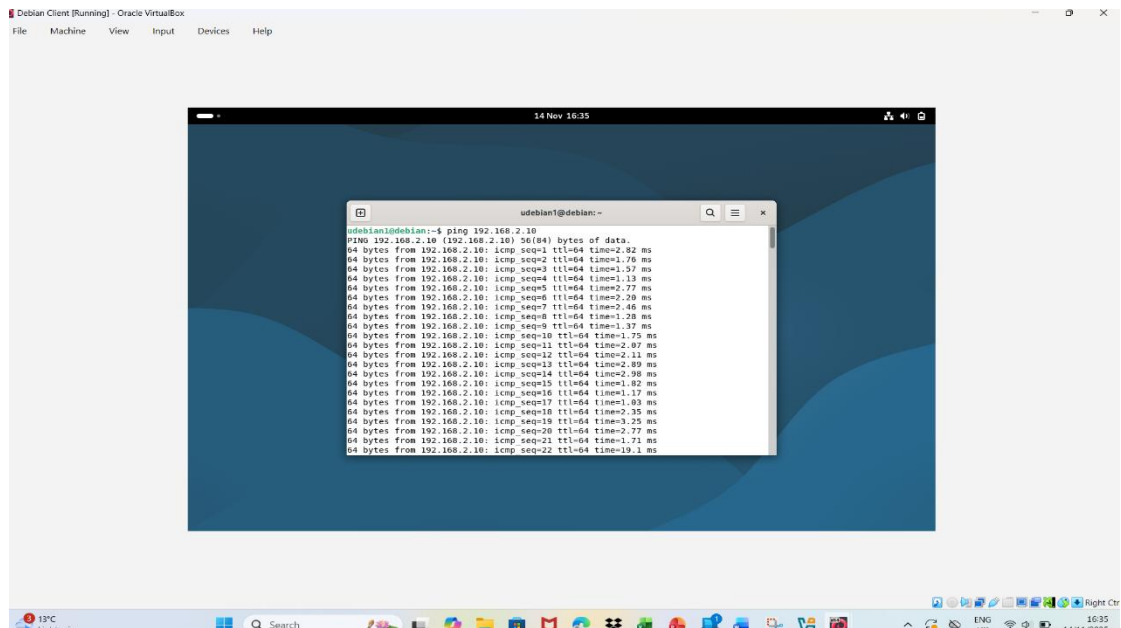


Debian Client NAT connection



Ping connectivity for Debian

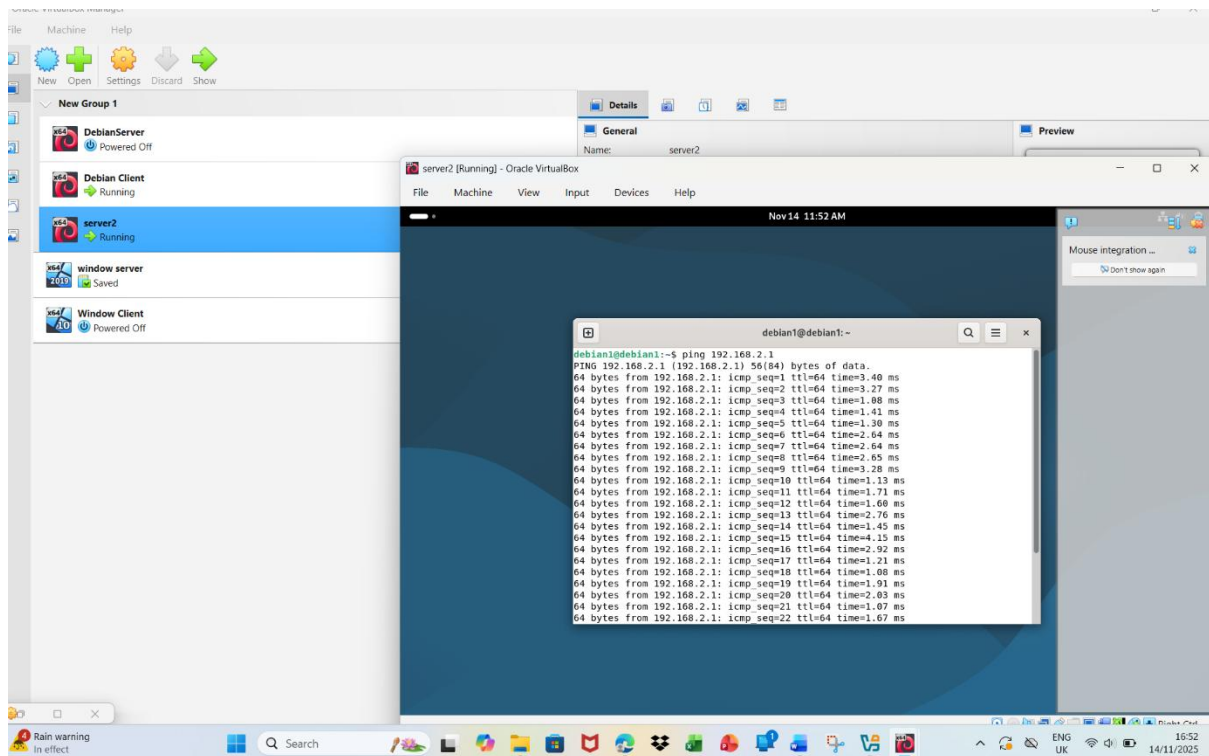
To establish a connection, I have used ping command to ping Debian Server from Debian client, pinging Debian server2 with it IP Address 192.168.2.10



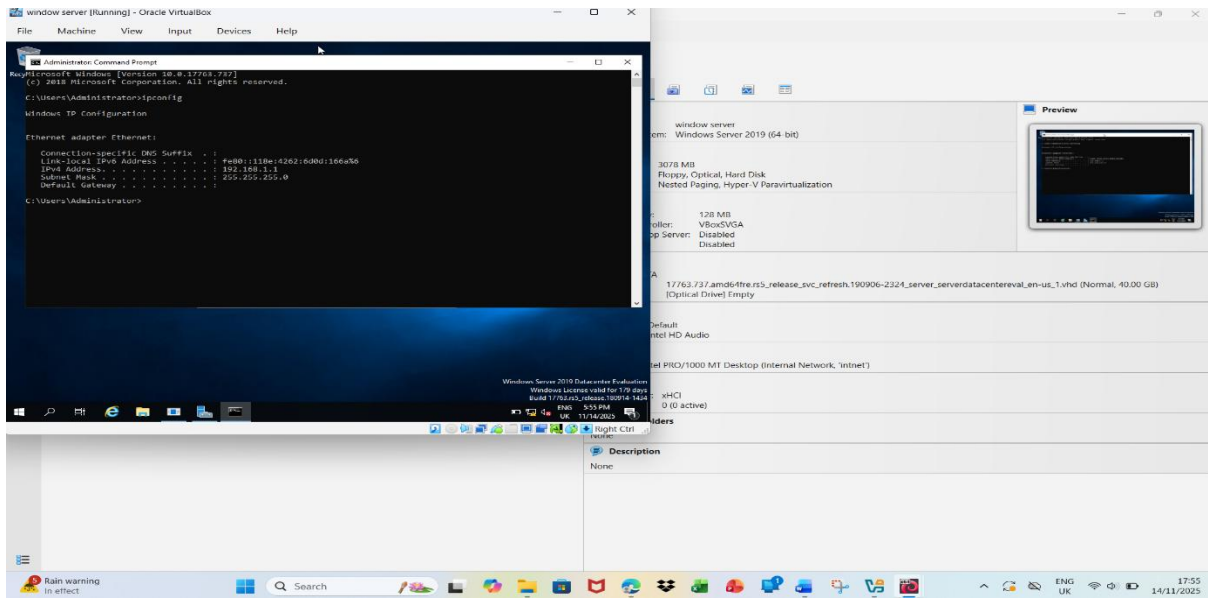
The screenshot shows a terminal window titled 'udebian1@debian: ~' with the following output:

```
udebian1@debian:~$ ping 192.168.2.10
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data:
64 bytes from 192.168.2.10: icmp_seq=1 ttl=64 time=2.82 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=64 time=1.76 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=64 time=1.57 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=64 time=1.13 ms
64 bytes from 192.168.2.10: icmp_seq=5 ttl=64 time=2.77 ms
64 bytes from 192.168.2.10: icmp_seq=6 ttl=64 time=2.20 ms
64 bytes from 192.168.2.10: icmp_seq=7 ttl=64 time=2.46 ms
64 bytes from 192.168.2.10: icmp_seq=8 ttl=64 time=1.28 ms
64 bytes from 192.168.2.10: icmp_seq=9 ttl=64 time=1.37 ms
64 bytes from 192.168.2.10: icmp_seq=10 ttl=64 time=1.75 ms
64 bytes from 192.168.2.10: icmp_seq=11 ttl=64 time=2.07 ms
64 bytes from 192.168.2.10: icmp_seq=12 ttl=64 time=2.11 ms
64 bytes from 192.168.2.10: icmp_seq=13 ttl=64 time=2.89 ms
64 bytes from 192.168.2.10: icmp_seq=14 ttl=64 time=2.98 ms
64 bytes from 192.168.2.10: icmp_seq=15 ttl=64 time=1.82 ms
64 bytes from 192.168.2.10: icmp_seq=16 ttl=64 time=1.17 ms
64 bytes from 192.168.2.10: icmp_seq=17 ttl=64 time=1.83 ms
64 bytes from 192.168.2.10: icmp_seq=18 ttl=64 time=2.35 ms
64 bytes from 192.168.2.10: icmp_seq=19 ttl=64 time=3.25 ms
64 bytes from 192.168.2.10: icmp_seq=20 ttl=64 time=2.77 ms
64 bytes from 192.168.2.10: icmp_seq=21 ttl=64 time=1.71 ms
64 bytes from 192.168.2.10: icmp_seq=22 ttl=64 time=19.1 ms
```

In order to establish a connection, I have used ping command to ping Debian client from Debian Server pinging Debian Client with its IP Address 192.168.2.1

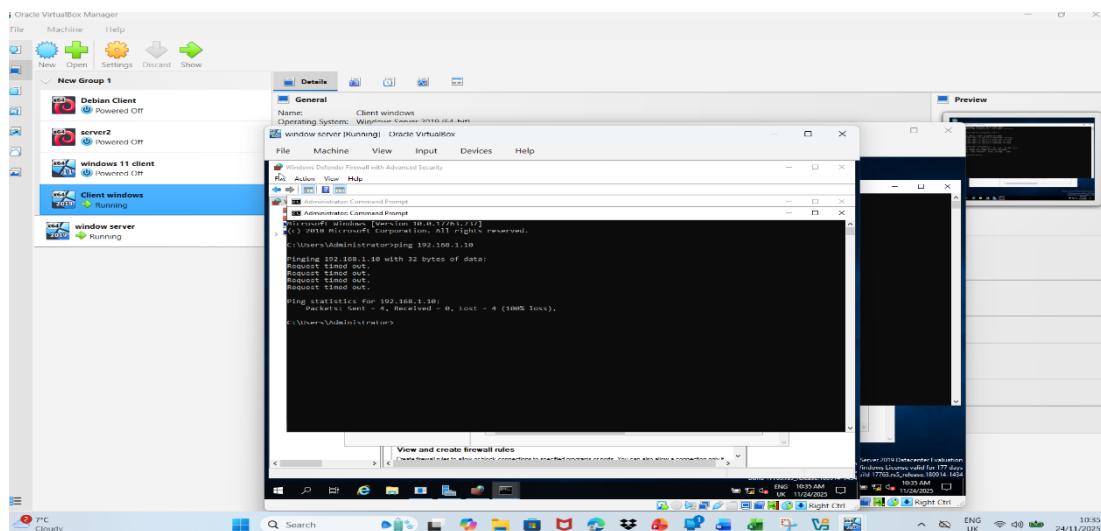
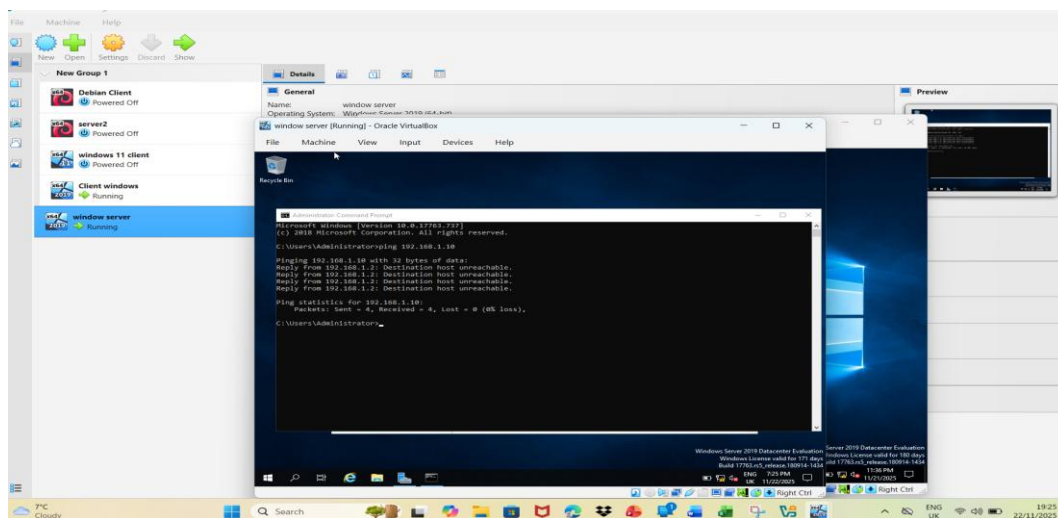


Windows Server IP Configuration using ipconfig command to confirm it



Unsuccessful Ping between Windows Server and Windows Client

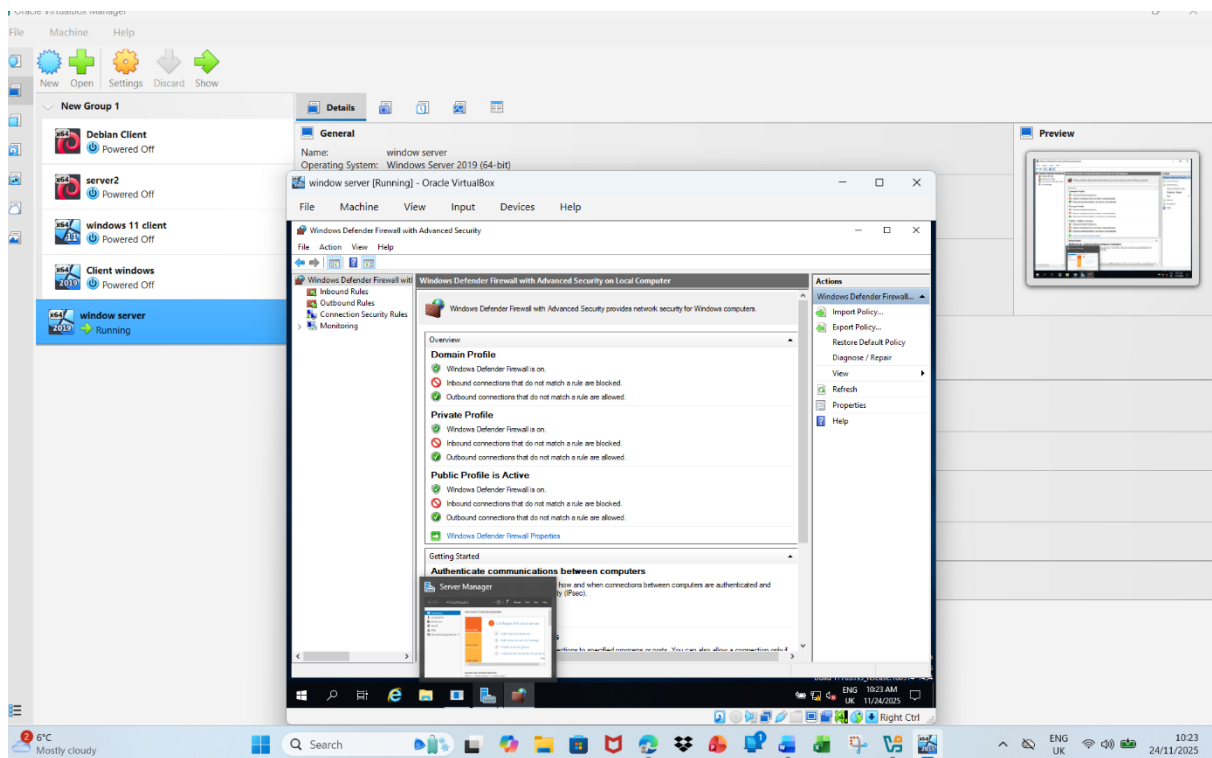
Evidence of unsuccessful ping from server to Client and Client to Server because the firewall is on, and new rules have not been created



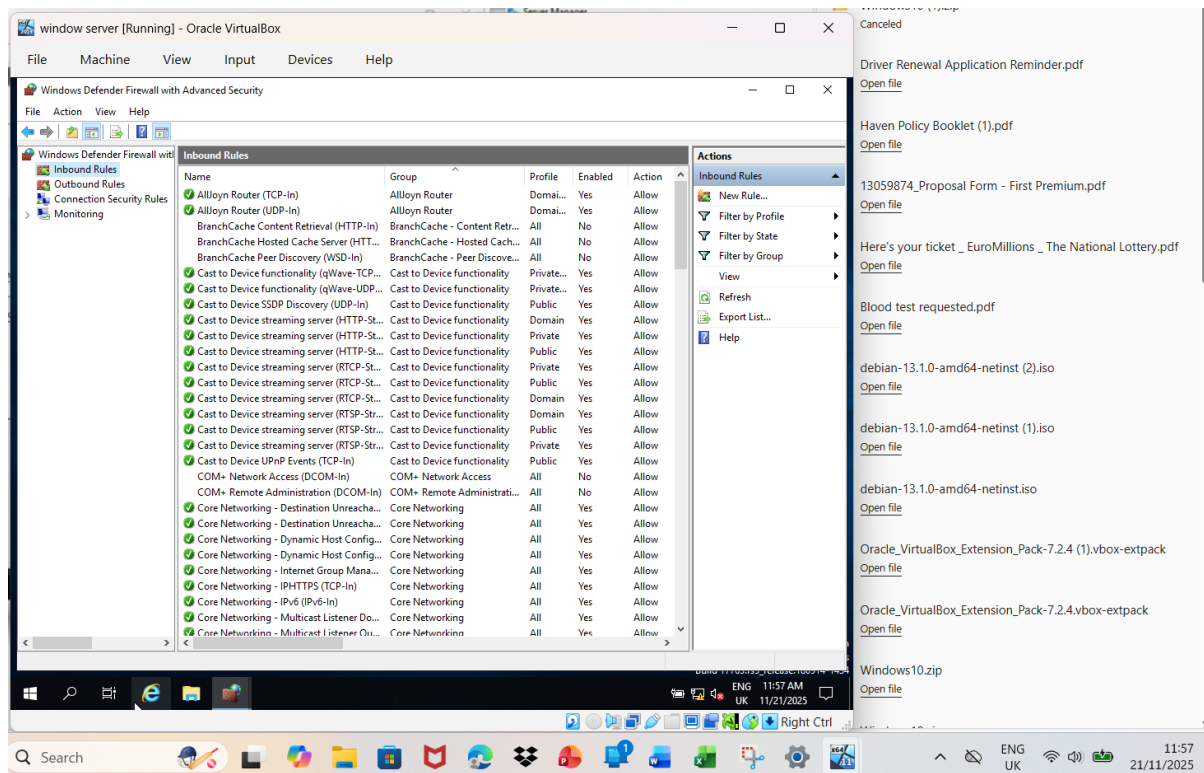
Windows Server configuration: the new rule to enable the ICMP protocol to enable ping testing while Firewall is on

The following screenshots are the step by steps on how I was able to configure Windows Server to enable the ping command to function and to ping a Windows client

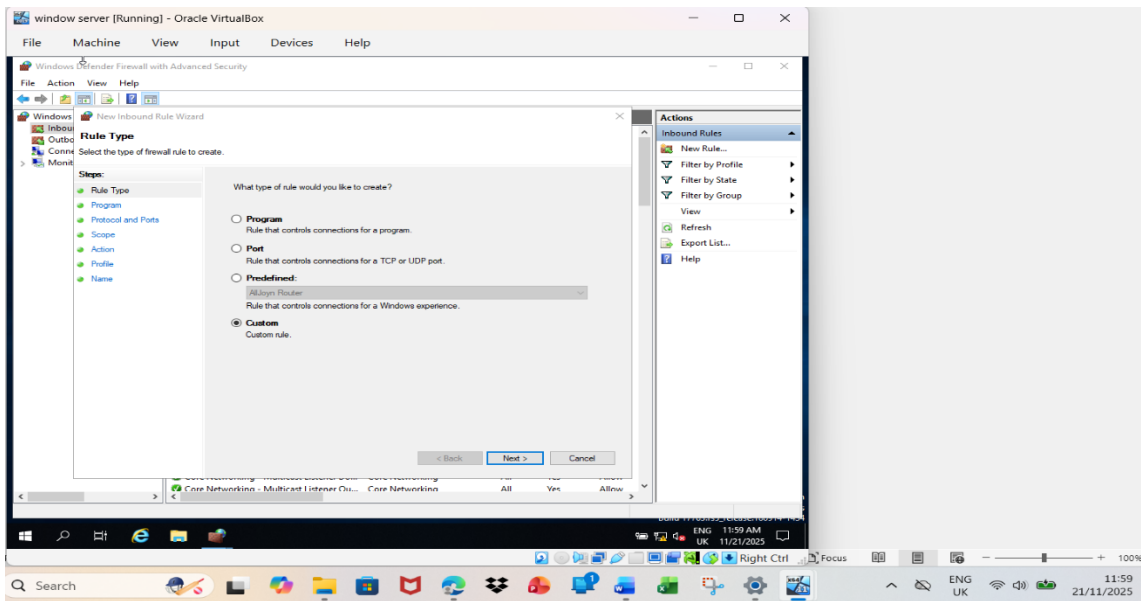
Step one clicks on window defender firewall with advance security



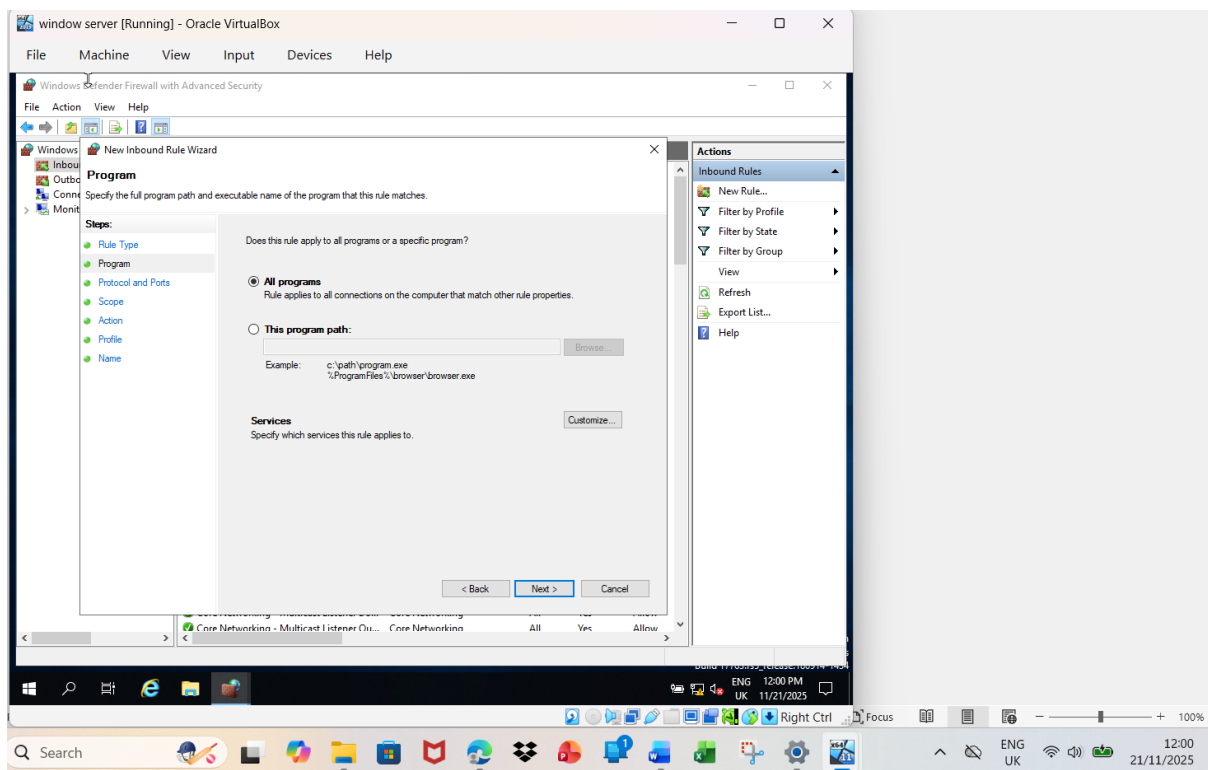
Step two clicks on Inbound rule and on the right side selects New Rule



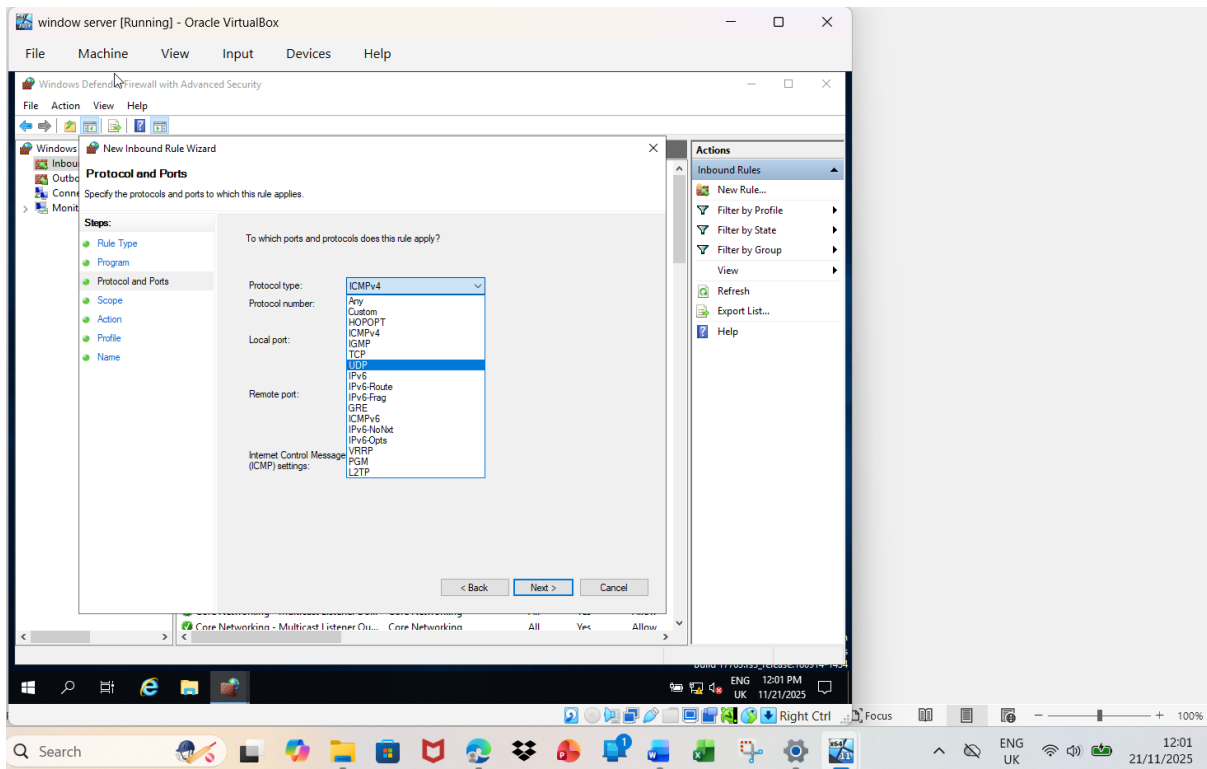
Step three: select Customise rule



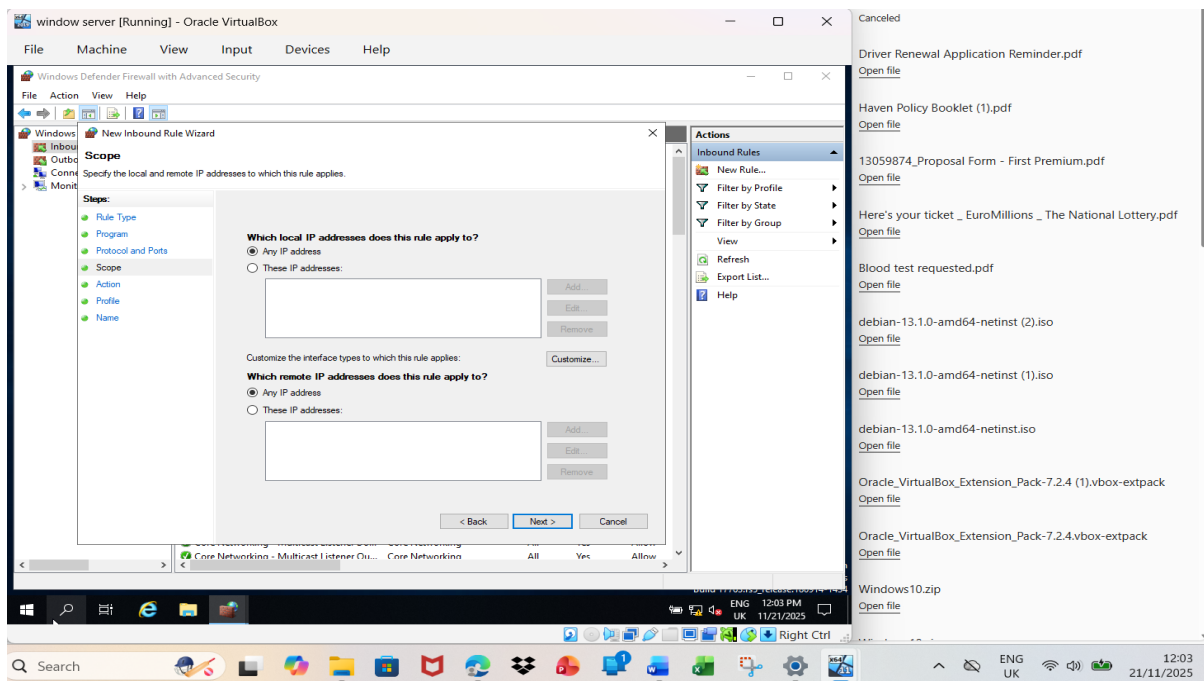
Step four: select All programs



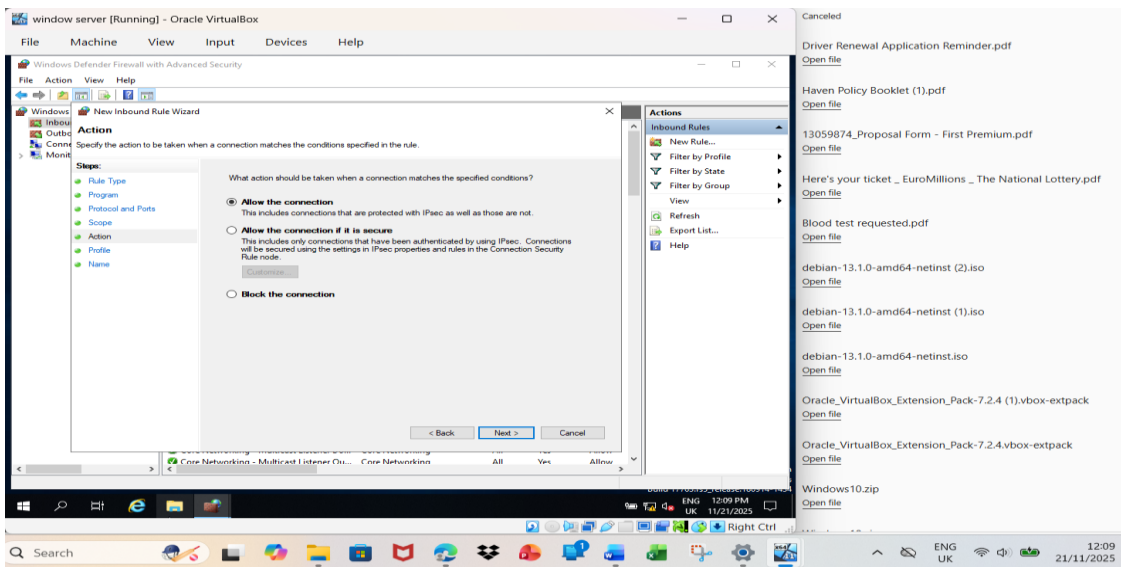
Step Five: specify the protocol, select ICMPv4



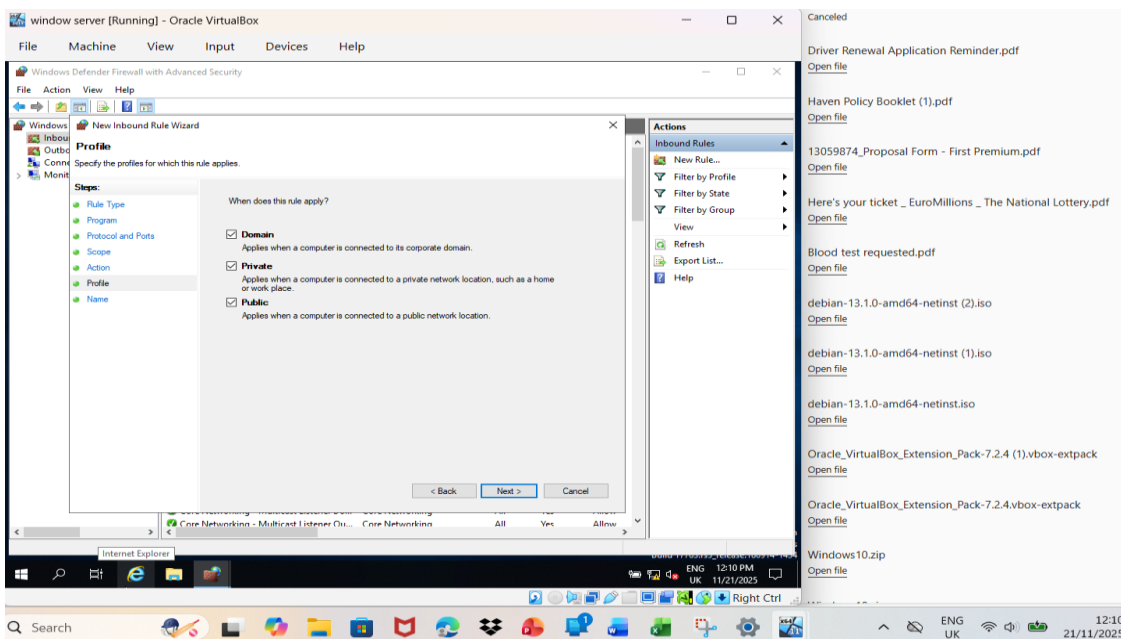
Step Six: Select any IP should be able to ping



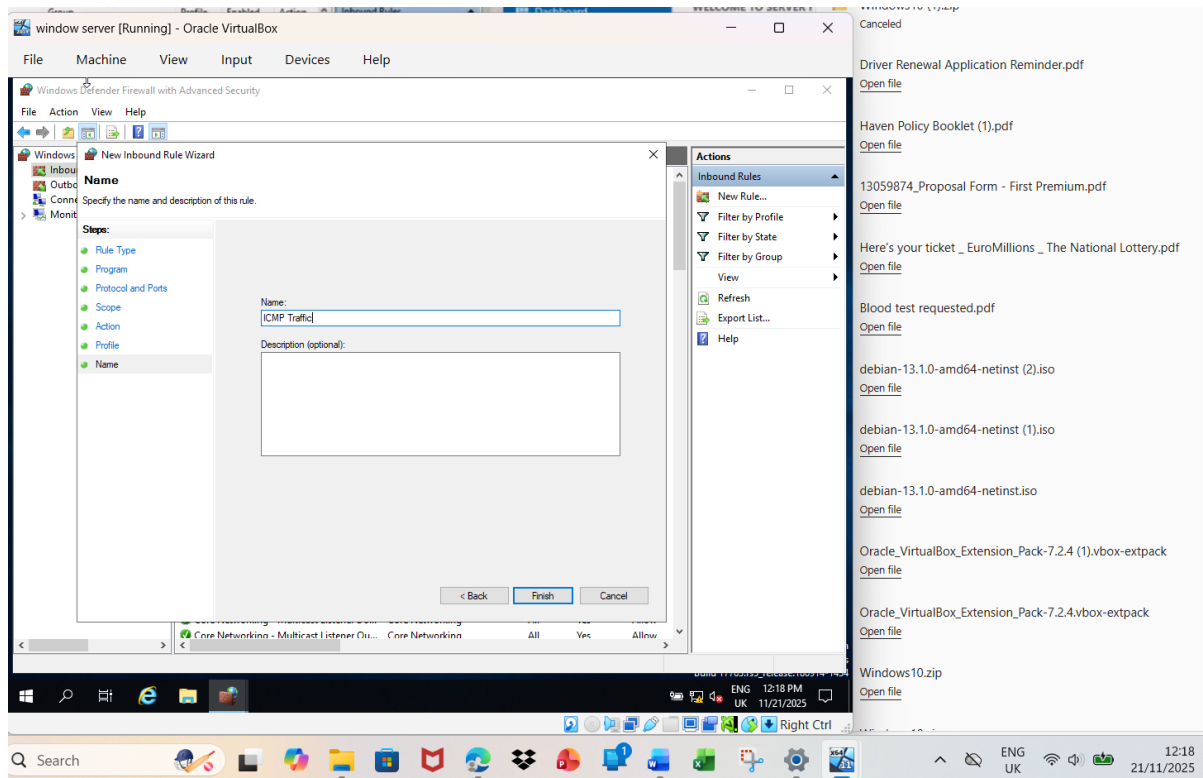
Step Seven clicks allow all connection



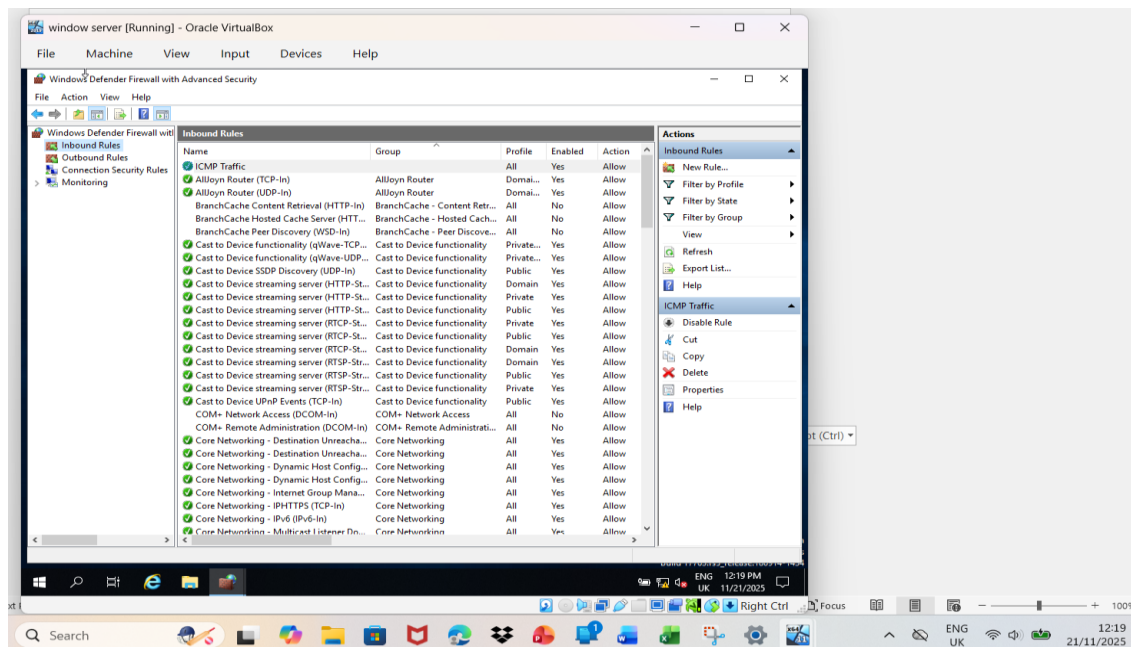
Step Eight: Allow any network to be able to ping



Step Nine: naming the rule I just configured ICMP Traffic

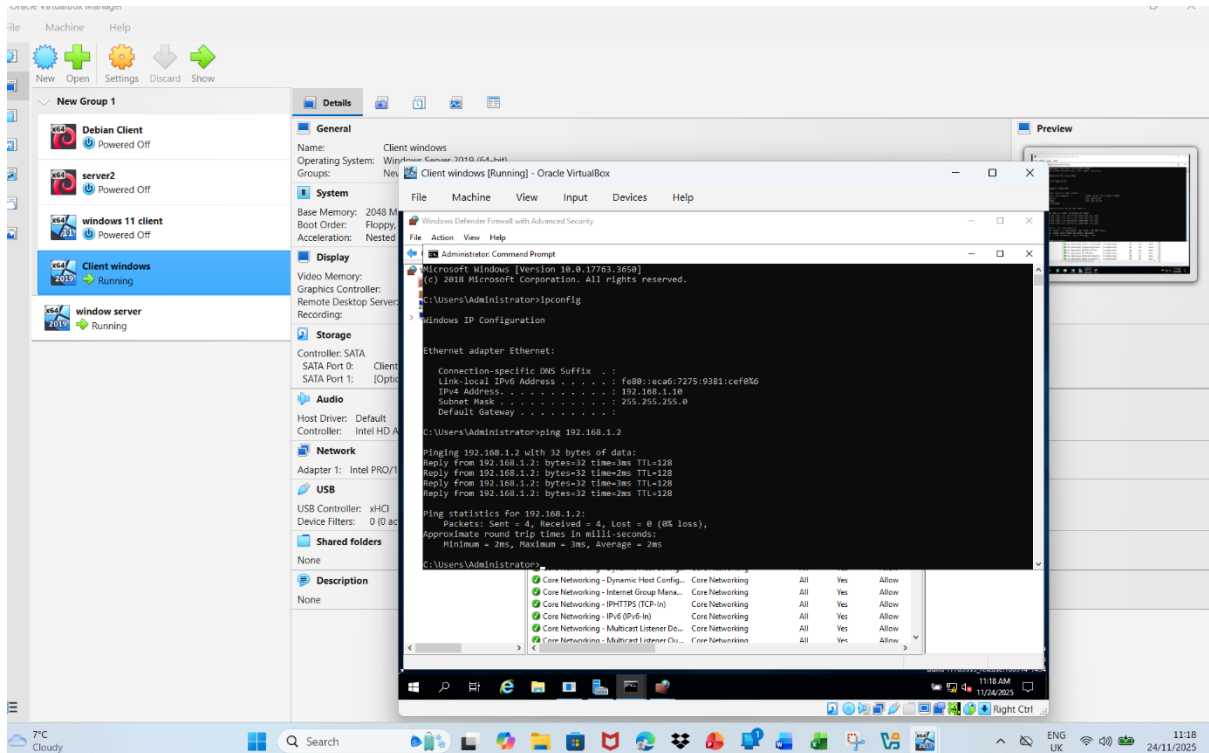


The rule has been set as you can see

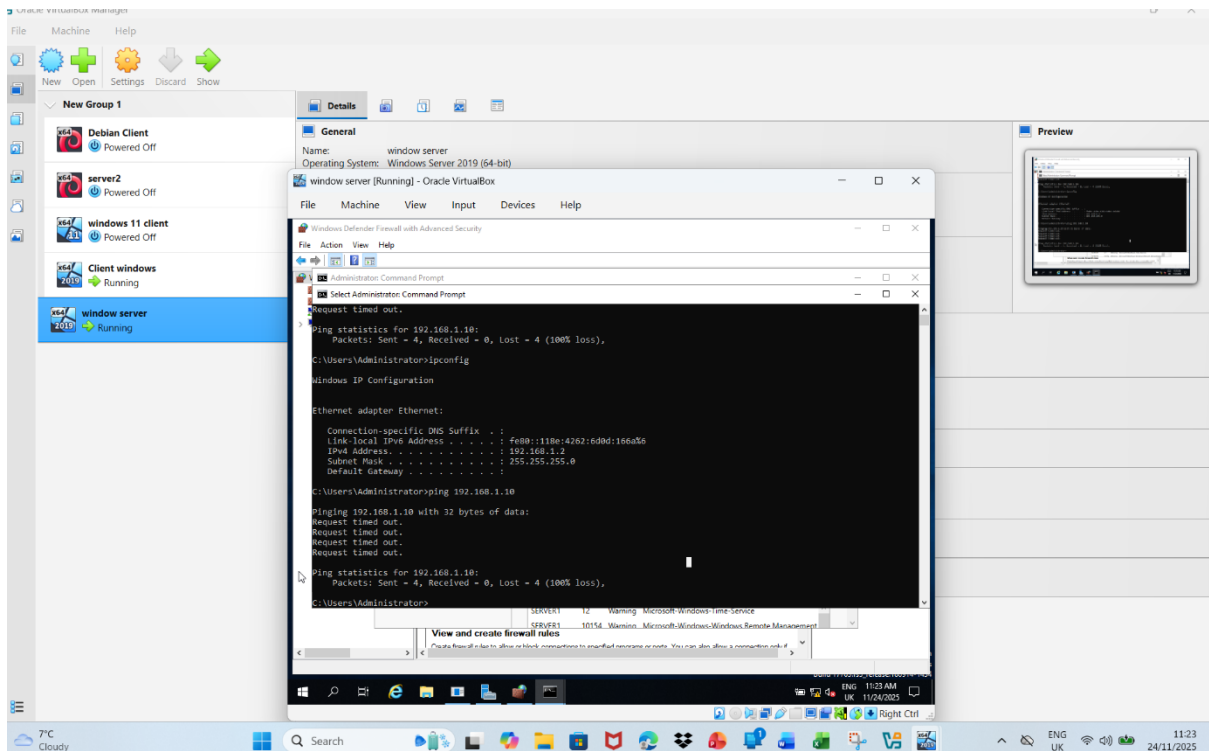


ping demonstration

Ping from the client window to the Server is working after a new rule has been set for Windows Server



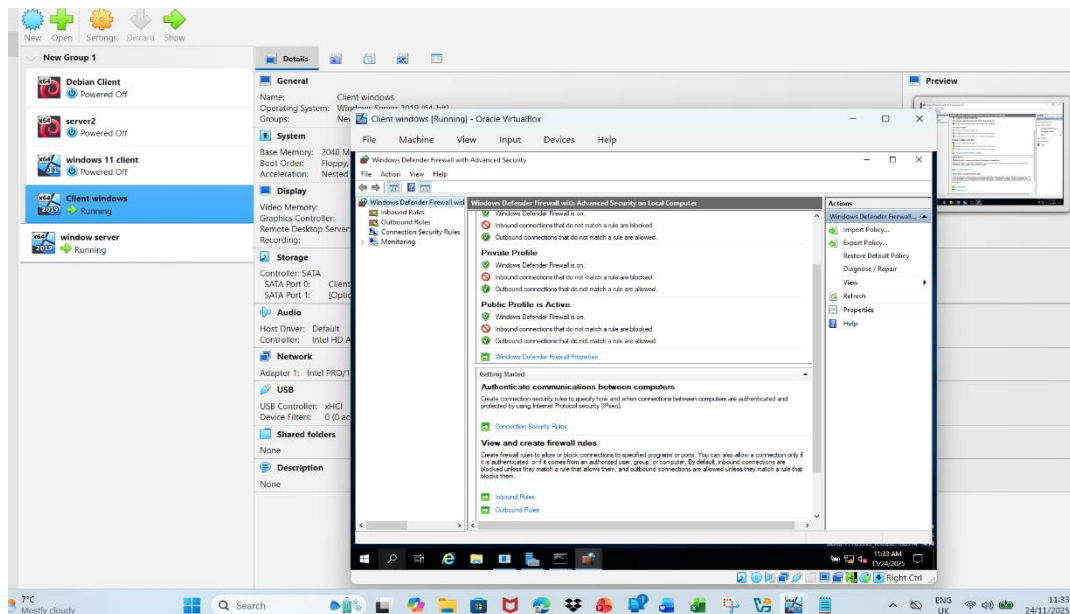
Ping from Windows Server to Windows Client is unsuccessful because new rule has not been enabled.



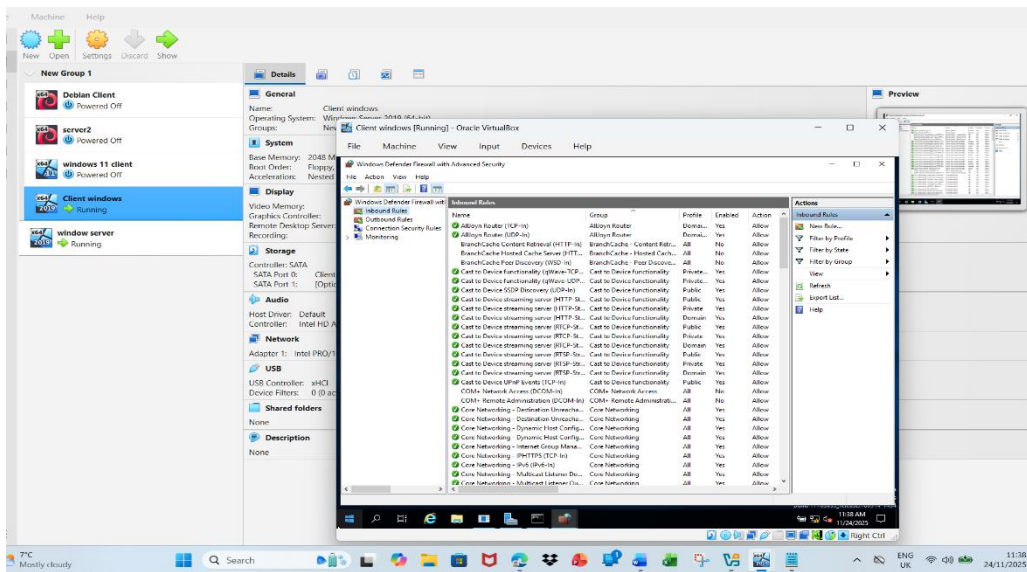
Windows Client configuration setting the new rule to enable the ICMP protocol to enable ping testing while Firewall is on

The following screenshots are the step-by-step instructions on how I was able to configure Windows Client to enable the ping command to function and to ping Windows Server.

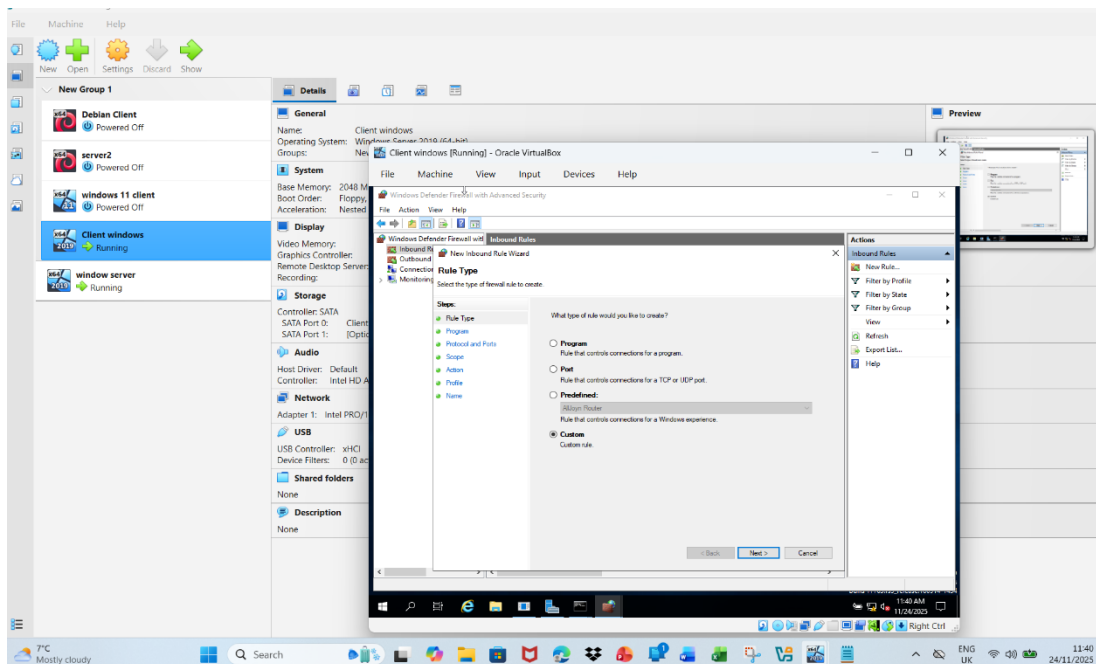
Step one clicks on window defender firewall with advance security



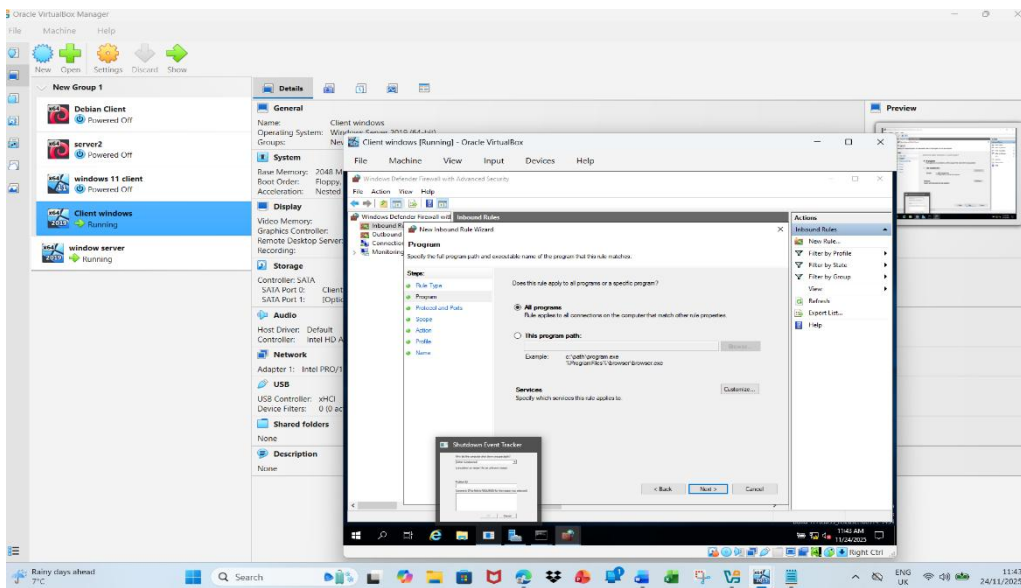
Step two clicks on Inbound rule and on the right side selects New Rule



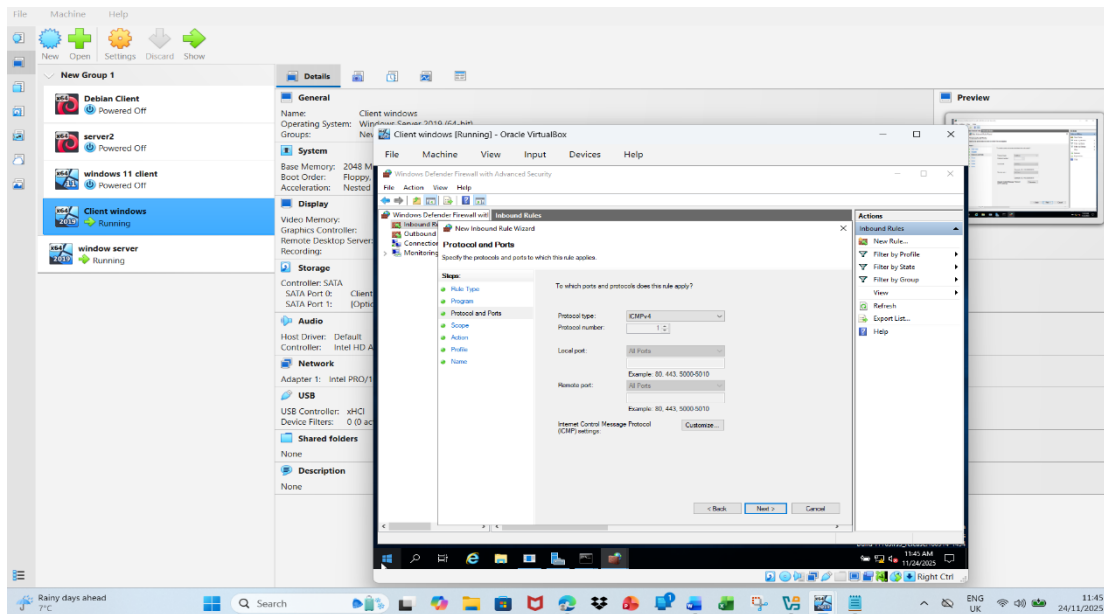
Step three: select Customise rule



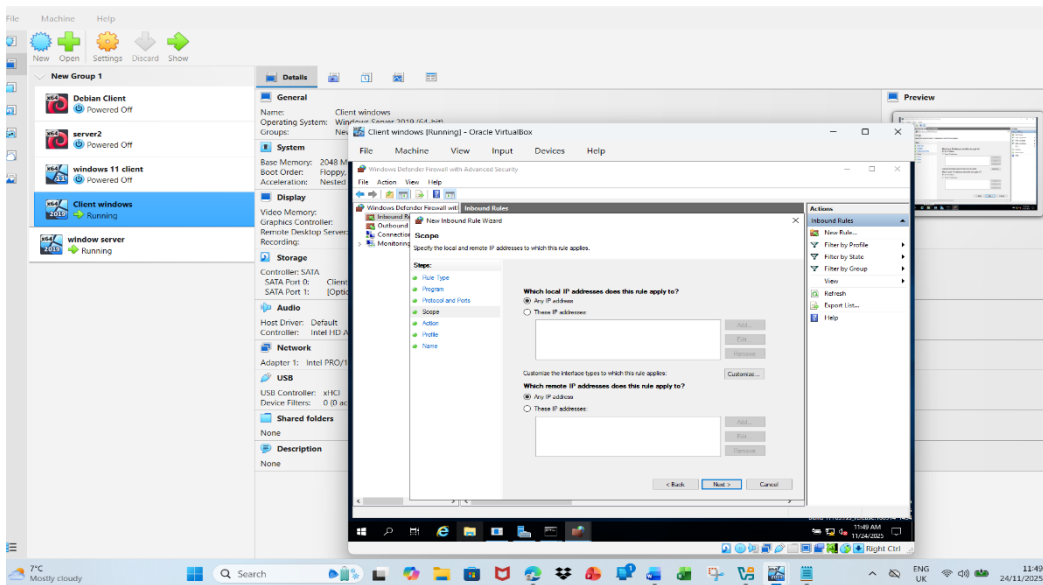
Step four: select All programs



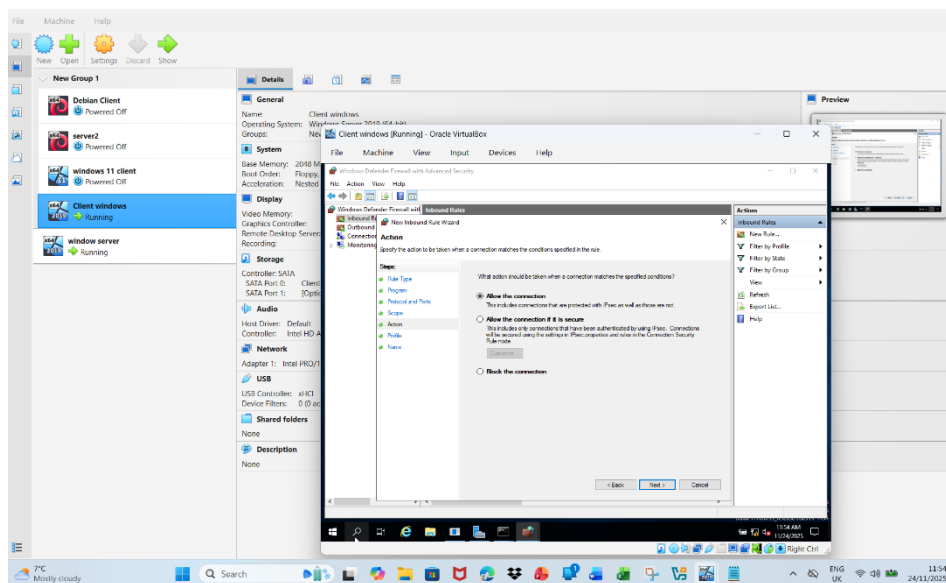
Step Five: specify the protocol, select ICMPv4



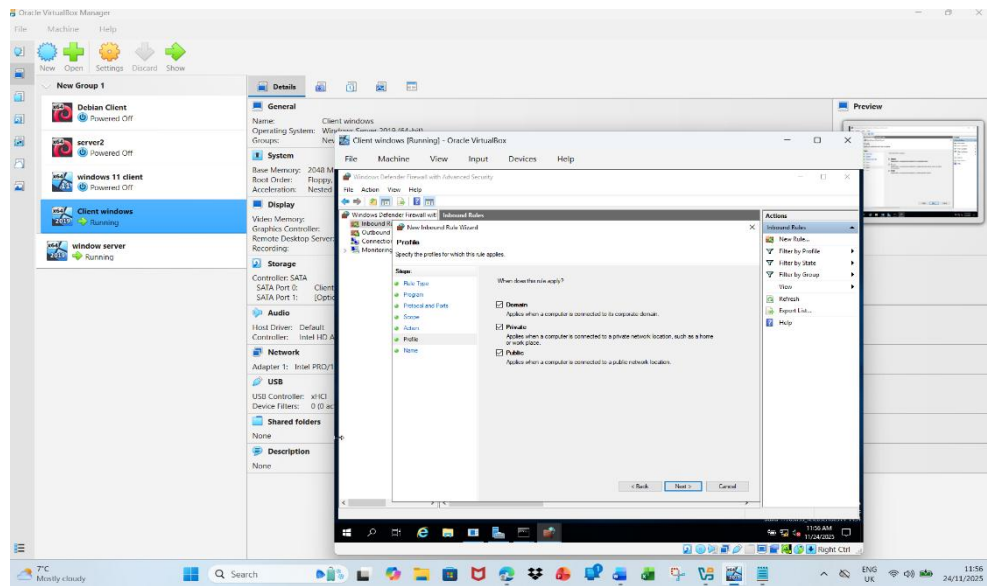
Step Six: Select any IP should be able to ping



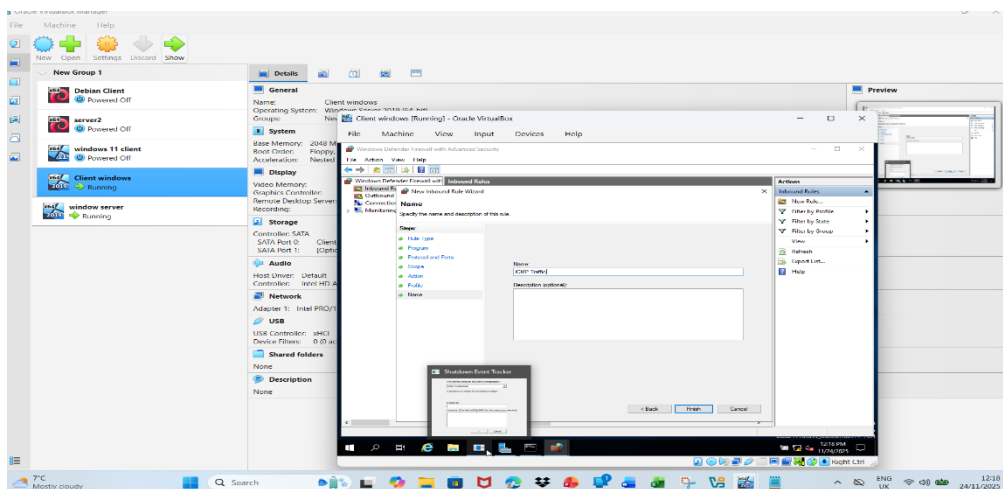
Step Seven clicks allow all connections



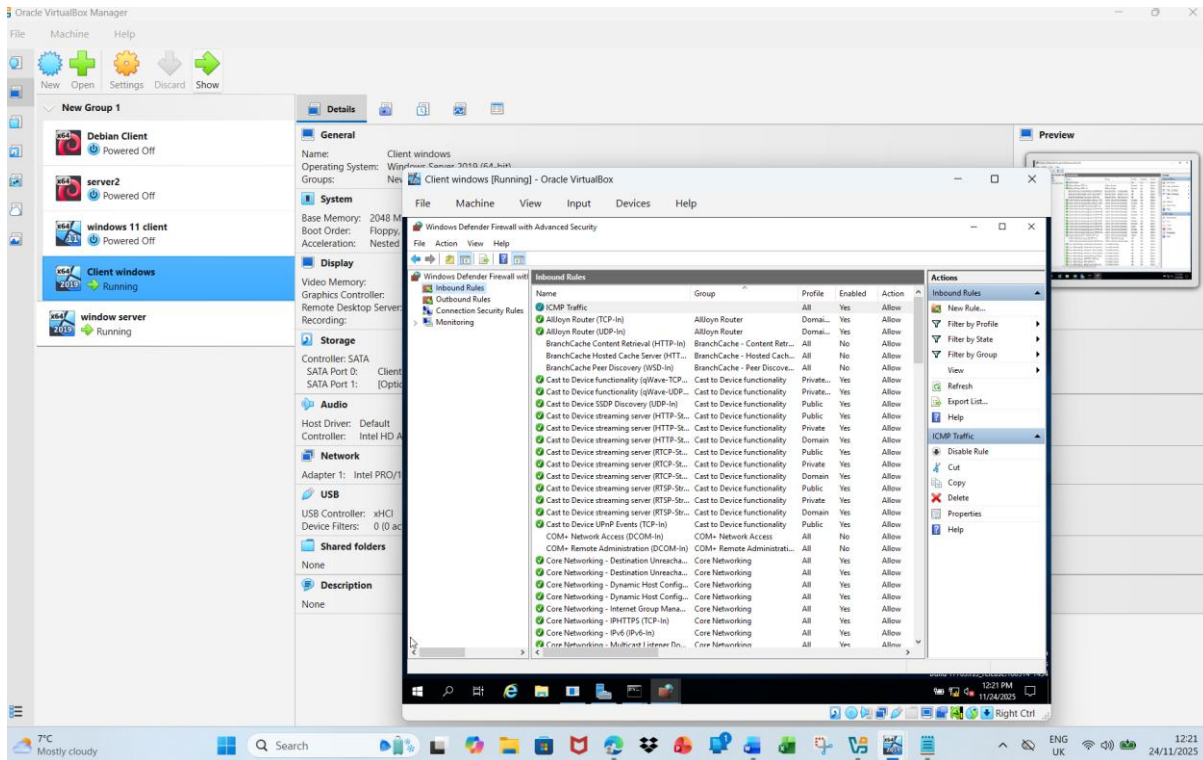
Step Eight: Allow any network to be able to ping



Step Nine: naming the rule I just configured ICMP Traffic

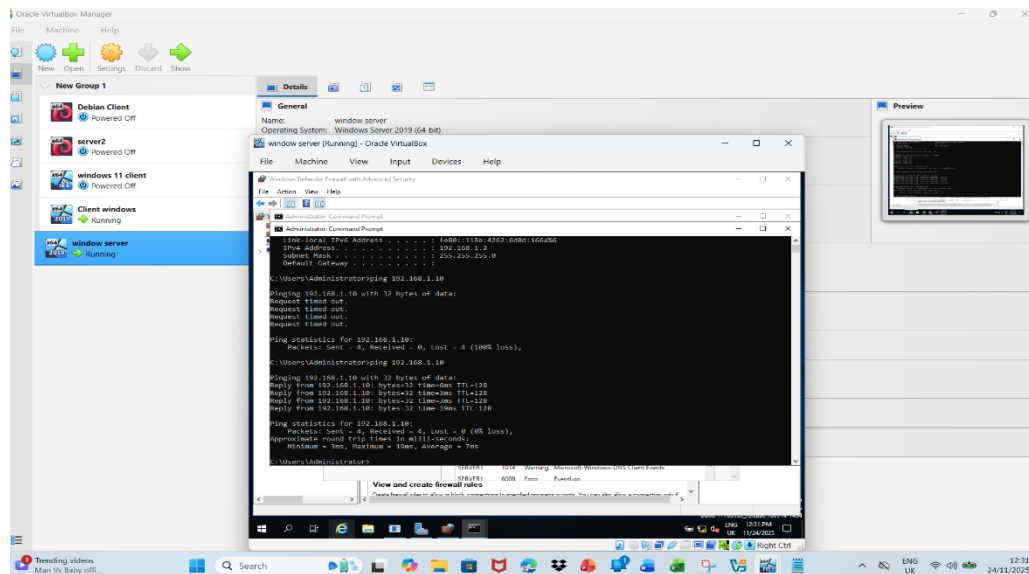


The rule has been set, as you can see

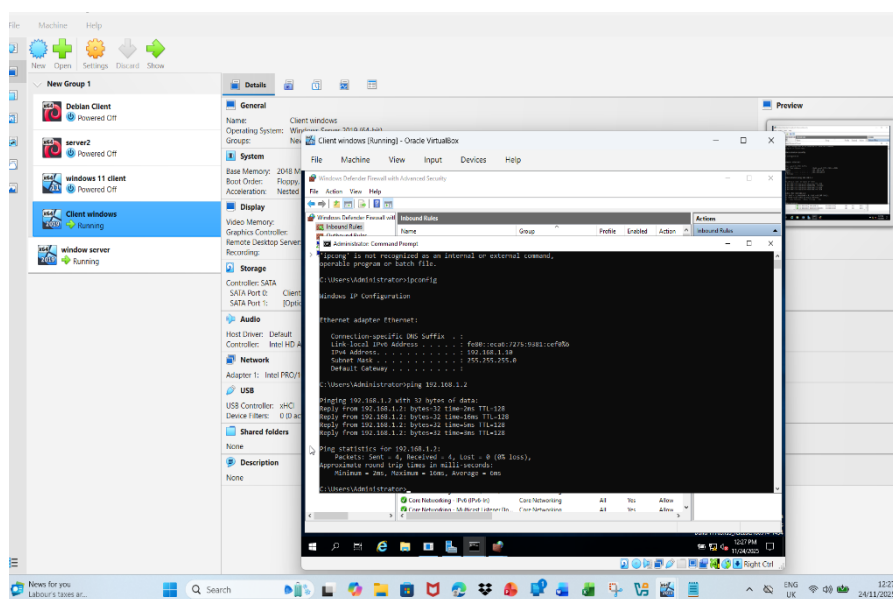


ping demonstration

Ping from the Server window to the Client is working after a new rule has been set for Windows Client



Ping from the Client window to the Server and Server to Client are working after a new rule has been set for both



Task 3

Reflection

Technical Reflection

Deploying Oracle VirtualBox and installing Windows Server and Client, and Debian Server and Client operating systems, provided valuable insights into virtualisation technology and multi-OS environments. The VirtualBox hypervisor efficiently allocated system resources, enabling simultaneous operation of both guest operating systems on a single host machine. Installing Windows required configuring adequate RAM and storage allocation, while Debian's lightweight nature demanded fewer resources. The process reinforced understanding of virtual hardware configuration, including network adapters, storage controllers, and display settings.

Challenges During Deployment and IP Address Configuration

Several challenges arose during the deployment and testing of VirtualBox. IP address conflicts occurred when both Windows Server and Windows Client virtual machines were assigned identical IP addresses on the Internal network, disrupting connectivity until manual IP configuration with unique addresses 192.168.1.1 and 192.168.1.10 resolved the issue. Windows Firewall initially blocked ping requests and network communication between Windows Server and Windows Client, requiring specific inbound new rule creation to permit ICMP traffic and file sharing protocols.

Personal Reflection

This virtualisation project significantly enhanced my technical confidence and problem-solving abilities. Initially, networking concepts like NAT adapters seemed abstract, but hands-on configuration clarified its practical applications. Troubleshooting IP conflicts and firewall issues developed my systematic diagnostic approach, checking configurations methodically rather than random trial-and-error. Encountering and resolving challenges independently built resilience and research skills. This experience reinforced that IT professionals must embrace continuous learning, as technology constantly evolves. The ability to create isolated testing environments through virtualisation will prove invaluable for future software development, security testing, and educational purposes throughout my career.

References

- [1] ONLINE, “AWS,” What’s the Difference Between Type 1 and Type 2 Hypervisors?, [Online]. Available: <https://aws.amazon.com/compare/the-difference-between-type-1-and-type-2-hypervisors/>. [Accessed 09 11 2025].
- [2] online, “storemagic,” Type 1 vs Type 2 Hypervisors: Key Differences Explained, 20 May 2025. [Online]. Available: <https://stormagic.com/company/blog/type-1-vs-type-2-hypervisors/>. [Accessed 09 November 2025].
- [3] S. Technologies, “Sangfor,” Type 1 vs. Type 2 Hypervisor: Key Differences, Advantages, and Use Cases, 18 november 2024. [Online]. Available: <https://www.sangfor.com/glossary/cloud-and-infrastructure/type-1-vs-type-2-hypervisor-key-differences>. [Accessed 10 november 2025].
- [4] C. Hayhurst, “Biztech,” CDW, 16 JULY 2025. [Online]. Available: <https://biztechmagazine.com/article/2024/08/type-1-vs-type-2-hypervisors-whats-difference-perfcon>. [Accessed 11 NOVEMBER 2025].
- [5] O. Pankevych, “Star Wind,” Type 1 vs. Type 2 Hypervisor: What Is The Difference, 20 July 2023. [Online]. Available: <https://www.starwindsoftware.com/blog/type-1-vs-type-2-hypervisor-what-is-the-difference/>. [Accessed 11 November 2025].
- [6] A. Timokhin, “InterLIR,” 2025. [Online]. Available: <https://interlir.com/2024/12/26/a-beginners-guide-to-subnetting-ipv4-and-ipv6-addresses/>. [Accessed 12 november 2025].
- [7] N. Brightwood, “ | NSC,” 22 August 2024. [Online]. Available: <https://netseccloud.com/ipv4-vs-ipv6-subnetting-differences>. [Accessed 11 november 2025].
- [8] V. D. Pallas, “PallasDigital,” 06 November 2022. [Online]. Available: <https://pall.as/ipv6-addressing-and-subnetting/>. [Accessed 10 November 2025].
- [9] n. Security, “WEBASHA,” 05 July 2025. [Online]. Available: <https://www.webasha.com/blog/what-is-the-difference-between-static-and->

dynamic-routing-and-how-can-you-configure-them. [Accessed 10 November 2025].

- [10] Moore, "QSFPTek," 09 April 2024. [Online]. Available: <https://www.qsfptek.com/qt-news/rip-vs-ospf.html>. [Accessed 10 November 2025].
- [11] Sheldon, "FS," 15 December 2021. [Online]. Available: <https://www.fs.com/blog/rip-vs-ospf-what-is-the-difference-3479.html>. [Accessed 10 November 2025].
- [12] M. Navsariwala, "Server Mania," What's the Difference Between Type-1 Hypervisor vs Type-2 Hypervisor?, 13 October 2023. [Online]. Available: <https://blog.servermania.com/type-1-hypervisor-vs-type-2-hypervisor>. [Accessed 10 November 2025].
- [13] W. Server, "Microsoft Ignite," Tutorial: Deploy Always On VPN infrastructure, 25 July 2025. [Online]. Available: <https://learn.microsoft.com/en-us/windows-server/remote/remote-access/tutorial-aovpn-deploy-setup>. [Accessed 10 November 2025].
- [14] J. Moody, "4sysops," Active Directory, Group Policy, and server certificates., 21 November 2017. [Online]. Available: <https://4sysops.com/archives/active-directory-group-policy-and-certificates-for-always-on-vpn/>. [Accessed 10 November 2025].
- [15] T. C. Team, "Trio," Active Directory Certificate Services, 30 September 2025. [Online]. Available: <https://www.trio.so/blog/active-directory-certificate-services>. [Accessed 12 November 2025].
- [16] Z. D. T. Temirbekova, "2025 IEEE 5th International Conference on Smart Information Systems and Technologies (SIST)," in *IEEE Xplore*., Astana, Kazakhstan, September 2025.
- [17] E. R. & G. H. A. Ivan Vakal, "Included in the following conference series;" in *Springer Nature*, 20 October 2025.
- [18] F. Ramalho and A. Neto, "17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)," in *IEEE Xplore*, Coimbra, Portugal, 28 July 2016.
- [19] R. Droms, "Automated configuration of TCP/IP with DHCP," *IEEE Internet Computing*, vol. 3, no. 4, pp. 45 - 53, 31 August 1999 .

- [20] C. Tomer, "Cloud computing and virtual machines in LIS education: options and resources," *Emerald Publishing*, vol. 33, no. 1, pp. 14 -39, 13 February 2017.