

Sarah LEVY
Student - 2422988



NETWORK OPERATING SYSTEMS AND SERVICES

- Research, build, and deploy, a Virtualized network -

Started on 30-01-25

Due on 07-03-25

SUMMARY:

TASK 1:	1
Introduction	1
Hypervisor	2
IP Addressing	3
Routing	6
Network Services	8
VPN	8
Dynamic Host Configuration Protocol	8
Active Directory	8
Certificate Authorities	8
TASK 2:	9
Choice of Hypervisor	9
Installing operating systems	9
Choosing and implementing network topology	12
Configuring IP Addresses and Routing	14
Configuring DHCP Servers	17
Swansea LAN – Windows Server	17
LAN Cardiff – Debian Server	18
Managing Connectivity Issues	18
Final Connectivity Testing and Validation	19
TASK 3:	22

TASK 1: Introduction

Virtualization is a technique that allows multiple operating systems or applications to run on a single computer by simulating various independent machines.

That way it's like creating multiple "virtual" computers inside only one computer.

→ *Where does it come from ?*

In the 1960s, IBM introduced virtualization for their central computers called "mainframes". The objective was to optimize the use of expensive resources of mainframes by allowing simultaneous processing of multiple tasks.

Virtualization experienced a revival only in the 1990s with the emergence of personal computers. Companies like VMware have developed solutions to run multiple operating systems on x86 machines, making virtualization more accessible to businesses and individuals.

→ *So how does it work ?*

Instead of installing an operating system directly on a computer, we use a software called a "**hypervisor**" that allows us to create and simulate those *virtual machines* (or VMs).

Each VM is an entire computer with its own operating system (Windows / Linux / MacOS...), but they share the same hardware (processor, memory, storage...).

→ *Here are some common use cases for virtualization*

- Can host multiple servers on a single computer. Rather than purchasing 3 physical servers for example, a company uses a single powerful server and creates 3 virtual machines on it, each assigned to a specific task.
- Cloud computing and website hosting. When we create a website on OVH, AWS or Google Cloud, the site does not run on a real computer dedicated only to us. These platforms use virtualization to run thousands of sites on a few servers.
- Gaming and emulation. If we want to play an old game that only runs on Windows XP. We can create a virtual machine with Windows XP and play on it without modifying our main PC.

→ *Benefits & Advantages*

- A single server can host multiple virtual machines, reducing purchasing costs and energy consumption.
- A single computer can run multiple OS and applications in parallel, without wasting power.
- Each virtual machine is isolated from the others, so an attack or crash does not affect the main machine.
- A virtual machine can be backed up to a single file and restored in minutes. (snapshots)
- We can clone a virtual machine and instantly deploy it to multiple computers.
- Reducing the number of physical servers leads to lower electricity consumption and less electronic waste.

¹ Source : Hewlett Packard Enterprise. Credits on resources page.

Hypervisor

As previously stated a hypervisor is a software that creates and manages Virtual Machines (VMs) by separating the physical hardware from the operating systems.

There are two main types of hypervisors:

To begin, there is **Type 1**, called “*bare metal*” which runs directly on Hardware, without an OS. It directly manages VMs and allocates resources (CPU, RAM, storage, network).

→ *How does it work ?*

The hypervisor controls the physical hardware, with each VM running independently on its own OS. It acts as a manager, it distributes resources as needed.

→ *Advantages*

Type 1 hypervisors provide near-native performance by interacting directly with hardware, reducing latency and optimizing resource use. Their lack of a host OS minimizes attack surfaces, making them ideal for high-security environments. They also support a lot of VMs by dynamically managing CPU, memory, storage, and network resources, ensuring scalability and reliability in large cloud infrastructures.

→ *Disadvantages*

Their complex setup requires advanced expertise, limiting accessibility for small businesses and non-technical users. Additionally, some need specific hardware configurations, restricting their deployment on existing systems.

→ *Hardware Requirements*

Type 1 needs CPUs with virtualization (Intel VT-x, AMD, AMD-V) for hardware acceleration. High-speed storage (NVMe, SSDs) and enterprise-grade network interfaces are recommended to optimize VM performance.

That leaves us with **Type 2**, called “*hosted*”. It runs on top of an existing OS, like a standard application, enabling VM execution.

→ *How does it work ?*

The host OS (Windows / Mac / Linux) manages hardware resources, while the hypervisor runs as software (examples: VirtualBox, VMware Workstation). VMs share resources with the host OS.

→ *Advantages*

Type 2 hypervisors are easy to install and use, requiring no technical expertise. They work on any PC or Mac, offering flexibility for OS testing. Developers can quickly set up isolated test environments without impacting their main system.

→ *Disadvantages*

Because they rely on a host OS, performance is lower than Type 1 due to additional resource management overhead. Security is weaker since host OS flaws can expose VMs.

² Sources from : TechTarget / StarWind Blog / IONOS Digital Guide. Credits on resources page.

→ **Hardware Requirements**

Unlike Type 1, Type 2 hypervisors don't require specialized hardware. However, a multi-core CPU, sufficient RAM, and SSD storage improve VM performance.

Here are some **examples of hypervisors**:

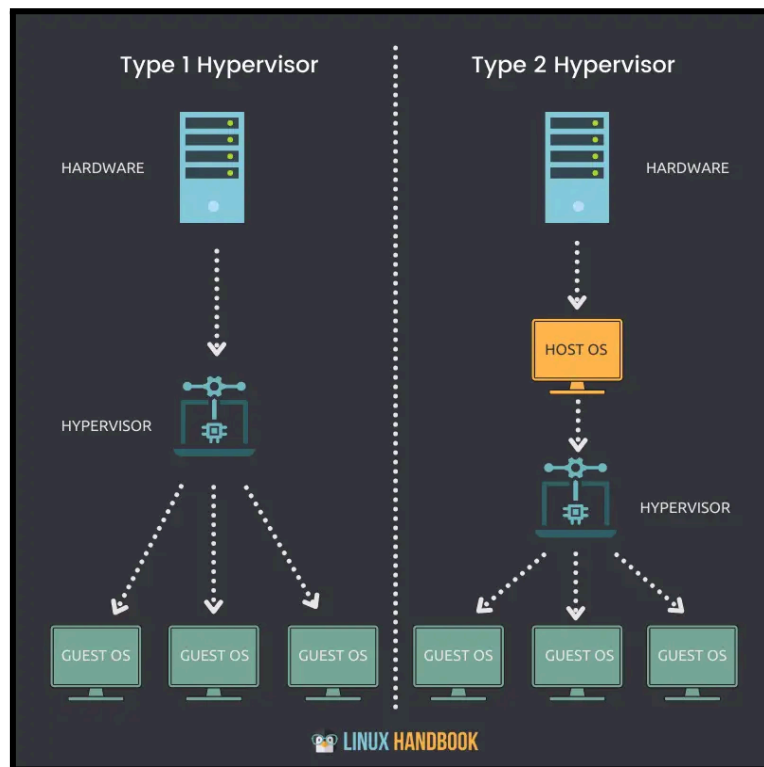
Type 1 : VMware ESXi, Microsoft Hyper-V (server mode), KVM, Xen...

Type 2 : VirtualBox, VMware Workstation, Parallels Desktop.

→ **Critical Analysis**

Despite their importance, hypervisors have challenges. Fair CPU sharing between VMs is hard in busy systems. Even Type 1 can face security risks, needing regular updates and monitoring.

While Type 1 is best for enterprises, Type 2 is more useful for testing and research. The choice depends on performance, security, and ease of use.



3 - Comparison of Type 1 and Type 2 Hypervisors in Virtualization -

³ Source from : Linux Handbook. Credits on resources page.

IP Addressing

Ever wondered how devices communicate seamlessly ? Each laptop, smartphone, or virtual machine relies on a unique IP address to connect. This identifier allows recognition and interaction and without it, a device stays isolated.

Addressing ensures connectivity, security, and efficiency. For example, Microsoft Azure uses private IPs for secure communication between virtual networks and on-prem systems.

→ How Does Data Flow on the Internet ?

According to *Kaspersky*⁴, the Internet follows a structured data exchange, breaking information into small packets for efficient transmission from A to B.

Each packet contains :

- A data fragment,
- Sender & recipient IPs,
- Metadata for routing.

As *Lifewire*⁵ explains, **IP** manages addressing / routing, while the Transmission Control Protocol (**TCP**) ensures complete, ordered delivery.

For example, when visiting a website, a device requests the server's IP. The server replies with data in packets, reassembled to display the page.

→ IPv4 vs. IPv6: Why two versions ?

IP addresses exist in two formats:

- **IPV4 (1981) :**
 - **32-bit system**, typically represented in decimal notation. (E.g., : **192.168.1.1**)
 - It's divided into a network prefix and a host identifier.
 - Limitation: Supports only 4.3 billion unique addresses, which is no longer enough for modern networking needs.
- **IPV6 (1998) :**
 - **128-bit system**, represented in hexadecimal notation. (E.g., **2001:0db8:85a3::8a2e:0370:7334**)
 - Addresses IPv4 address exhaustion and improves security and speed⁶.
 - Uses a network prefix + interface identifier, similar to IPv4.

→ Subnetting (Optimizing IP Allocation)

Subnetting⁷ divides a network into smaller subnets for efficiency and easier management.

- **IPv4:** Uses subnet masks to separate network/host. A /24 mask (255.255.255.0) allocates **24 bits** to the network, **8 bits** to hosts.
- **IPv6:** Uses a **64-bit prefix**, leaving **64 bits** for hosts, simplifying auto-configuration and network hierarchy.

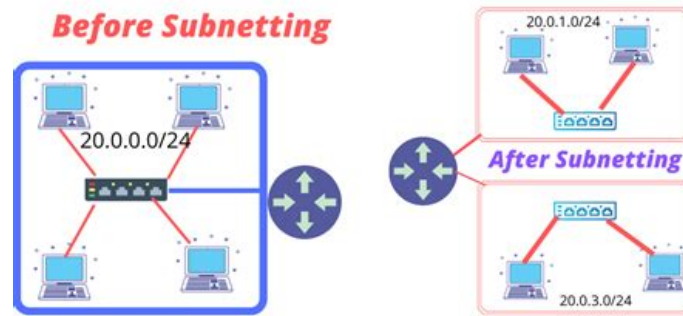
Subnetting helps improve network efficiency, reduce congestion, and enhance security.

⁴ Source from : Kaspersky. Credits on resources page.

⁵ Source from : Lifewire. Credits on resources page.

⁶ Source from : Jandl Digital. Credits on resources page.

⁷ Source from : Techtarget. Credits on resources page.



8 - Before and After Subnetting: Network Segmentation -

→ Detailed Structure of IP Addresses

As said, an IP address consists of two parts :

- **Network Prefix** : Identifies the network to which the device belongs.
- **Host Identifier** : Identifies the device within the network.

⇒ For example, in the address **192.168.1.10** **192.168.1** represents the **network**, and **.10** represents the **host (device)** within that network.

This distinction matters because routers use the network prefix to direct packets efficiently.

While **private IPs** secure internal communication, **public IPs** enable access to web services and APIs.

⇒ IPv4 Address Classification :

IPv4 addresses were initially divided into classes based on network size:

Class	Range	Usage
Class A	1.0.0.0 - 126.255.255.255	Very large networks (ISPs, enterprises)
Class B	128.0.0.0 - 191.255.255.255	Medium-sized networks (businesses)
Class C	192.0.0.0 - 223.255.255.255	Small networks (home networks, small businesses)
Class D	224.0.0.0 - 239.255.255.255	Multicast (data sent to multiple devices)
Class E	240.0.0.0 - 255.255.255.255	Experimental and reserved

→ Applications of IP addressing

- **Web hosting** : Public IPs make websites accessible, ensuring load balancing.
- **Cloud computing** : Dynamic IP allocation enables scalability.
- **Internet of Things (IoT)** : Each device needs a unique IP. IPv6 is key for handling many devices securely.

→ Security Risks

⚠ **IP Spoofing** → Attackers disguise their identity.

⚠ **DDoS Attacks** → Overloading a server with requests.

⇒ Firewalls and IP filtering help mitigate these threats.

⁸ Source from : CsPs Protocol. Credits on resources page.

Routing

Once IP addresses are assigned, data needs to reach its destination. Routing optimizes this process by selecting the most efficient paths. Routers use protocols to automate the process : either the static or dynamic protocols. This choice influences performance, security, and scalability differently.

→ The fundamental concepts of routing protocols

- **Static routing** : Routes are manually configured by the network administrator, defining fixed paths for data transmission. This method is precise and reliable but lacks flexibility in case of network changes. It is ideal for small infrastructures with stable and predictable data paths.
- **Dynamic routing** : Routers use specific protocols to automatically exchange real-time information about network topology. This enables fast adaptation to changes, such as adding or removing routes, without human intervention.

Dynamic routing are divided into several categories like :

⇒ **Distance Vector Routing Protocols** : Each router informs its neighbors about distances to various destinations, usually measured in the number of hops.

The Routing Information Protocol (RIP) is an example of a simple protocol, but it is limited (15 hops max). As it uses less resources, it is less suitable for large networks and is mainly used in small local networks such as those of small businesses or home routers.

⇒ **Link State Routing Protocols** : Each router has a complete view of the network topology and calculates the shortest paths to each destination.

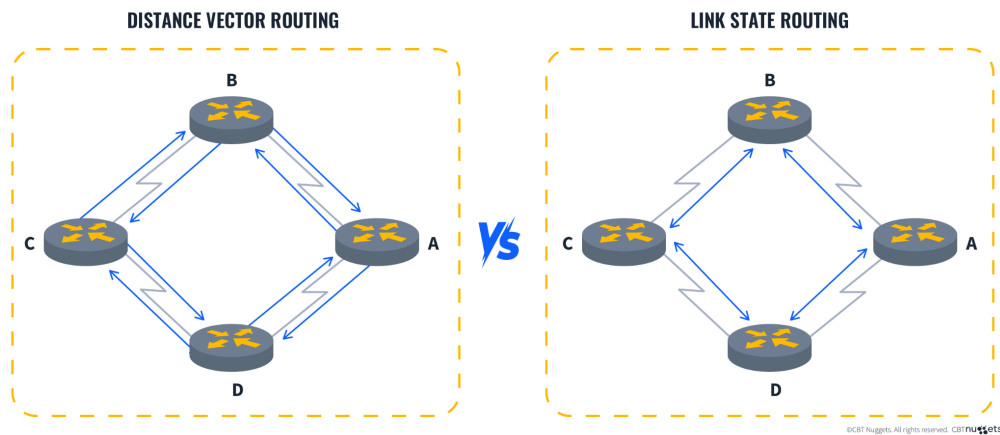
Open Shortest Path First (OSPF) is often used in enterprise networks such as banking networks or large universities for its speed and ability to recalculate routes in case of changes. Big companies like Microsoft for instance use this protocol to interconnect across the world.

⇒ **Hybrid Routing Protocols** : These protocols combine elements from both categories to optimize routing.

The Enhanced Interior Gateway Routing Protocol (EIGRP), developed by Cisco, offers a compromise between speed and low resource consumption, making it suitable for complex infrastructures. These protocols optimize paths based on metrics like latency and bandwidth. It is primarily used in enterprises with Cisco hardware, especially for internal cloud services.

⁹ Static vs dynamic routing protocols. Credits on resources page.

¹⁰ Different categories of dynamic routing & image : Credits on resources page.



10 - Different categories of dynamic routing -

→ **Comparison between static and dynamic routing**

Criteria	Static routing	Dynamic routing
Configuration	Manual	Automatic
Simplicity	Easy to configure	Complex, requires expertise
Resource Consumption	Low (no background processing)	High (continuous calculations and route updates)
Flexibility	None, must be updated manually	High, adjusts routes automatically
Adaptability	Not suitable for evolving networks	Ideal for complex, dynamic networks
Use Cases	Small networks, fixed connections	Large infrastructures, Internet, enterprises

→ **Benefits and Challenges of Routing Protocols**

Routing protocols help optimize data paths, adapt to breakdowns and improve traffic management. However they come with challenges like complex configuration, higher resource usage and some potential vulnerabilities regarding security. For example, dynamic routing needs a good understanding of commands and is less secure since updates are shared through protocol-identified interfaces.

¹¹ Information of the table found on Indeed. Credits on resources page.

Network Services

VPN

A **Virtual Private Network (VPN)** is a technology that establishes a secure and encrypted connection over a less secure network, such as the internet. A VPN hides the user's IP address, protecting personal data and online activity from interceptions. It can also bypass geographic restrictions and access blocked content. Using a VPN is like sending a letter in a sealed envelope instead of a postcard that everyone can see.

There are several types of VPNs adapted for different uses. For example, *Remote Access VPN* allows employees to connect securely to their company network from anywhere, whereas *Site-to-Site VPN* connects multiple offices of the same company via a secure tunnel.

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is a network protocol that automatically assigns IP addresses and other configuration parameters to devices all connected to the same network, simplifying IP address management. This eliminates the need for manual configuration and makes it easier to add or remove devices from the network. However, if the DHCP server goes down, new devices will no longer receive an IP address, creating a dependency on the server.

Active Directory

Active Directory Domain Services (AD DS) is a system used by businesses to manage employee access to computers, files, and applications. It defines who can access what and ensures the security of user accounts. In a large company like Microsoft, Active Directory is used to manage employee logins, which means that an employee can log in to any workstation in the company with their ID. Additionally, managers have access to confidential documents, while regular employees can only access files related to their department.

Certificate Authorities

Certificate Authorities (CAs) issue digital certificates that verify the authenticity of websites and organizations. This helps secure data exchanges and ensure that users are communicating with legitimate entities.

The most well-known certificate authorities include:

- Let's Encrypt (free certificates for websites)
- DigiCert (premium certificates for large companies)
- GlobalSign (used by banks and government services)

When accessing an HTTPS site, the padlock in the address bar indicates that the site has a valid certificate issued by a trusted certificate authority.

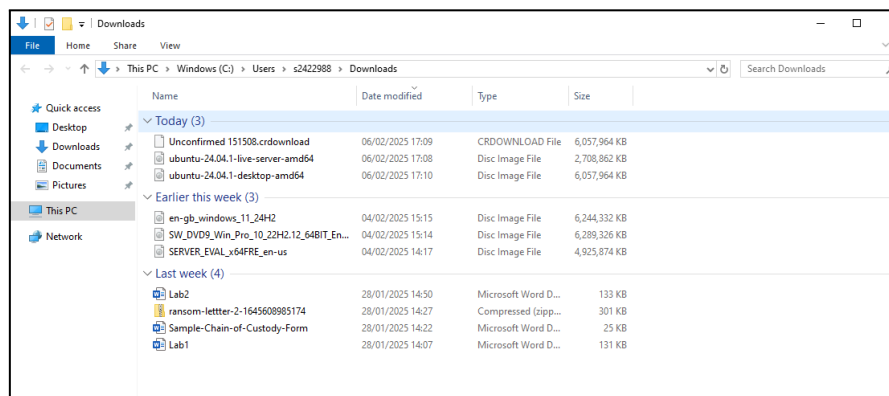
TASK 2:

Choice of Hypervisor

A type 2 hypervisor was selected because virtualization was new, and it appeared more accessible. With no prior knowledge in this area, research and external advice pointed towards this option, as it is easier to manage for a first experience. However, this choice also meant that running the project on a personal computer (a MacBook Pro M4) was not possible, as it cannot support some OSs such as Windows Server 2022 (x64 architecture only). As a result, the project was carried out on the university's computer.

Installing operating systems

The process began with downloading ISO files from their official websites.



- All files were downloaded - ¹²

Once the files were recovered, virtual machines were created in VirtualBox, the chosen Type 2 hypervisor. During the creation process, **the disk size**, amount of **RAM**, and number of **cores** allocated to each VM were defined. The corresponding ISO files were then mounted for each machine. It was observed that Windows 10 and Windows Server 2022 were already connected to the internet by default, which made the installation easier.

After launching the virtual machines, the installation of the operating systems was carried out. During this step, the basic settings were configured, particularly the language (**English US**), the time zone (**UK**), and the keyboard layout (**UK**). The same username and password were used for each VM to simplify management.

¹² Note that after taking this screenshot, we later switched the Ubuntu server to a Debian server.

- NETWORK OPERATING SYSTEMS AND SERVICES -

The image displays four sequential screenshots of the Oracle VM VirtualBox 'Create Virtual Machine' wizard, illustrating the steps for creating a new virtual machine.

Screenshot 1: Virtual machine Name and Operating System
This screen allows the user to choose a descriptive name and destination folder for the new virtual machine. The name chosen is 'Windows 10 (SWANSEA)'. The folder is 'C:\Users\p2422988\VirtualBox VMs'. The ISO image is 'C:\Users\p2422988\VirtualBox VMs\SW_DVD9_Win_Pro_10_22H2.12_64BIT_English_Pro_Ent_EDU_N_MLF_X23-61953.ISO'. The edition is 'Windows 10 Education (10.0.19041.3570 / x64 / en-US)'. The type is 'Microsoft Windows' and the version is 'Windows 10 (64-bit)'. There is a checkbox for 'Skip Unattended Installation' which is unchecked. A message states: 'Detected OS type: Windows 10 (64-bit). This OS type can be installed unattended. The install will start after this wizard is closed. Go to Settings to activate Windows.'

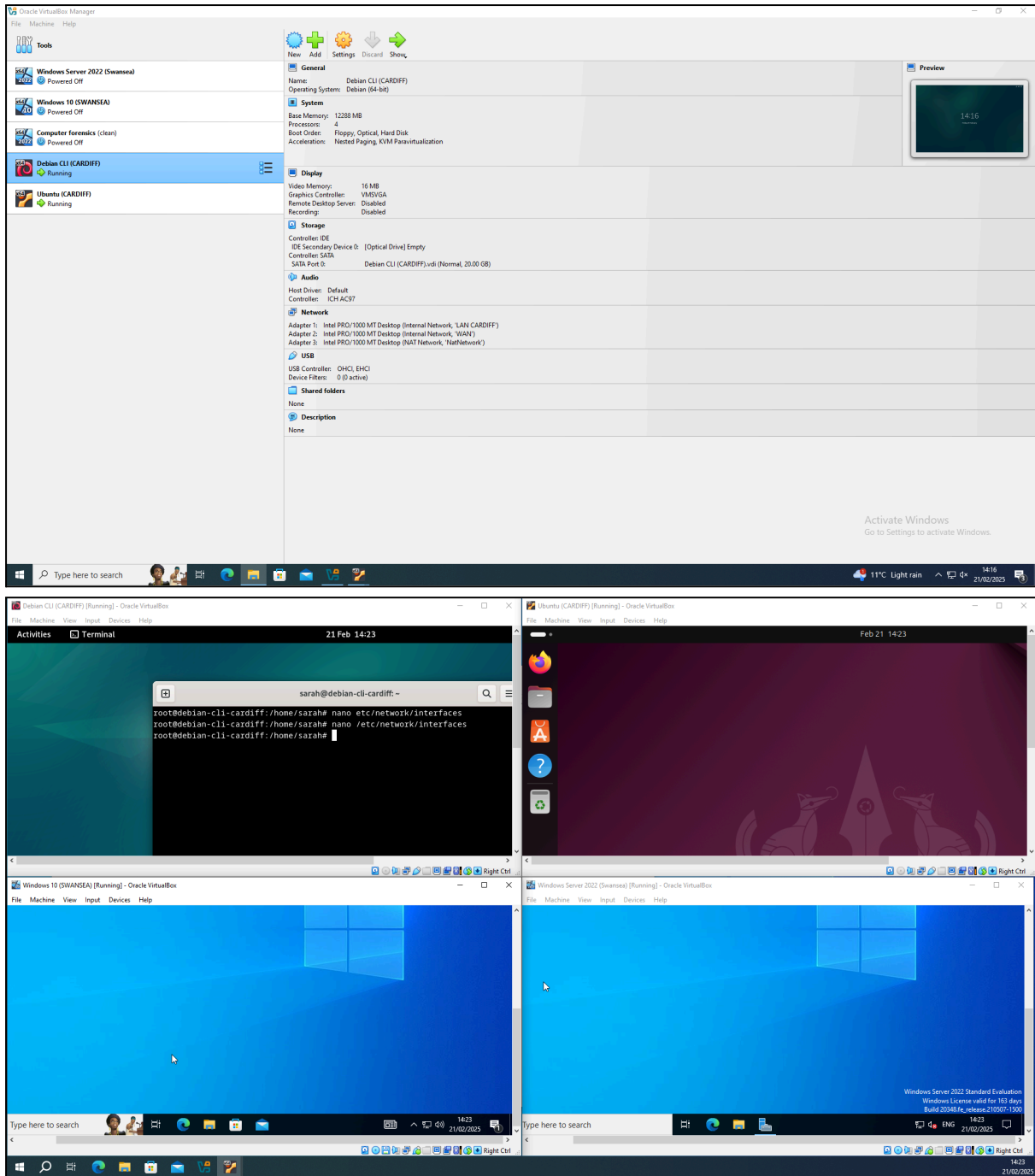
Screenshot 2: Unattended Guest OS Install Setup
This screen allows the user to configure the unattended guest OS install by modifying username, password, and hostname. The username is 'Sarah', the password is masked with dots, and the repeat password is also masked. The product key is '#####-#####-#####-#####-#####'. The hostname is 'Windows' and the domain name is 'myguest.virtualbox.org'. There is a checkbox for 'Install in Background' which is unchecked. The guest additions ISO is 'C:\Program Files\Oracle\VirtualBox\BoxGuestAdditions.iso'. A message states: 'Go to Settings to activate Windows.'

Screenshot 3: Hardware
This screen allows the user to modify the virtual machine's hardware by changing the amount of RAM and virtual CPU count. The base memory is set to 8000 MB (with a slider from 4 MB to 65536 MB). The number of processors is set to 4 (with a slider from 1 CPU to 24 CPUs). There is a checkbox for 'Enable EFI (special OSes only)' which is unchecked. A message states: 'Activate Windows. Go to Settings to activate Windows.'

Screenshot 4: Virtual Hard disk
This screen allows the user to add a virtual hard disk to the new machine. The user can either create a new hard disk file or select an existing one. The 'Create a Virtual Hard Disk Now' option is selected. The disk size is set to 50.00 GB (with a slider from 4.00 MB to 2.00 TB). There is a checkbox for 'Pre-allocate Full Size' which is unchecked. The 'Use an Existing Virtual Hard Disk File' option is selected, and the file is 'Windows Server 2022.vdi (Normal, 50.00 GB)'. There is a checkbox for 'Do Not Add a Virtual Hard Disk' which is unchecked. A message states: 'Activate Windows. Go to Settings to activate Windows.'

- VM Installation Process -

- NETWORK OPERATING SYSTEMS AND SERVICES -



- All 4 VM are working -

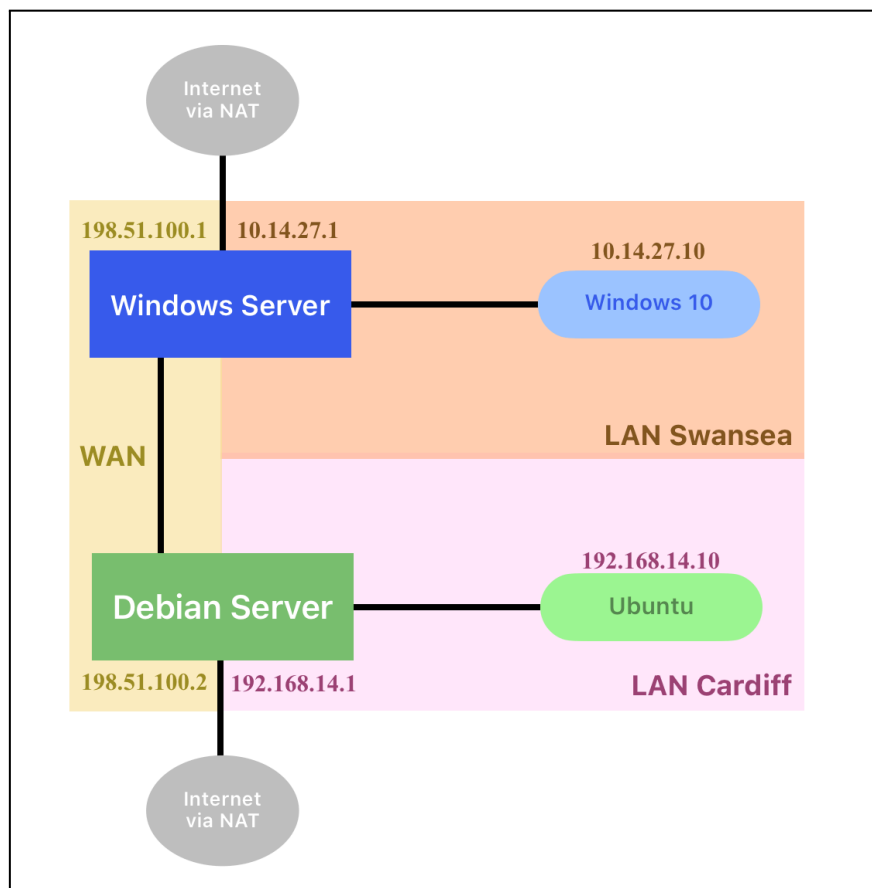
Choosing and implementing network topology

Next, the network topology was set up by creating the **Swansea LAN (10.14.27.0/24)**, **Cardiff LAN (192.168.14.0/24)**, and the **WAN (198.51.100.0/30)** networks.

These addresses were selected in accordance with best corporate addressing practices. The **10.14.27.0/24 & 192.168.14.0/24** addresses belong to the **private address ranges** defined by *RFC 1918*, which are specifically intended for internal networks. Using separate subnets ensures proper segmentation of the Swansea and Cardiff sites and allows for efficient routing management.

For the **WAN**, **198.51.100.0/30** was chosen, as it falls within the documentation range defined by *RFC 5737* and simulates a point-to-point link between the two networks. Using a /30 subnet mask optimizes address allocation by providing only two usable addresses (**198.51.100.1 and 198.51.100.2**), assigned to the routers at each site.

For **NAT**, IP addresses are automatically assigned by VirtualBox, which functions as a gateway between the virtual machines and the Internet. In this project, both Windows Server and Debian Server have an interface connected to a **NAT** network (the UWTSD one). Clients on the Swansea LAN and Cardiff LAN can access the Internet through their respective server, which acts as a NAT gateway.

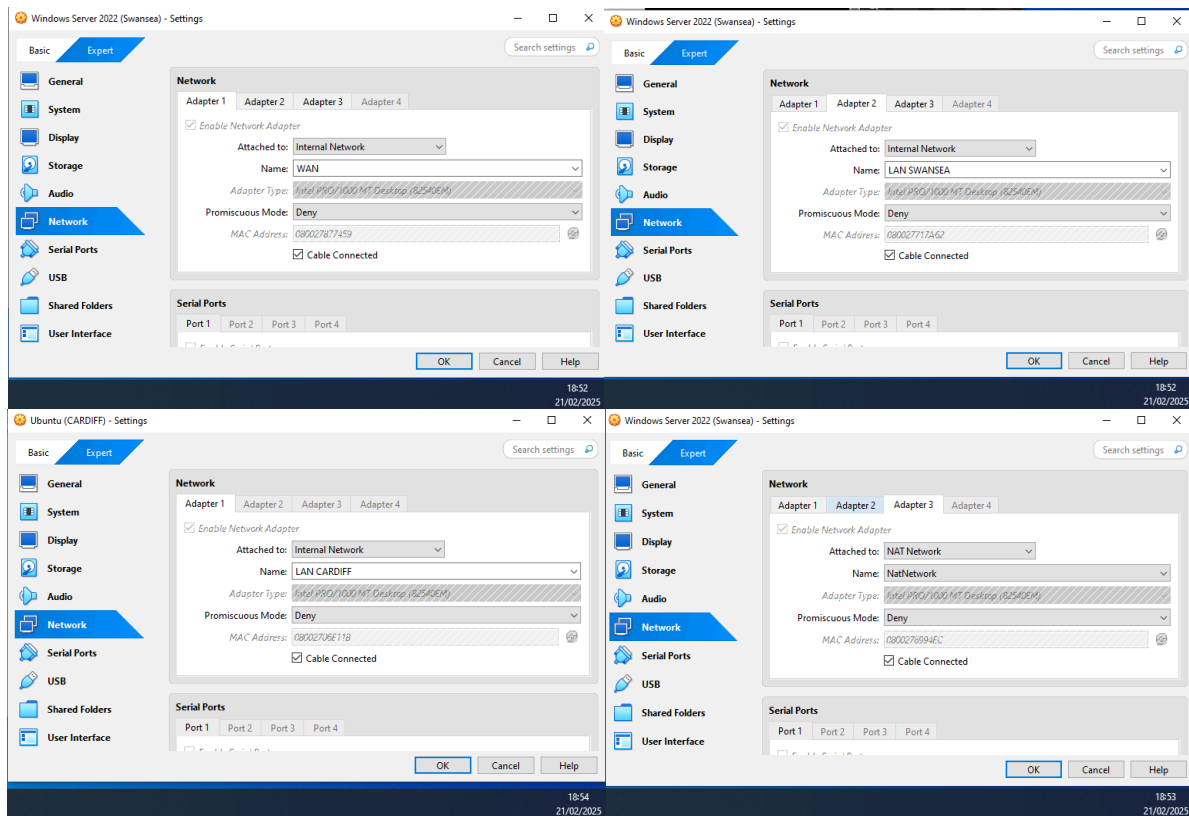


- Diagram of the Network Topology -

- NETWORK OPERATING SYSTEMS AND SERVICES -

In VirtualBox, the network cards of the machines were configured as follows:

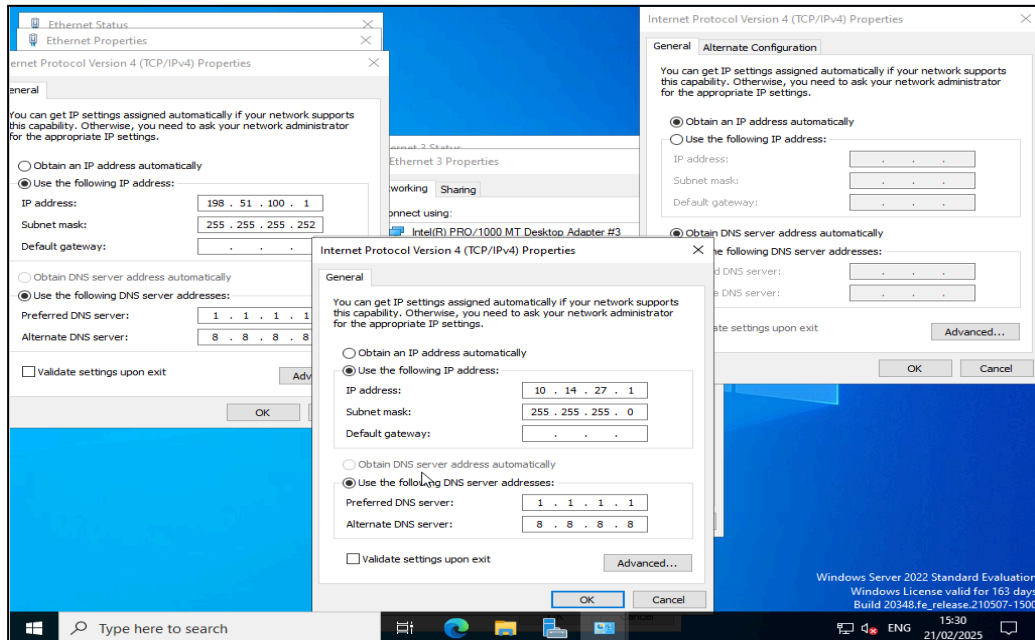
- **Windows Server** is connected to three networks: **LAN Swansea**, **WAN**, and **NAT**.
- **Windows 10** is connected to **LAN Swansea**.
- **Debian Server** is connected to three networks: **LAN Cardiff**, **WAN**, and **NAT**.
- **Ubuntu** is connected to **LAN Cardiff**.



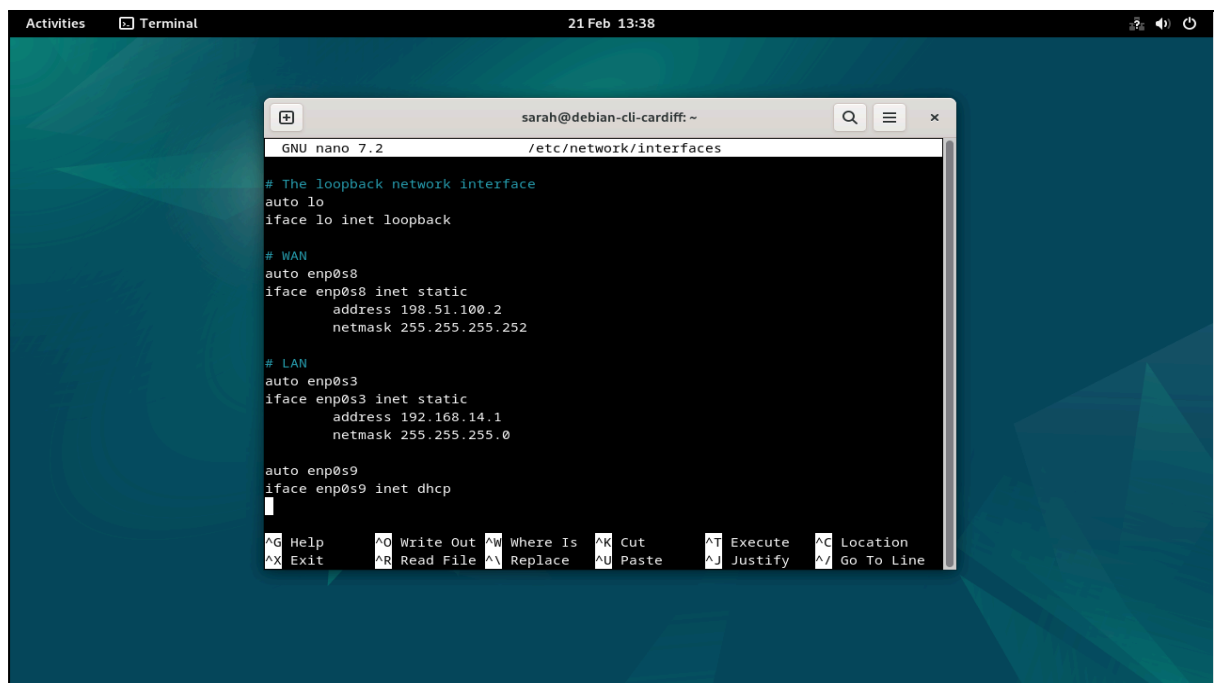
*- Screenshot of the configuration of Windows Server and Ubuntu -
(Same process was used for the other two ones)*

Configuring IP Addresses and Routing

First, static IP addresses were configured for the servers.



- Windows Static IP Address -

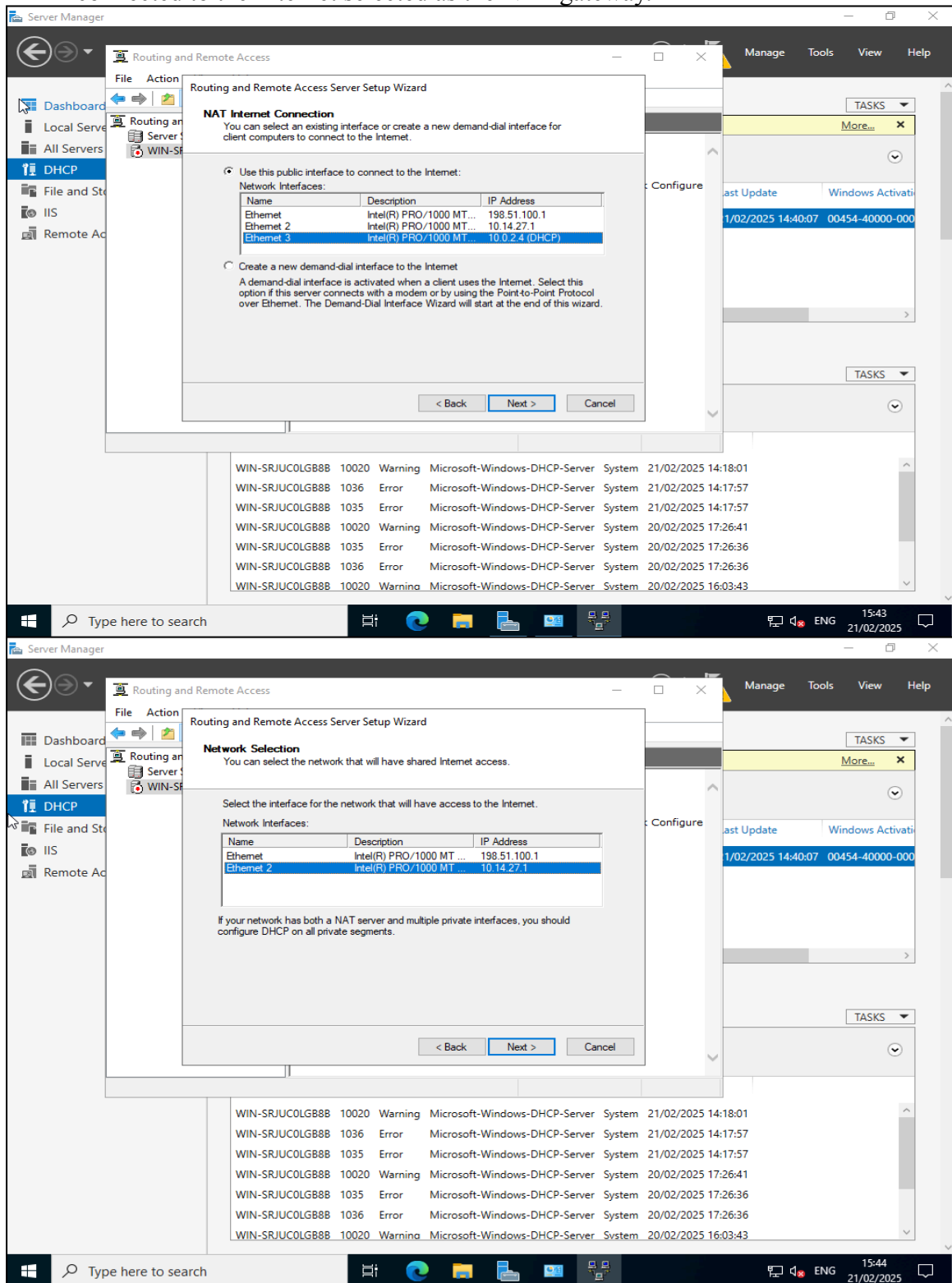


- Debian Static IP Address -

- NETWORK OPERATING SYSTEMS AND SERVICES -

Next, NAT was set up on each server to allow Internet access for machines on the local network:

- **On Windows Server, Routing and Remote Access** was enabled, with the interface connected to the Internet selected as the NAT gateway.



- Routing & Remote Access configuration -

- NETWORK OPERATING SYSTEMS AND SERVICES -

- **On Debian Server, IP forwarding** was enabled, network interfaces were identified, and the necessary **Iptables** rules were applied to ensure address translation.

```
Debian CLI (CARDIFF) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal 21 Feb 18:48
sarah@debian-cli-cardiff: ~
GNU nano 7.2 /etc/sysctl.conf
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
#net.ipv4.conf.all.accept_redirects = 0
#net.ipv6.conf.all.accept_redirects = 0
#_or_
# Accept ICMP redirects only for gateways listed in our default
# gateway list (enabled by default)
# net.ipv4.conf.all.secure_redirects = 1
#
# Do not send ICMP redirects (we are not a router)
#net.ipv4.conf.all.send_redirects = 0
#
# Do not accept IP source route packets (we are not a router)
#net.ipv4.conf.all.accept_source_route = 0
#net.ipv6.conf.all.accept_source_route = 0
#
# Log Martian Packets
#net.ipv4.conf.all.log_martians = 1
#
#####
# Magic system request Key
# 0=disable, 1=enable all, >1 bitmask of sysrq functions
# See https://www.kernel.org/doc/html/latest/admin-guide/sysrq.html
# for what other values do
#kernel.sysrq=438
net.ipv4.ip_forward=1
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location ^U Undo ^M-A Set Mark ^M-] To Bracket
^X Exit ^R Read File ^\ Replace ^V Paste ^J Justify ^_ Go To Line ^M-E Redo ^M-G Copy ^_ Where Was
Debian CLI (CARDIFF) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal 21 Feb 18:50
sarah@debian-cli-cardiff: ~
root@debian-cli-cardiff:/home/sarah# sudo iptables -L INPUT -v -n --line-numbers
Chain INPUT (policy ACCEPT 119 packets, 15645 bytes)
num pkts bytes target prot opt in out source destination
1 5 420 DROP 1 -- enp0s3 * 0.0.0.0/0 198.51.100.2 icmptype 8
root@debian-cli-cardiff:/home/sarah# sudo iptables -t nat -L POSTROUTING -v -n --line-numbers
Chain POSTROUTING (policy ACCEPT 9 packets, 757 bytes)
num pkts bytes target prot opt in out source destination
1 35 4438 MASQUERADE 0 -- * enp0s9 0.0.0.0/0 0.0.0.0/0
root@debian-cli-cardiff:/home/sarah# date
Fri 21 Feb 18:50:28 GMT 2025
root@debian-cli-cardiff:/home/sarah#
```

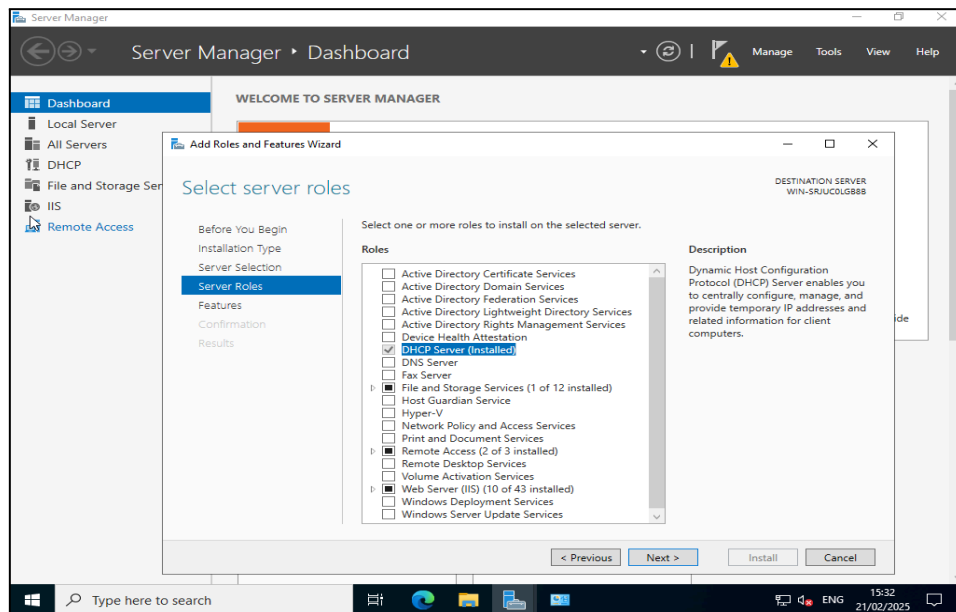
- IP Forwarding & Iptables Rules configuration -

Configuring DHCP Servers

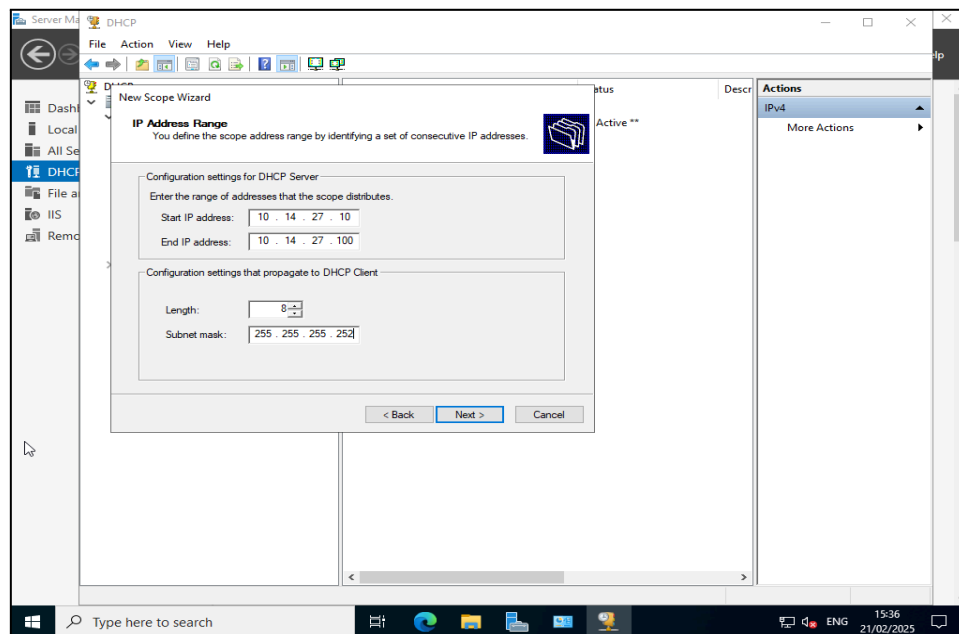
DHCP was set up at each site to ensure that clients automatically obtained their IP addresses.

Swansea LAN – Windows Server

The **DHCP** server was installed and configured on Windows Server. An IPv4 address range from **10.14.27.10 to 10.14.27.100** was defined, with the server's IP address (10.14.27.1) set as the default gateway. Once the DHCP service was enabled, Windows 10 successfully obtained its IP address automatically.



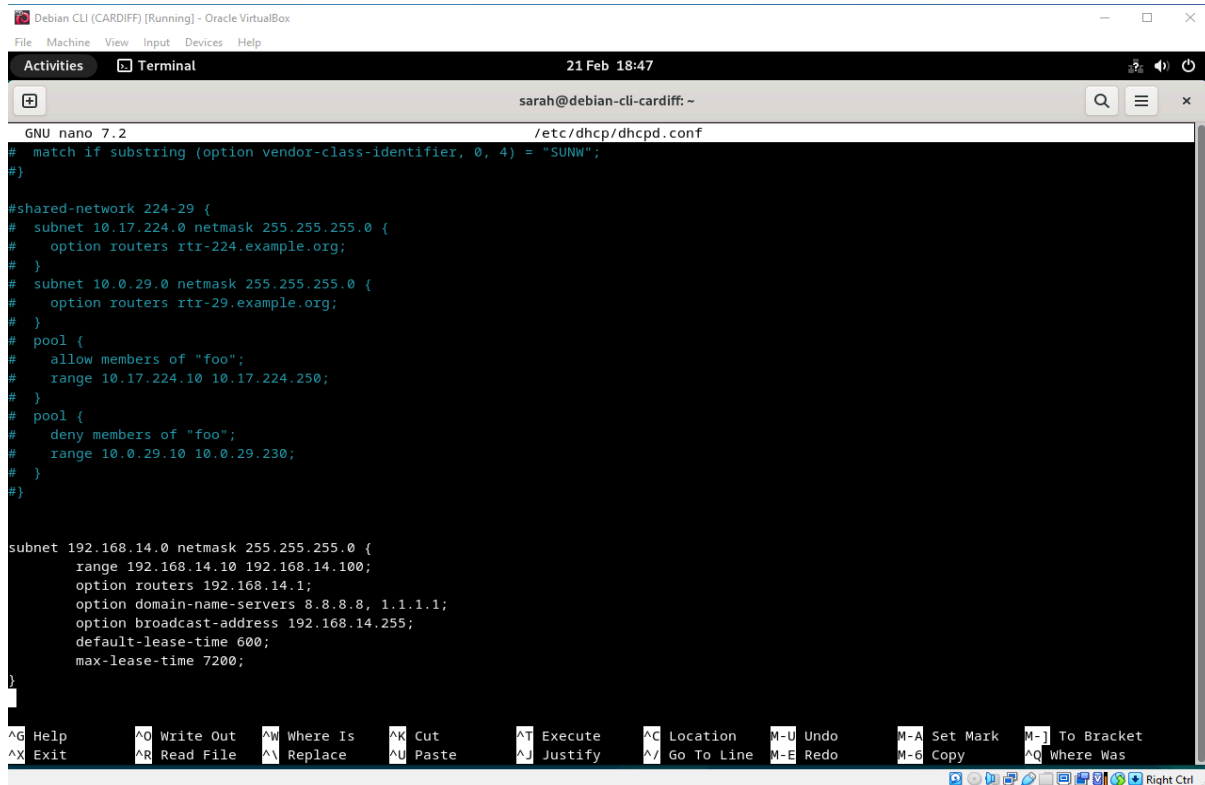
- DHCP installed Windows -



- DHCP IP Address Range on Windows -

LAN Cardiff – Debian Server

The **ISC DHCP SERVER** package was installed on the Debian Server, the network interface used by the service was specified, and the same address range for client distribution was configured. After restarting the service, Ubuntu successfully obtained an IP address automatically.



```
GNU nano 7.2 /etc/dhcp/dhcpd.conf
# match if substring (option vendor-class-identifier, 0, 4) = "SUNW";
#}

#shared-network 224-29 {
# subnet 10.17.224.0 netmask 255.255.255.0 {
#   option routers rtr-224.example.org;
# }
# subnet 10.0.29.0 netmask 255.255.255.0 {
#   option routers rtr-29.example.org;
# }
# pool {
#   allow members of "foo";
#   range 10.17.224.10 10.17.224.250;
# }
# pool {
#   deny members of "foo";
#   range 10.0.29.10 10.0.29.230;
# }
#}

subnet 192.168.14.0 netmask 255.255.255.0 {
  range 192.168.14.10 192.168.14.100;
  option routers 192.168.14.1;
  option domain-name-servers 8.8.8.8, 1.1.1.1;
  option broadcast-address 192.168.14.255;
  default-lease-time 600;
  max-lease-time 7200;
}
```

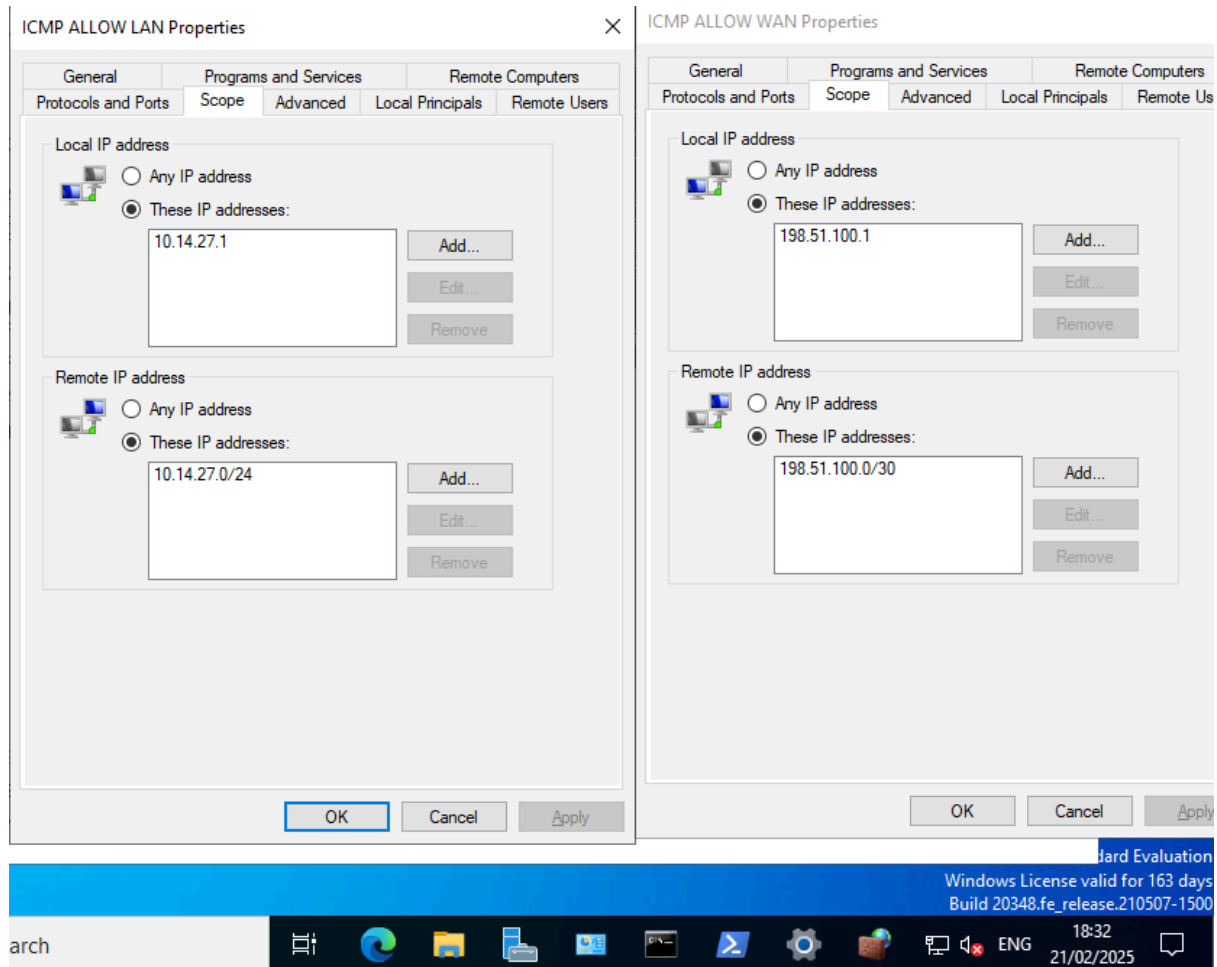
- DHCP IP Address range on Debian -

Managing Connectivity Issues

During testing, the same issue was encountered on both **LAN Swansea** and **LAN Cardiff**: client machines were able to ping their server's **WAN IP** because of the NAT configuration, which was not intended.

- **On LAN Swansea**, the issue was caused by a default Windows firewall rule that allowed ICMP requests on all interfaces. To resolve this, **two specific firewall rules** were created: one to allow **ping echo requests** only within the LAN and another one for only within the WAN. Those rules successfully blocked ping requests between the two. The **Windows 10 client** could no longer ping the **WAN IP** of the server, and the firewall was correctly filtering traffic.
- **On LAN Cardiff**, the issue was addressed by manually adjusting the **iptables** rules, explicitly allowing or blocking certain **ICMP requests** based on the interface. These configurations were then made **persistent** to ensure they remained after a reboot. After testing, the **Debian server** was correctly filtering ICMP requests, and the client could only communicate as intended.

By implementing these two different approaches, both networks were properly isolated while maintaining the necessary **network isolation**.

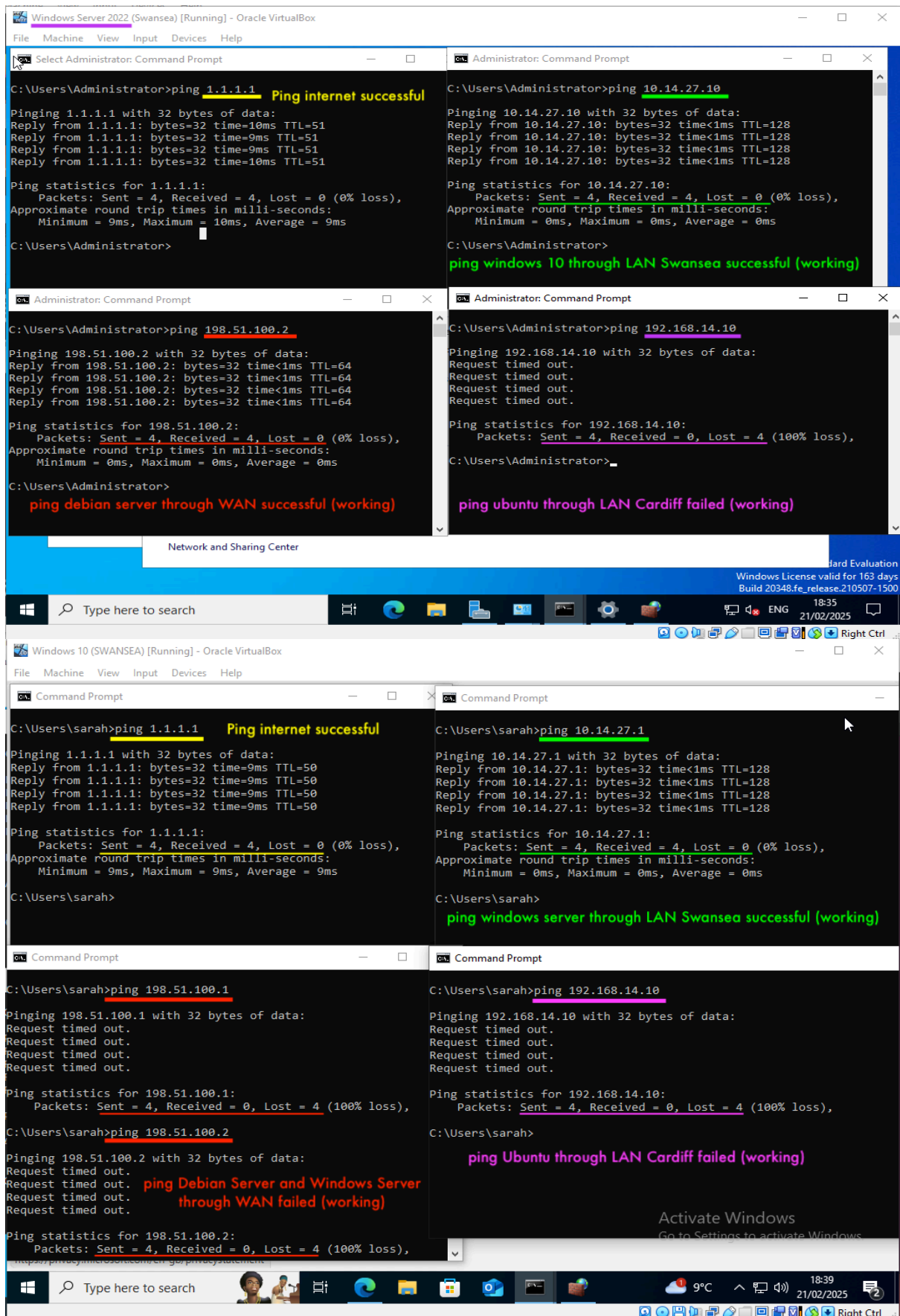


- New ICMP rules -

Final Connectivity Testing and Validation

Finally, connectivity was tested by pinging all machines from each other using their respective IP addresses and verifying their access to the Internet. Each device successfully communicated as expected within its designated network, and all routing and firewall rules functioned correctly. The network setup was fully operational, ensuring proper isolation between LANs while allowing controlled access to external resources.

- NETWORK OPERATING SYSTEMS AND SERVICES -



- Ping Test On Windows Server and computer -

- NETWORK OPERATING SYSTEMS AND SERVICES -

```
Debian CLI (CARDIFF) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal 21 Feb 18:42

sarah@debian-cli-cardiff: ~
root@debian-cli-cardiff:/home/sarah# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data:
64 bytes from 1.1.1.1: icmp_seq=1 ttl=51 time=9.70 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=51 time=9.40 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=51 time=9.38 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=51 time=9.33 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=51 time=9.40 ms
^C
--- 1.1.1.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4081ms
rtt min/avg/max/mdev = 9.332/9.441/9.697/0.130 ms
root@debian-cli-cardiff:/home/sarah# ping internet successful

sarah@debian-cli-cardiff: ~
sarah@debian-cli-cardiff:~$ ping 192.168.14.10
PING 192.168.14.10 (192.168.14.10) 56(84) bytes of data:
64 bytes from 192.168.14.10: icmp_seq=1 ttl=64 time=0.285 ms
64 bytes from 192.168.14.10: icmp_seq=2 ttl=64 time=0.265 ms
64 bytes from 192.168.14.10: icmp_seq=3 ttl=64 time=0.247 ms
64 bytes from 192.168.14.10: icmp_seq=4 ttl=64 time=0.378 ms
^C
--- 192.168.14.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3207ms
rtt min/avg/max/mdev = 0.247/0.293/0.378/0.050 ms
sarah@debian-cli-cardiff:~$ ping ubuntu through LAN Cardiff successful (Working)

sarah@debian-cli-cardiff: ~
sarah@debian-cli-cardiff:~$ ping 198.51.100.1
PING 198.51.100.1 (198.51.100.1) 56(84) bytes of data:
64 bytes from 198.51.100.1: icmp_seq=1 ttl=128 time=0.352 ms
64 bytes from 198.51.100.1: icmp_seq=2 ttl=128 time=0.310 ms
64 bytes from 198.51.100.1: icmp_seq=3 ttl=128 time=0.324 ms
64 bytes from 198.51.100.1: icmp_seq=4 ttl=128 time=0.399 ms
64 bytes from 198.51.100.1: icmp_seq=5 ttl=128 time=0.305 ms
^C
--- 198.51.100.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4103ms
rtt min/avg/max/mdev = 0.305/0.338/0.399/0.034 ms
sarah@debian-cli-cardiff:~$ ping Windows Server through WAN successful (Working)

sarah@debian-cli-cardiff: ~
sarah@debian-cli-cardiff:~$ ping 10.14.27.10
PING 10.14.27.10 (10.14.27.10) 56(84) bytes of data:
^C
--- 10.14.27.10 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4190ms

sarah@debian-cli-cardiff:~$ ping 10.14.27.1
PING 10.14.27.1 (10.14.27.1) 56(84) bytes of data:
^C
--- 10.14.27.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1043ms
sarah@debian-cli-cardiff:~$ ping Windows 10 through LAN Swansea failed (Working)

Ubuntu (CARDIFF) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Feb 21 18:45

sarah@sarah-VirtualBox: ~
sarah@sarah-VirtualBox:~$ ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data:
64 bytes from 1.1.1.1: icmp_seq=1 ttl=50 time=32.4 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=50 time=10.8 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=50 time=9.59 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=50 time=9.58 ms
^C
--- 1.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3038ms
rtt min/avg/max/mdev = 9.581/15.582/32.402/9.722 ms
sarah@sarah-VirtualBox:~$ ping internet successful

sarah@sarah-VirtualBox: ~
sarah@sarah-VirtualBox:~$ ping 192.168.14.1
PING 192.168.14.1 (192.168.14.1) 56(84) bytes of data:
64 bytes from 192.168.14.1: icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from 192.168.14.1: icmp_seq=2 ttl=64 time=0.272 ms
64 bytes from 192.168.14.1: icmp_seq=3 ttl=64 time=0.291 ms
64 bytes from 192.168.14.1: icmp_seq=4 ttl=64 time=0.273 ms
^C
--- 192.168.14.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3423ms
rtt min/avg/max/mdev = 0.272/0.372/0.653/0.162 ms
sarah@sarah-VirtualBox:~$ ping Debian Server through LAN Cardiff successful (Working)

sarah@sarah-VirtualBox: ~
sarah@sarah-VirtualBox:~$ ping 198.51.100.1
PING 198.51.100.1 (198.51.100.1) 56(84) bytes of data:
^C
--- 198.51.100.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2055ms

sarah@sarah-VirtualBox:~$ ping 198.51.100.2
PING 198.51.100.2 (198.51.100.2) 56(84) bytes of data:
^C
--- 198.51.100.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1155ms
sarah@sarah-VirtualBox:~$ ping Debian's & Windows's servers through WAN failed (Working)

sarah@sarah-VirtualBox: ~
sarah@sarah-VirtualBox:~$ ping 10.14.27.10
PING 10.14.27.10 (10.14.27.10) 56(84) bytes of data:
^C
--- 10.14.27.10 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3292ms
sarah@sarah-VirtualBox:~$ ping windows 10 through LAN Swansea failed (Working)
```

- Ping Test on Debian Server & Ubuntu Computer -

TASK 3:

During the deployment and testing of the network, two main issues were encountered: **network isolation and NAT configuration**. At first, LANs were not properly separated, allowing clients to ping the servers' WAN IPs. To fix this and after much research, firewall rules and Iptables settings were adjusted to block unwanted connections.

Another problem found was that VirtualBox's NAT did not provide Internet access as expected. It was found that the same problem happened for other persons on the internet that were also using VirtualBox and so a solution was found to restore the connection.

After all that work, everything is working perfectly and even for a beginner it was quite accessible with proper research.

Resources :

- [1] Hewlett Packard Enterprise. “What is Virtualization?”
HPE. Accessed feb.1, 2025. [Online]
Available : <https://www.hpe.com/uk/en/what-is/virtualization.html>
- [2] -
S.J. Bigelow. “What's the difference between Type 1 vs. Type 2 hypervisor?”
techtarget. Accessed feb.4, 2025. [Online]
Available :
<https://www.techtarget.com/searchitoperations/tip/Whats-the-difference-between-Type-1-vs-Type-2-hypervisor>

O. Pankevych. “Hypervisors: Type 1 vs Type 2. [PART 1]”
StarWind Hyperconvergence. Accessed feb.4, 2025. [Online]
Available :
<https://www.starwindsoftware.com/blog/type-1-vs-type-2-hypervisor-what-is-the-difference>
- IONOS editorial team. “What’s the difference between type 1 and type 2 hypervisors?”
IONOS Digital Guide. Accessed feb.4, 2025. [Online]
Available :
<https://www.ionos.com/digitalguide/server/know-how/hypervisor-type-1-and-type-2>
- [3] A. Bandyopadhyay. “Introduction to Virtualization: A Comprehensive Guide for Beginners”
Linux Handbook. Accessed feb.4, 2025. [Online]
Available :
<https://linuxhandbook.com/virtualization/>
- [4] Kaspersky. “What is an IP Address – Definition and Explanation”
Kaspersky. Accessed feb.5, 2025. [Online]
Available :
<https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address?>
- [5] J.Martindale. “What Is TCP/IP?”
Lifewire. Accessed feb.5, 2025. [Online]
Available :
<https://www.lifewire.com/what-is-tcp-ip-8693053?>
- [6] T. Jarrett. “Understanding IP Addresses and Their Role in Internet Communication” *Jandl Digital*. Accessed feb.5, 2025. [Online]
Available :
<https://www.jandl.digital/resources/blog/article/understanding-ip-addresses-and-their-role-in-internet-communication?>

- [7] D.Garn. "Introduction to IP addressing and subnetting"
TechTarget. Accessed feb.5, 2025. [Online]
Available : <https://www.techtarget.com/searchnetworking/tip/Introduction-to-IP-addressing-and-subnetting?>
- [8] CsPs Protocol. "Subnetting and Subnet Mask Explained with Examples."
CspsProtocol - Simplified Tutorial. Accessed feb.8, 2025. [Online]
Available : <https://www.cspsprotocol.com/subnetting-explained/>
- [9] A. Balchunas. "Static vs. Dynamic Routing "
routeralley. Accessed feb.11, 2025. [Online]
Available : https://www.routeralley.com/guides/static_dynamic_routing.pdf
- [10] M. Kafami. "Link State vs Distance Vector vs Hybrid Routing Protocols"
cbtnuggets. Accessed feb.11, 2025. [Online]
Available : <https://www.cbtnuggets.com/blog/technology/networking/link-state-distance-vector-vs-hybrid-routing-protocols>
- [11] Indeed Editorial Team.. "Static Routing vs. Dynamic Routing: What's the Difference?" *Indeed*. Accessed feb.11, 2025. [Online]
Available : <https://www.indeed.com/career-advice/career-development/dynamic-routing-vs-static-routing>