



Prifysgol Cymru  
Y Drindod Dewi Sant  
University of Wales  
Trinity Saint David

Network Operating Systems and Services  
ACCA5023  
Dr. Nitheesh Murugan Kaliyamurthy



---

# COURSEWORK 1

# PROJECT REPORT

---



|                                                                                    |    |
|------------------------------------------------------------------------------------|----|
| I) Hypervisors: Architectures, Types, Features, and Applications in Computing..... | 3  |
| Definition and Function .....                                                      | 3  |
| Architectures.....                                                                 | 3  |
| Features .....                                                                     | 4  |
| Hardware Requirements.....                                                         | 4  |
| Advantages .....                                                                   | 4  |
| Scalability .....                                                                  | 4  |
| Security .....                                                                     | 5  |
| Compatibility.....                                                                 | 5  |
| Use Cases .....                                                                    | 5  |
| II) IP Addressing: Foundations and Applications in Networking.....                 | 6  |
| Definition and Function .....                                                      | 6  |
| Types of IP Addresses .....                                                        | 6  |
| Features and Considerations .....                                                  | 7  |
| Hardware Requirements.....                                                         | 7  |
| Advantages .....                                                                   | 7  |
| Limitations and Challenges .....                                                   | 7  |
| Applications in Networking.....                                                    | 7  |
| III) Network Testing and Troubleshooting Techniques: A Comprehensive Guide.....    | 9  |
| A. Connectivity Tests: .....                                                       | 9  |
| B. Bandwidth Testing .....                                                         | 9  |
| C. Packet Loss Testing: .....                                                      | 9  |
| D. Security Testing: .....                                                         | 9  |
| E. Common Connectivity Issues and Troubleshooting: .....                           | 9  |
| Systematic Troubleshooting Steps: .....                                            | 10 |
| IV) Virtual Network Configuration .....                                            | 11 |
| The different issues I had during this project:.....                               | 14 |

## I) Hypervisors: Architectures, Types, Features, and Applications in Computing

The advancement of virtualization has significantly changed the IT environment, allowing for better resource allocation and enhanced adaptability in managing infrastructure. Central to this transformation are hypervisors, crucial software that coordinates the operation of virtual machines (VMs) on a sole physical server.

### Definition and Function

A hypervisor, also referred to as a Virtual Machine Monitor (VMM), is a software abstraction layer positioned between the physical hardware and VMs. Each VM operates with its own operating system and applications, essentially acting as a standalone computer without impacting other VMs.

**Two types of hypervisors are distinguished:**

#### 1. Type 1 Hypervisors (bare metal):

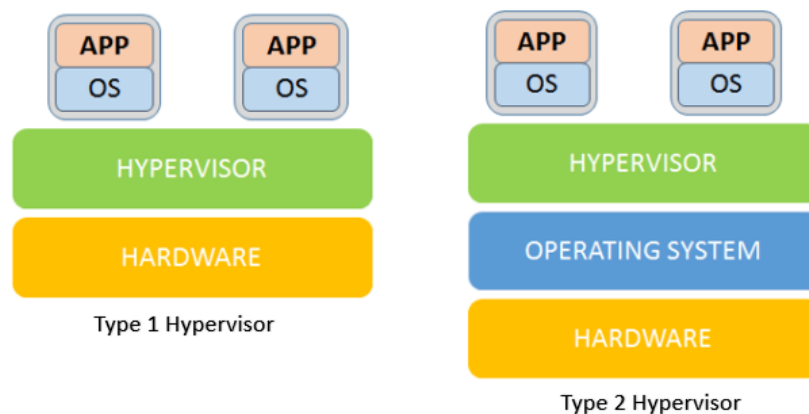
A type 1 hypervisor is installed and runs directly on the physical hardware. It permits optimal performance and improves security. The type 1 hypervisor seems to be the preferred solution for critical and high-performance environments. VMware ESXi, Microsoft Hyper-V, KVMv are some.

#### 2. Type 2 Hypervisors (hosted):

On the other hand, type 2 hypervisor runs as an application within a host operating system. It is easier to install and manage. However, it may exhibit slight performance drops and dependence on the host operating system. Here are few examples, VMware Workstation, VirtualBox, Oracle VM VirtualBox

### Architectures

- **x86 Architecture:** The most common and compatible with a lot of hardware and operating systems
- **ARM Architecture:** More and more popular in mobile devices and low power servers
- **PowerPC Architecture:** Used in some upmarket servers



## Features

- **Processor Virtualization:** Enables multiple virtual machines (VMs) to utilize a single physical processor, thereby maximizing resource utilization and efficiency.
- **Memory Virtualization:** Ensures that each VM has its own dedicated virtual memory, providing isolation and flexibility in managing memory resources.
- **Storage Virtualization:** Grants each VM its own virtual storage space
- **Network Management:** Allows VMs to communicate with each other and the external world
- **Backup and Restore:** Permits backing up and restoring VM states

## Hardware Requirements

- **Processor:** Must be compatible with the hypervisor architecture and powerful enough for all VMs
- **Memory:** Adequate memory to fulfil all VM needs
- **Storage:** Sufficient storage to hold all VM operating systems and data

## Advantages

- **Increased Efficiency:** Maximize server resource usage by sharing computing power and memory across VMs
- **Flexibility and Scalability:** Easily deploy and manage VMs based on requirements, scaling capacity up or down as needed
- **Reduced Costs:** Diminish hardware expenses by requiring fewer physical servers
- **Enhanced Security:** Isolate VMs from each other for improved security and confidentiality

## Scalability

- **Type 1 Hypervisors:** Offer better scalability due to handling a large number of VMs
- **Type 2 Hypervisors:** Scalability limited by the host operating system

## Security

Type 1 hypervisors are generally more secure as they run directly on the hardware while type 2 hypervisors can be more vulnerable to attacks due to dependence on the host operating system.

## Compatibility

- Type 1 hypervisors are typically compatible with a wide range of hardware and operating systems
- Type 2 hypervisors may be less compatible due to reliance on the host operating system

## Use Cases

- **Server Virtualization:** Increase server capacity and reduce costs by hosting multiple virtual servers on a single physical machine
- **Software Development and Testing:** Create isolated testing environments for each project without affecting the main system
- **Virtual Desktop Infrastructure (VDI):** Provide users with personalized and secure work environments accessible from any device
- **Cloud Computing:** Cloud providers use hypervisors to host and manage VMs for their clients

Hypervisors have revolutionized computing by enabling more efficient use of resources, greater flexibility and reduced costs. Their varied architectures, types, features and applications meet a wide range of needs in different fields.

In addition to the benefits mentioned, the adoption of hypervisors contributes to the advancement of the IT architecture. They facilitate the deployment of scalable and secure infrastructures that meet the growing demands of the modern digital landscape.

However, it is essential to consider the limitations of each type of hypervisor based on specific needs. Understanding the architecture, features and hardware requirements is critical to choosing the best solution for your particular use case.

As virtualization continues to grow, hypervisors will continue to play a critical role in optimizing digital infrastructure and creating a more efficient and flexible computing environment.

## II) IP Addressing: Foundations and Applications in Networking

The digital world thrives on connectivity, facilitated by a unique addressing system known as IP addressing. Just like addresses guide us to physical locations, IP addresses route data across networks, ensuring information reaches the intended destination. This comprehensive guide delves into the core concepts of IP addressing, exploring its architectures, types, features, and diverse applications in various networking scenarios.

### Definition and Function

An IP address, short for Internet Protocol address, acts as a unique identifier assigned to each device connected to an IP network. It functions like a digital postal code, enabling devices to locate and communicate with each other across the vast expanse of the internet.

**Two prominent IP address architectures exist:**

#### 1. IPv4 (Internet Protocol version 4):

- The most widely used architecture, represented by a 32-bit number divided into four octets (e.g., 192.168.1.1).
- Offers a finite address space, leading to the depletion of available addresses.

#### 2. IPv6 (Internet Protocol version 6):

- The next-generation architecture, utilizing 128-bit numbers for a significantly larger address space.
- Gradually being adopted to address the limitations of IPv4.

### Types of IP Addresses

Static IP addresses are permanently assigned to a specific device, ensuring consistent connectivity and simplifying network administration tasks. On the other hand, dynamic IP addresses are automatically assigned by a DHCP server, which allows for more flexible allocation of resources and more efficient use of available addresses. Public IP addresses are globally unique identifiers accessible from the Internet that facilitate external communication with devices or networks. Conversely, private IP addresses are used in internal networks and are not directly accessible from the Internet, which enhances security by separating internal traffic from external access. Each type of IP address serves distinct purposes in network management, balancing factors such as reliability, flexibility, accessibility and security to suit specific organizational needs.

## Features and Considerations

- **Subnet Masks:** Define the network portion and host portion of an IP address, enabling network segmentation and efficient routing.
- **Default Gateways:** Act as the primary router in a network, directing outbound traffic to the correct destination.
- **DNS (Domain Name System):** Translates human-readable domain names into corresponding IP addresses, simplifying user experience.

## Hardware Requirements

The physical requirements of the network infrastructure encompass a variety of components that are essential for smooth communication and data transmission. Network Interface Cards (NICs) are physical components that are integrated into devices and have unique Media Access Control (MAC) addresses that work together with IP addresses to facilitate network communication. These network cards act as intermediaries between devices and the network, allowing data exchange through wired or wireless connections. Additionally, routers play a crucial role as devices that are responsible for directing data packets across networks based on their IP addresses. By effectively managing traffic flow, routers ensure fast and accurate data delivery to specified destinations, thereby improving network performance and connectivity. Together, network cards and routers are vital elements of the network infrastructure, establishing the groundwork for reliable and efficient data transmission in modern digital environments.

## Advantages

- **Unique Identification:** Ensures clear identification of devices on a network, preventing communication conflicts.
- **Scalability:** IPv6 provides a vast address space, accommodating the ever-increasing number of connected devices.
- **Flexibility:** Dynamic IP allocation allows efficient resource utilization and simplifies network management.
- **Security:** Private IP addresses enhance security by restricting direct access from the public internet.

## Limitations and Challenges

- **IPv4 Depletion:** The limited address space of IPv4 poses challenges for future growth and expansion.
- **IPv6 Adoption:** The transition from IPv4 to IPv6 requires infrastructure upgrades and compatibility considerations.
- **Security Threats:** IP spoofing and other malicious activities highlight the need for robust security measures.

## Applications in Networking

- **Internet Access:** Enables devices to connect to the internet and access online resources.

- **Intranet Communication:** Facilitates communication within internal networks for sharing resources and collaboration.
- **Cloud Computing:** Underpins the delivery of cloud services, allowing users to access applications and data remotely.
- **Virtualization:** Enables the creation of virtual machines with their own IP addresses, optimizing resource utilization.

IP addressing plays a crucial role in connecting devices and enabling communication across the digital realm. By understanding the different structures, categories, characteristics and uses of IP addressing, individuals and organizations gain the ability to use networking technologies efficiently. As the Internet advances, IP addressing will remain an essential component, constantly adapting and pioneering to meet the growing demands of our interconnected world.

### III) Network Testing and Troubleshooting Techniques: A Comprehensive Guide

Maintaining a healthy and reliable network is crucial for any organization today. Effective network testing and troubleshooting techniques are essential for identifying and resolving issues before they impact productivity and user experience. This guide delves into various testing methodologies, addressing common connectivity problems, and providing systematic troubleshooting approaches.

#### A. Connectivity Tests:

The ping is a fundamental tool that verifies basic connectivity between two devices by sending and receiving data packets. It helps identify network hops and potential latency issues. Traceroutes traces the path taken by packets to reach a destination, revealing potential bottlenecks or routing problems.

ICMP (Internet Control Message Protocol) tools is Utilized for advanced diagnostics, including ping sweep (identifying active devices on a network) and path MTU discovery (determining the largest possible packet size).

#### B. Bandwidth Testing:

Bandwidth testing involves assessing the speed and performance of your internet connection through various tools. One common method is conducting bandwidth speed tests, which compare the actual throughput of your connection to its advertised speed.

#### C. Packet Loss Testing:

Packet Loss Testing involves several methods. Ping with a packet loss option measures the percentage of packets not received, indicating potential network congestion or hardware issues. MTR (MuttTraceroute) combines traceroute with packet loss information, aiding in pinpointing the location of packet loss along the network path.

#### D. Security Testing:

Security Testing encompasses various techniques. Port Scanning identifies open ports on devices, revealing potential vulnerabilities. Tools like Nmap and Nessus are commonly utilized. Vulnerability Scanning checks for known software vulnerabilities on network devices and systems, with tools like OpenVAS and Qualys Vulnerability Management Platform being popular options. Penetration Testing simulates real-world attacks to assess network security posture and identify exploitable weaknesses.

#### E. Common Connectivity Issues and Troubleshooting:

- **IP Address Conflicts:** Ensure devices have unique IP addresses within the network subnet. Use tools like Angry IP Scanner or Advanced IP Scanner to identify duplicates.
- **DNS Resolution:** Verify DNS server settings and functionality on devices. Tools like nslookup and dig can diagnose DNS issues.

- **Firewall Configurations:** Check firewall rules to ensure authorized traffic is allowed and unauthorized traffic is blocked. Review firewall logs for suspicious activity.

#### Systematic Troubleshooting Steps:

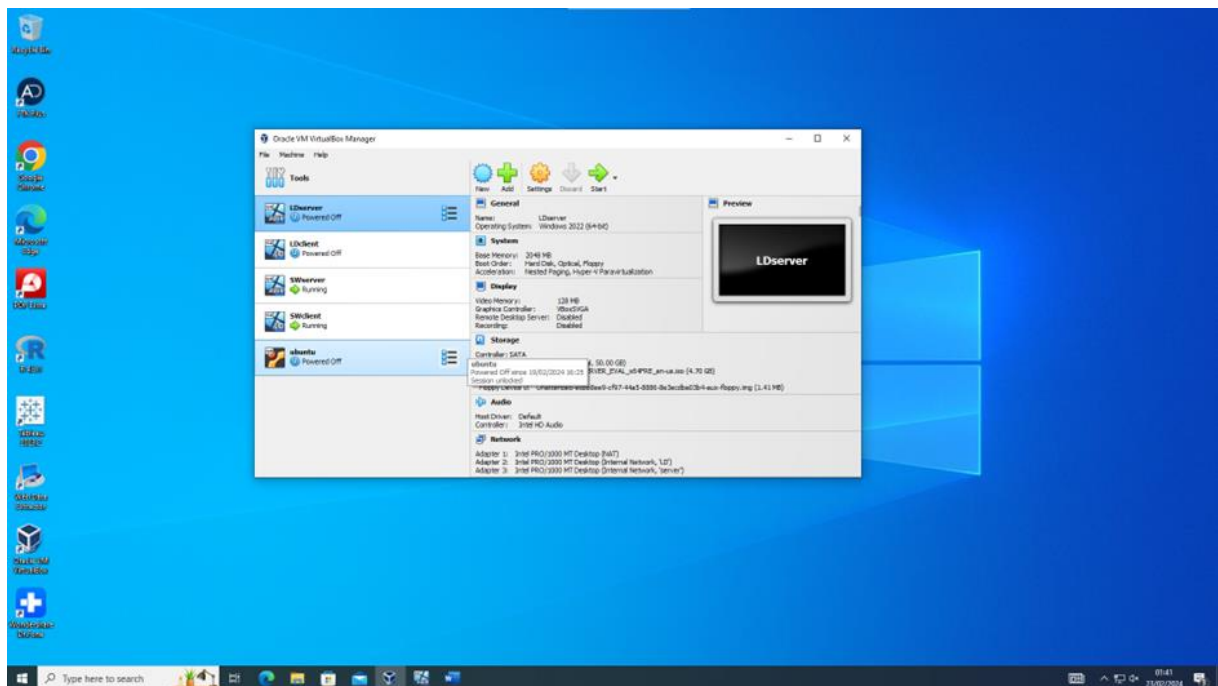
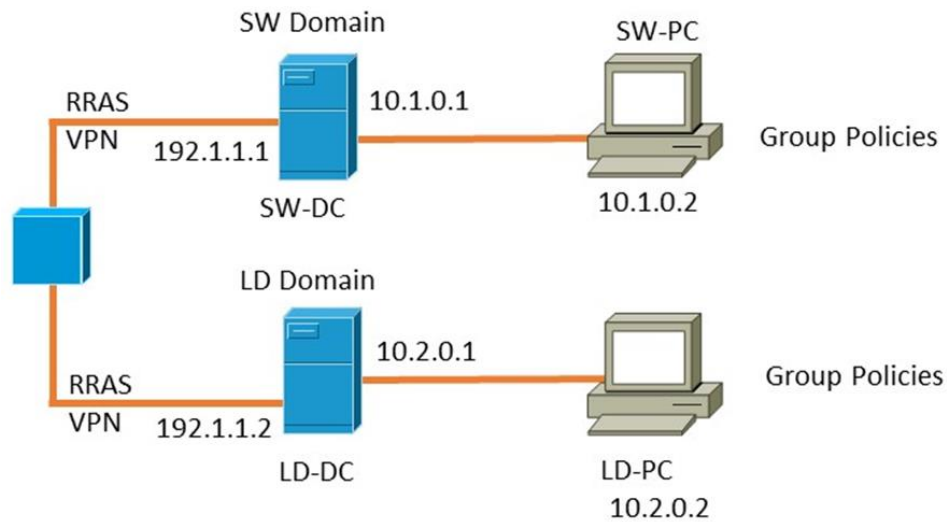
1. **Gather Information:** Document symptoms, affected devices, and network layout.
2. **Isolate the Problem:** Use testing tools to narrow down the issue's scope (e.g., specific device, network segment).
3. **Research and Analyze:** Consult documentation, online resources, and community forums for potential solutions.
4. **Implement Changes:** Adjust carefully, documenting each step for rollback if needed.
5. **Verify and Test:** Confirm the fix resolves the issue and monitor for recurrence.

Effective network testing and troubleshooting require a combination of tools, knowledge, and systematic approaches. This guide provides a foundational understanding of various techniques and addresses common connectivity issues. By leveraging these resources and developing strong troubleshooting skills, you can ensure your network operates smoothly and efficiently.

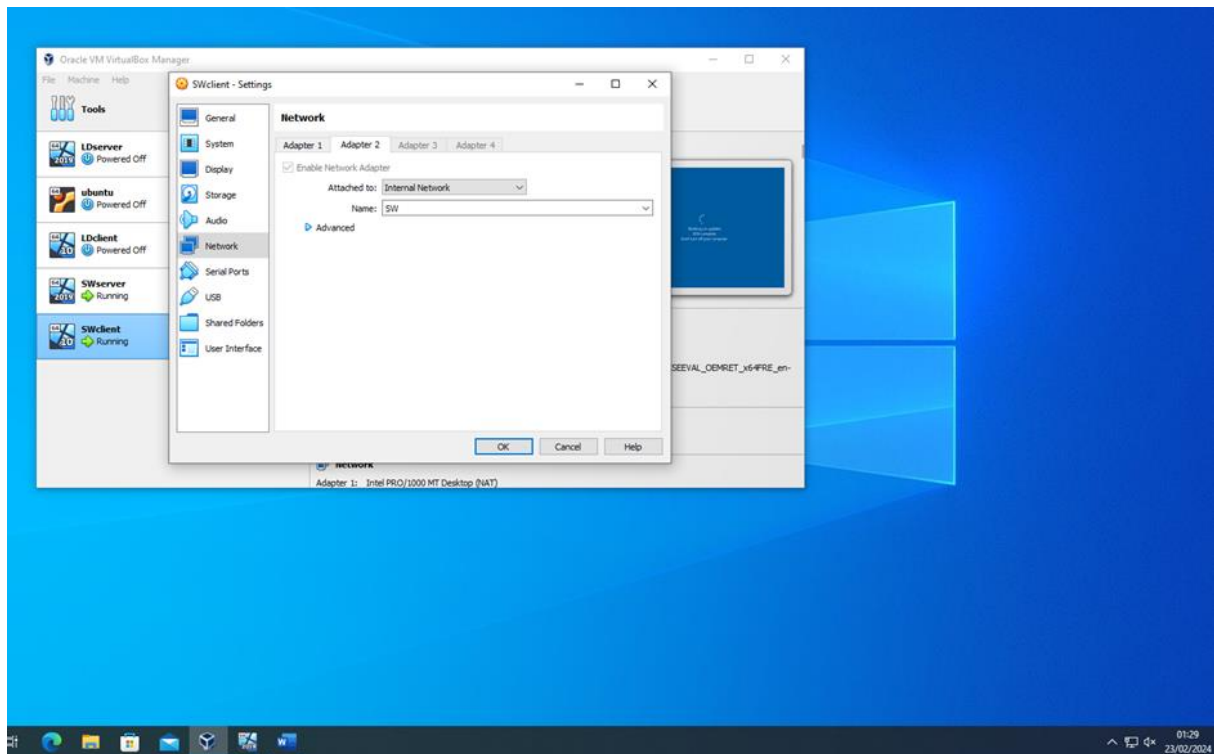
## IV) Virtual Network Configuration

First thing first, we need to install a Hypervisor, Let's take VirtualBox.

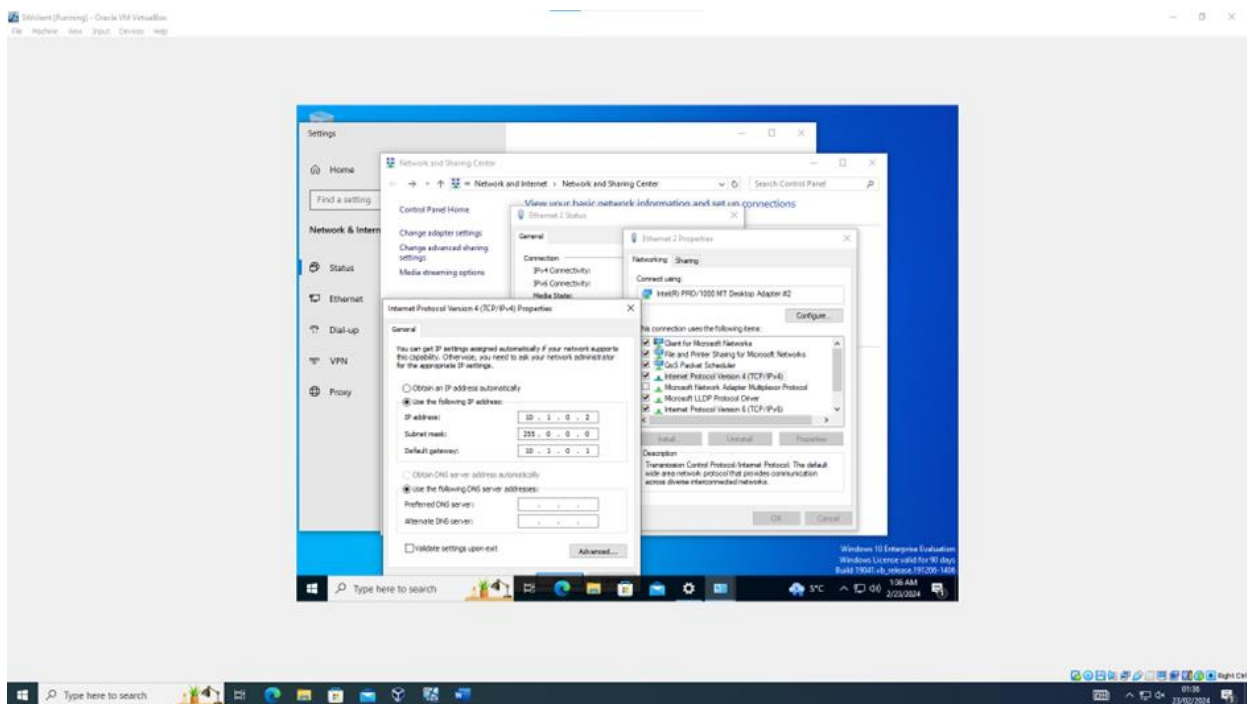
We must create 4 virtual machines, two servers and two clients to recreate this scheme.

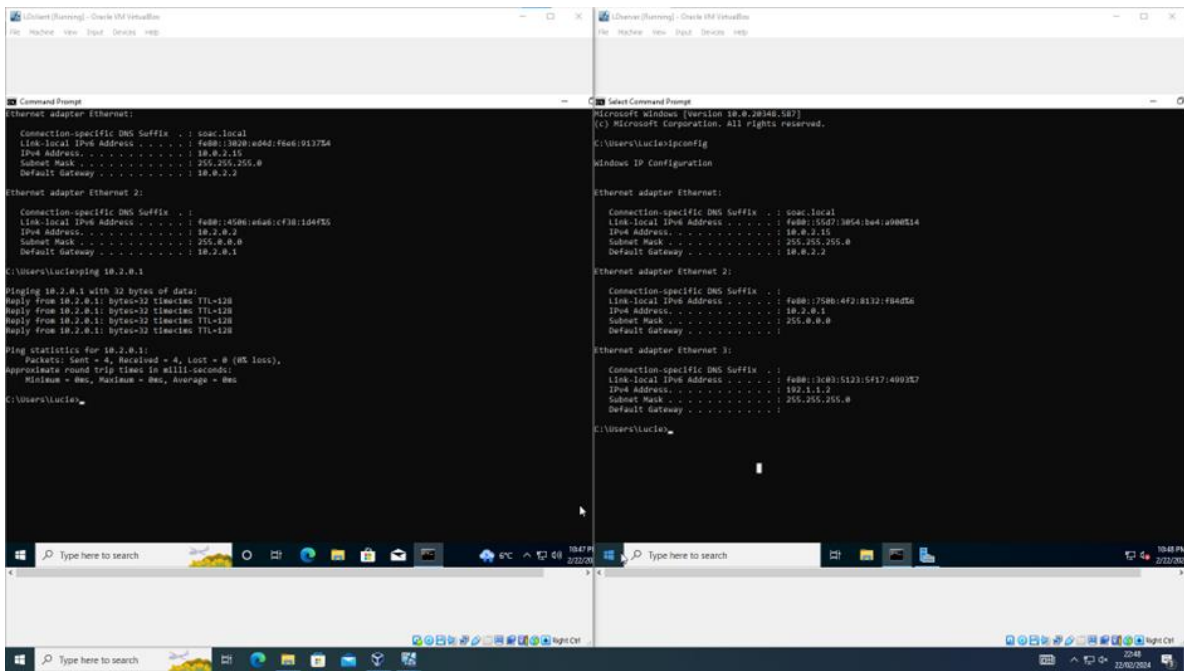


Once these virtual machines created, we need to setup the servers and clients.

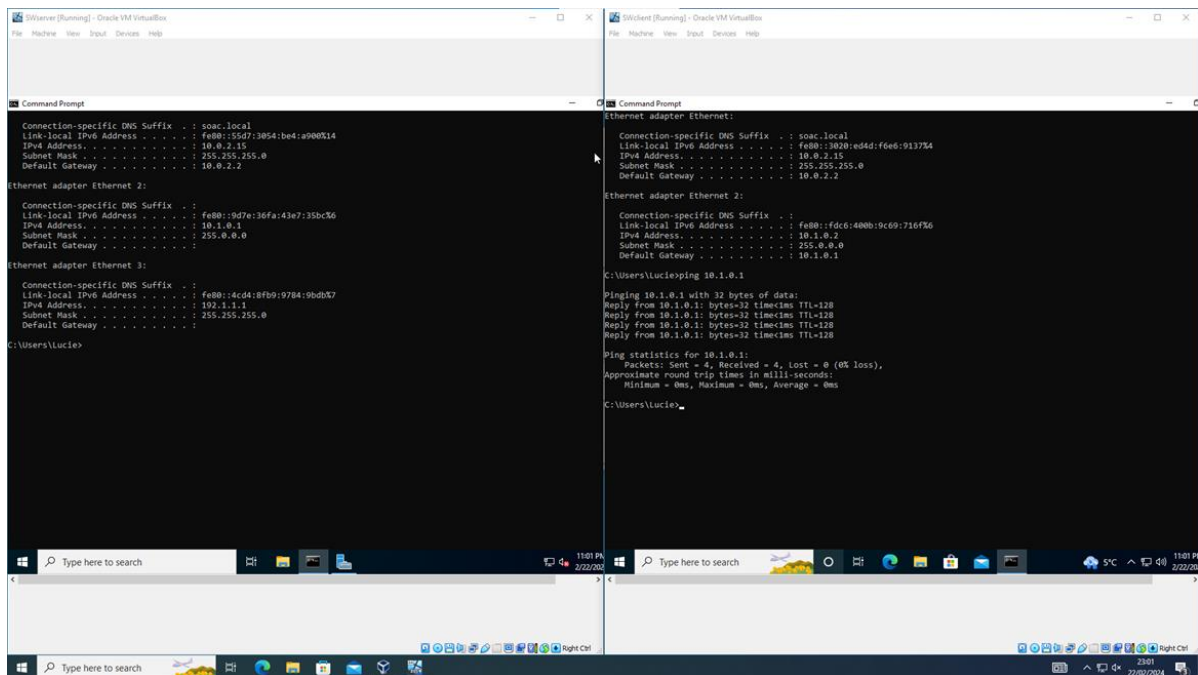


Following the topology, we connect the LD server with the LD client by putting the right IP addresses, we do the same for the SW client and SW server. To see if it worked, we ping the server in the client.

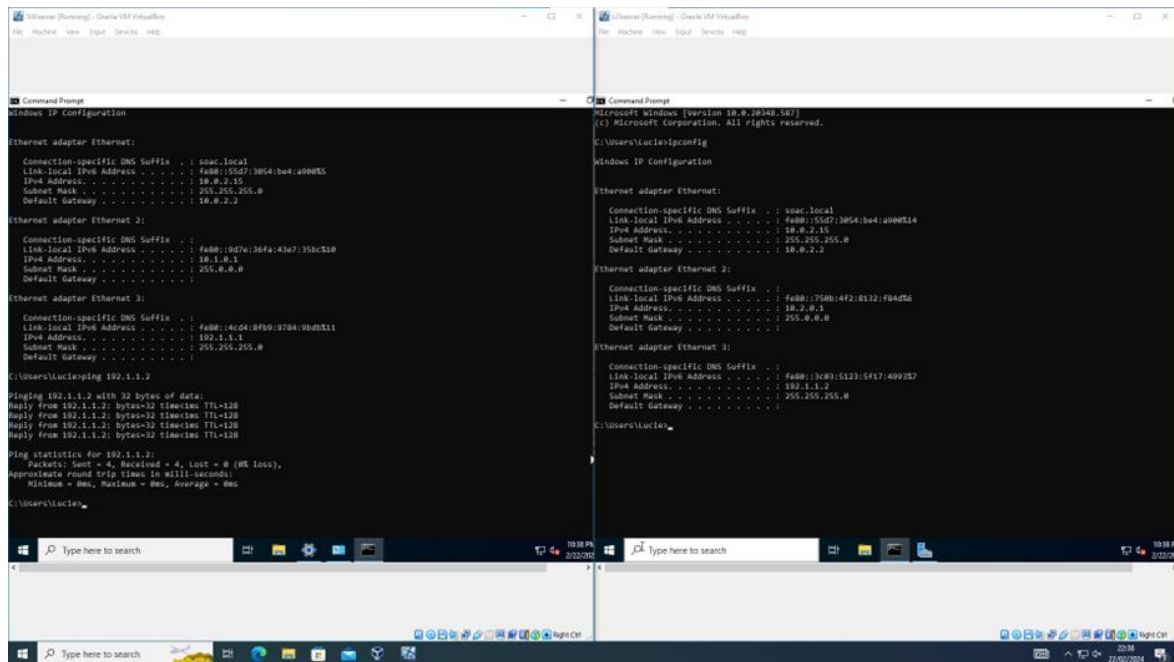




## LDserver and LDclient connection + ping



## SWclient and SWserver



Then we link the two servers together to finalize the network using the same method.

### The different issues I had during this project:

First, I had to start all over again due to the lack of storage space in my own laptop, I also had difficulties because of the slowness of my computer.

I worked on a computer in the lab and reinstall all the ISO for my virtual machines. I put all the virtual machines on an external hard drive to import them on the Uni computer more easily.