Thomas QIAN

TASK 1

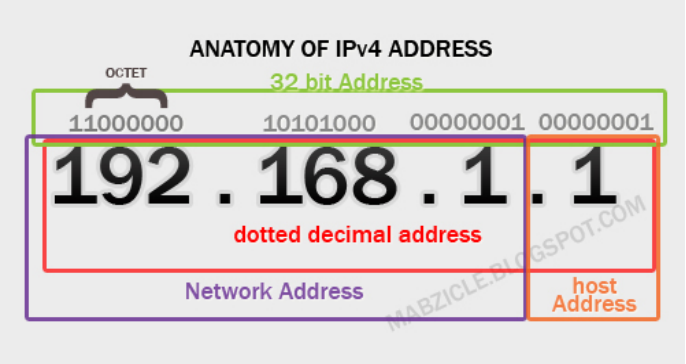
30/01/2025 - 06/02/2025 – Research on IP Addressing

+ **Research on IP Addressing:** (Maximum: 400 Words)
  Refer to your Group Activity during one of your lectures asking you to discuss in a group about
  - How does data get from one computer to another on the Internet and what is the role of IP addresses in the transmission of data on the Internet?
  - How do you think routers and switches work on the Internet to facilitate the flow of data between different networks?

Based on the above Group Activity, reflect your understanding with appropriate and adequate in-text citations on IP Addressing.

- Explore how IP Addressing contributes to the functionality and effectiveness of the network.
- You need to address the structure, format, and representation of IPv4, IPv6 addressing, concept of subnetting, efficient utilization of IP addresses.
- Include diagrams and examples of IP Addressing concepts and their practical applications.

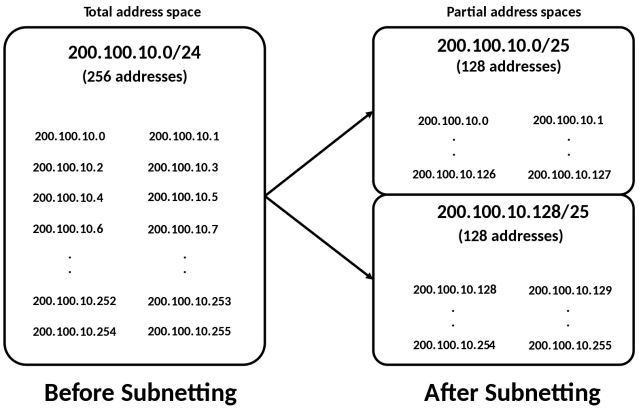
Data travels on Internet divided into packets using a protocol called TCP/IP [0], ensuring communication by data packets to devices identified by unique IP addresses. This method is divided into 4 different layers: Application layer (HTTP, FTP etc. Protocols), Transport (TCP, UDP), Internet (IP, ICMP) and Network access (Ethernet, Wi-Fi...). Routers and switches are components connecting devices together on the Internet. Switches permits communication on a local network, where routers let it connect to the Internet. They facilitate the flow of data because they determine the most optimal way for data to travel to their destination.



IP Addressing enables efficient data location and retrieval thanks to identification, and uses 2 main types of representation: IPv4, a 32-bit address going from 0.0.0.0 to 255.255.255.255 but its combinations are almost all used, which explain the transition to IPv6 [1], a 128-bit long address with different types of IP: Public (accessible all over the internet), Private (Used for devices within private networks), Static (Fixed and manually assigned) and Dynamic (Automatically assigned and can change). Those addresses are given automatically by a protocol call "DHCP" (Dynamic Host Configuration Protocol). Subnetting [2] involves dividing a network into smaller subnetworks to improve performance, reduce broadcast traffic, and

efficiently allocate IP addresses *[3]*. It permits the limitation of broadcast transmission (emitter sending data to every device under a network without differentiation) that can cost a lot of resources if it's not well considered.

For a better utilization of IP addresses, it's possible to manage them to ensure more connectivity, security, and scalability *(larus.net) [4]*. There are many practices used for IP Address management such as planning subnetting using CIDR notation (Classless Inter-Domain Routing, classless routing compatible protocol giving 256 addresses to an IP, for example from 1.255.1.0 to 1.255.1.255) and giving separate addresses for different networks or departments in an enterprise for a more efficient resource utilization and a scalability support. In informatics, it's said that a router is doing network address translation when it's connecting an IP address to other addresses.



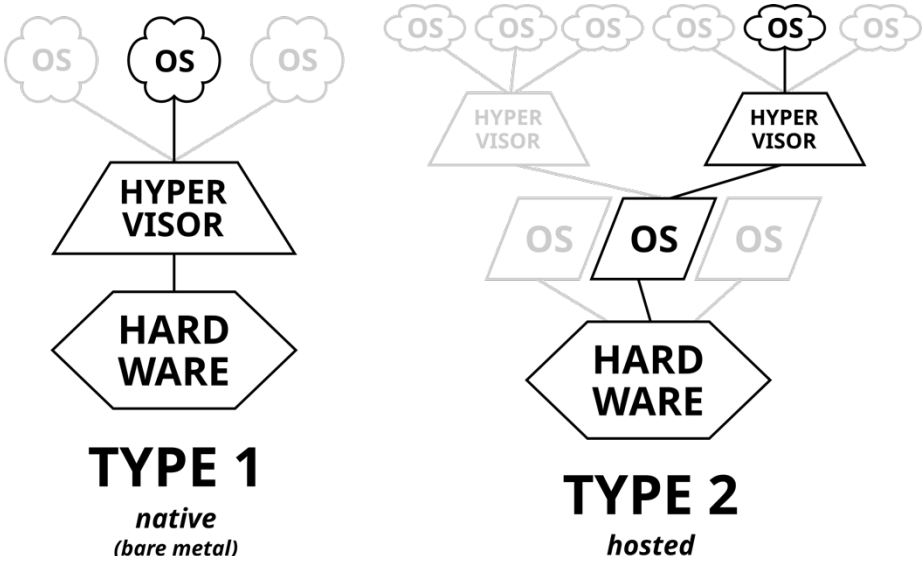
[0] (Microsoft) https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj573587(v=ws.11)
[1] (Cisco) https://ipcisco.com/lesson/ipv4-vs-ipv6/
[2] (SolarWinds) https://www.solarwinds.com/resources/it-glossary/subnetting
[3] (Michel Bakni) https://en.wikipedia.org/wiki/Subnet
[4] (larus.net) https://larus.net/blog/best-practices-for-managing-ip-addresses/#:~:text=Effective%20planning%20involves%20organizing%20IP,utilization%20and%20supports%20future%20scalability.
[] (Oracle) https://www.oracle.com/uk/cloud/networking/ip-address-insights/
[] (mabzicle.blogspot.com) https://thecybersecurityman.com/2017/12/29/ip-addresses-version-4/

13/02/2025 – Research about Hypervisor architecture

+ **Research on Hypervisor:** (Maximum: 400 Words)
    - ***Do detailed research*** on different types of hypervisors in virtualization.
        - Discuss about their architecture,
        - address their features,
        - hardware requirements,
        - advantages,
        - scalability, security and compatibility.
        - Find out details about different types of hypervisor solutions available in the market.

A hypervisor is a type of computer software that allows the creation of virtual machines (VM). It's classified by two types: type-1 hypervisors which executes on a hardware as a control tool of the operating system, and type 2 hypervisors that runs directly inside the operating system as a "host" to create sub-operating systems called "guests".

Type-1 hypervisors have a use of being between the material and virtual machines taking directly resources such as memory or CPU. Here, a type-2 is depending on the operating system to use the resources. Compared to type 1, it is more powerful and efficient, with the cost to use a physical material. They are used in most professional areas compared to type 2 hypervisors, which are less efficient but simpler, cheaper and can be used for tests. To create virtual machines, a type-1 hypervisor has some requirements: Type-1 hypervisors require at least one modern 64-bit CPU with hardware virtualization support (SLAT), a RAM with a great memory of 4 GB and a fast storage system where type-2 hypervisors needs a computer allowing visualization to be produced, a compatibility "VT-x/AMD-V" activated in the BIOS (Basic Input/Output System software in the computer) with a random access memory between 2 and 4 GB.



Hypervisors allow the use more of a system's available resources and to stock them in a more efficient (faster data retrieval) and secure way (data viability). Type-1 hypervisors offer better isolation, reducing security risks by preventing VMs from directly interacting with host operating systems. Type-2 hypervisors rely on host OS security, being slightly less secured. The bests type-1 hypervisors that you can find on the market are VMware vSphere, that offers an advanced resource management with automation tools, and Microsoft Hyper-V, that comes up with Windows Server being free and efficient without licensing restrictions. For type-2 hypervisors, you have Oracle VM Virtualbox, VMware and Parallels. The choice of those hypervisors depends on the device, budget and space you have.

18/02/2025 - Network Services

+ **Research on Network Services:** (Maximum: 300 Words)
    - **Do detailed research to summarize the key concepts, features and best practices associated with**
        - VPNs,
        - DHCP,
        - Active Directory Domain Services and
        - Certificate Authorities.

In short, Network Services are informatically services that facilitate gestion, communication and security of networks thanks to methods such as VPNs, DHCP, ADDS and CA. VPNs (Virtual Private Network) permits the creation of secured connections of a user to Internet by encrypting data, protecting confidentiality and communication. It's mostly known to hide the IP address online, give access to another geographic location content without restrictions and to safely connect to work company's network at home [].

DHCP is, as explained, a service that automatically attributes IP addresses, gateway and DNS to devices of a network, avoiding the need to have a manually given IP address. It's efficient since it avoids the use of the same IP address and can give a new one to each connection of a device.

ADDS (Active Directory Domain Services) is a Microsoft service that manages users, computers, employees of a companies, or groups and resources of a Windows' network thanks to an Active directory. It permits authentication and access control on a network. And is hierarchically organized thanks to branch-like system (such as domains, forests, and trees).

Certificate authorities are entities (such as people or tools) that are used to allow one's identity on a device. They are mainly used to secure numerical communications such as email or in-web protocols (such as HTTPS, where authorities such as "Let's Encrypt" can give free certificates). It's also useful in recognition in numerical documents where digital signatures (keys) are secured.

[] (Microsoft) https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn#:~:text=A%20VPN%2C%20which%20stands%20for,and%20firewalls%20on%20the%20internet.

13/02/2025 – Research on Routing

+ **Research on Routing:** (Maximum: 400 Words)
    - **Do detailed research** on
        - the fundamental concepts of routing protocols,
        - including how they work, their role, what is their purpose etc.
        - Focus on the key differences between static and dynamic routing protocols.
        - Refer to real-world examples and/or case studies on how routing protocols are deployed in a real time network.
        - Analyse different routing protocols used in network scenarios and reflect on the benefits and challenges on each routing protocols based on those scenarios.

Simply put, routing protocols are essential rules that permit routers to determine the best path for data to be transported in packets from one point to another inside a network, permitting efficiency and safe information sharing on a local network or Internet. Each router uses a routing table / data table that traces paths towards different destination points of a network, making easier to solve troubleshooting network issues []. The protocols used uses specific algorithms to optimize and reduce latency, but also to respond to breakdowns or in-network traffic increase.

```
---------------------------------------------------------------------------

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0         10.0.0.1        10.0.0.32     35
         10.0.0.0    255.255.255.0         On-link         10.0.0.32    291
        10.0.0.32  255.255.255.255         On-link         10.0.0.32    291
       10.0.0.255  255.255.255.255         On-link         10.0.0.32    291
         127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
         127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link         10.0.0.32    291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link         10.0.0.32    291
===========================================================================
Persistent Routes:
  None
```

Routing table – TechTarget

Key differences between static and dynamic routing protocols are linked to security and usability factors. Static routing are paths manually configured by an administrator. They are safer since they don't need automatic updates and easier to control in a stable environment but limited since it lacks flexibility and requires a more complex maintenance when a network is being edited. Where dynamic routing protocols are automatized tools that adjusts paths in function of a network's updated status (such as Routing Information Protocol that is one of the most used ones thanks to its simplicity and needs less resources in a domestic network []) but are more difficult to configure.

In real world, big companies use OSPF (Open Shortest Path First) protocol in intern networks that take charges of processors state (Intranet) to quickly process changes of it. For example, Amazon AWS uses it in its Intranet to ensure connectivity of its data centers. A BGP (Border Gateway Protocol) is used to make Internet suppliers connect with each other, making it essential on whole world Internet scale. It has caused for example, Facebook's breakdown in 2021 because of a bad BGP configuration that removed its path from the global network []. In short, protocol choices are crucial in real life uses and depends on the type of network, its scale and its needs.

[] Cisco Press - https://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=12

[] TechTarget - https://www.techtarget.com/searchnetworking/definition/Routing-Information-Protocol

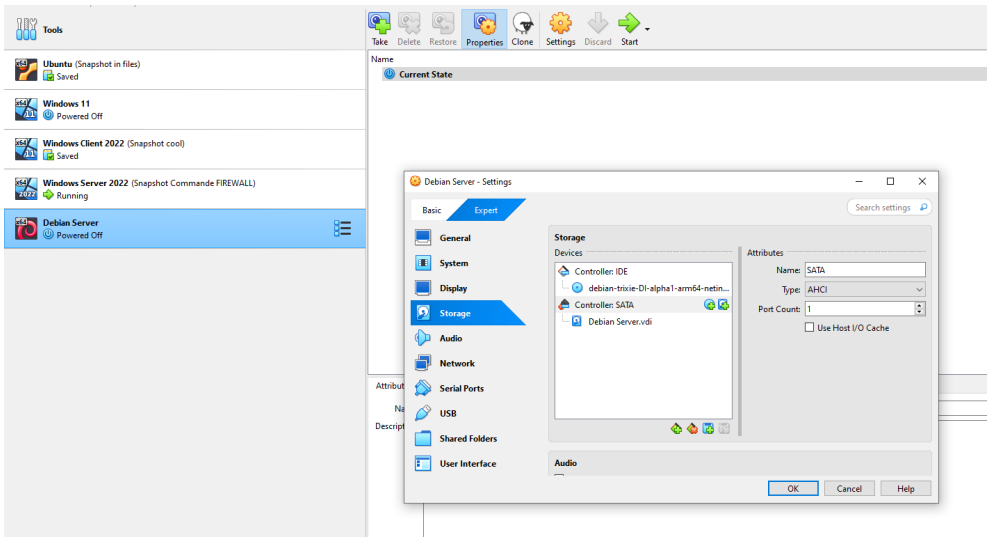
[] Wikipedia - https://en.wikipedia.org/wiki/2021_Facebook_outage

TASK 2

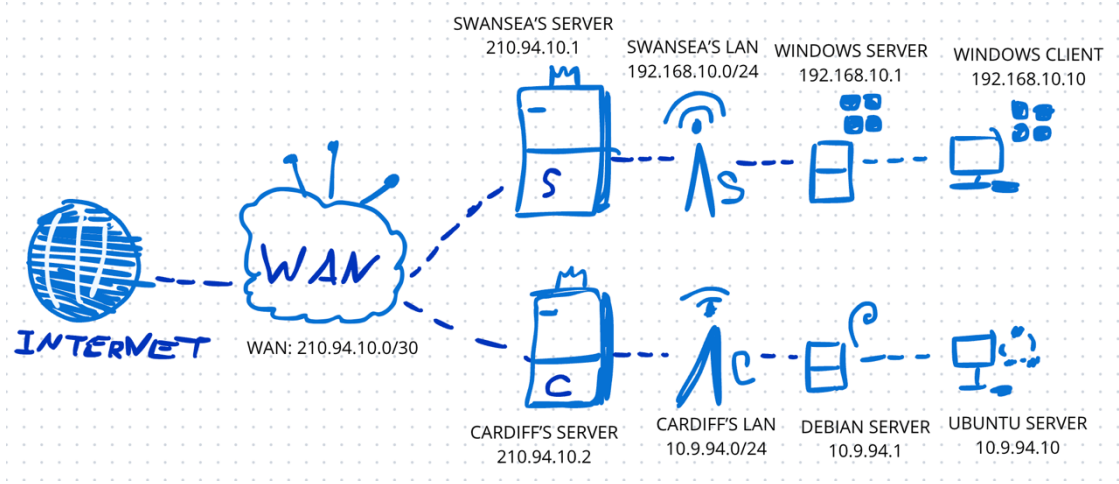
2.1. Choice of the Hypervisor

The Hypervisor used in my case was Oracle VM VirtualBox, which is known to have a good performance, a powerful virtualization system, and is a free virtual machine license. It was useful in our task because we needed to use different operating systems. To start doing virtualization, Windows 11 was first used to ping between its server and client on “Swansea’s LAN”. It has a simpler interface to configurate since it includes multiple visual configuration tools than Linux and less in-depth knowledge to be understood. For Linux’s configuration, I used a Debian Server and a Ubuntu Client on “Cardiff’s LAN”, since Debian is commonly used as a server thanks to its stability and control, where Ubuntu is mostly used as a client since it’s a preferred choice for developing and tests.

2.1. Download and Setup – 2.3 IP addressing

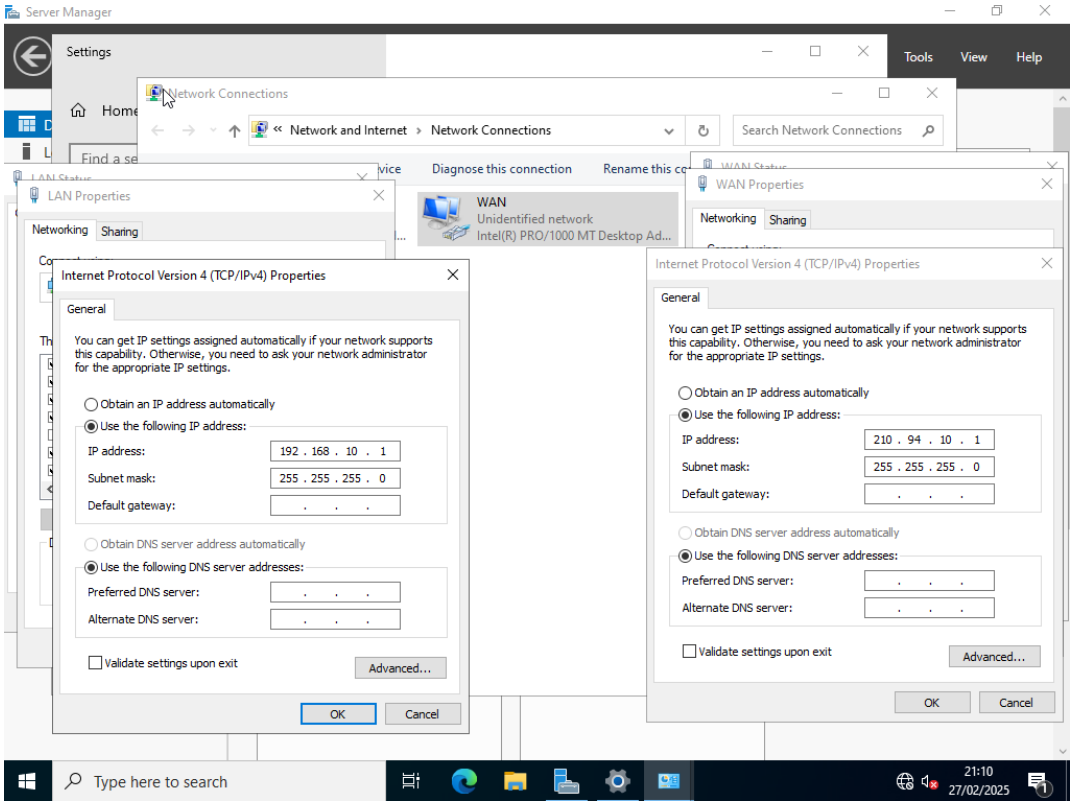


First servers & client’s configuration – 20/02/2025 at 18:09



Scheme of the topology

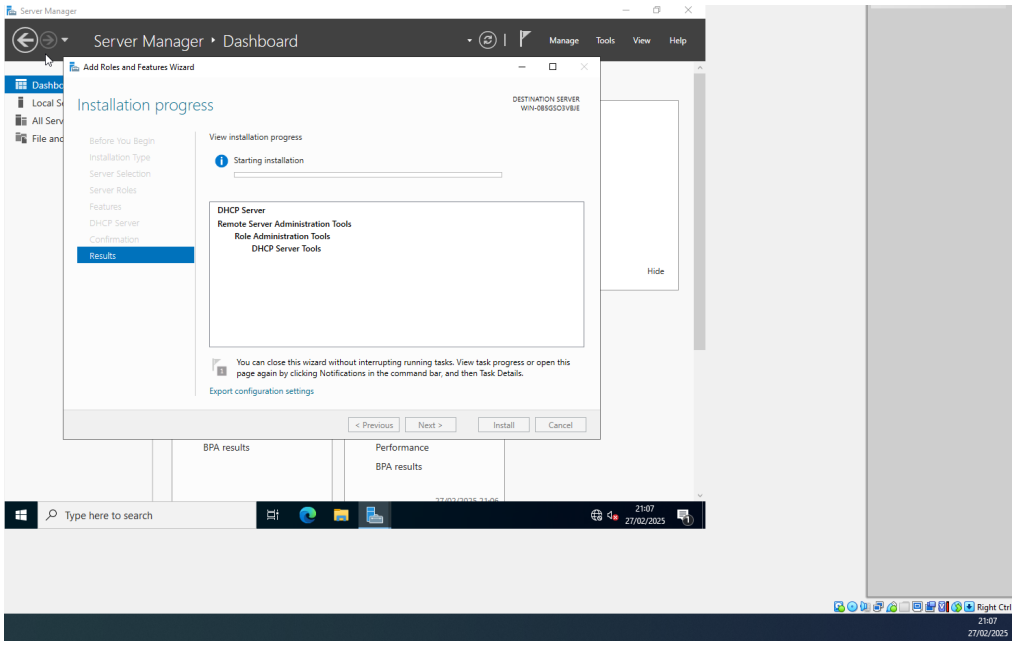
Here's how the topology was configured with the IP address configuration: Each server is composed of 3 network cards. It has a LAN that permits local communication with clients, WAN permits connection between the servers for external routing, and the Internet, where a NAT can give access to it (even if we use an Internal Network at first for this work).



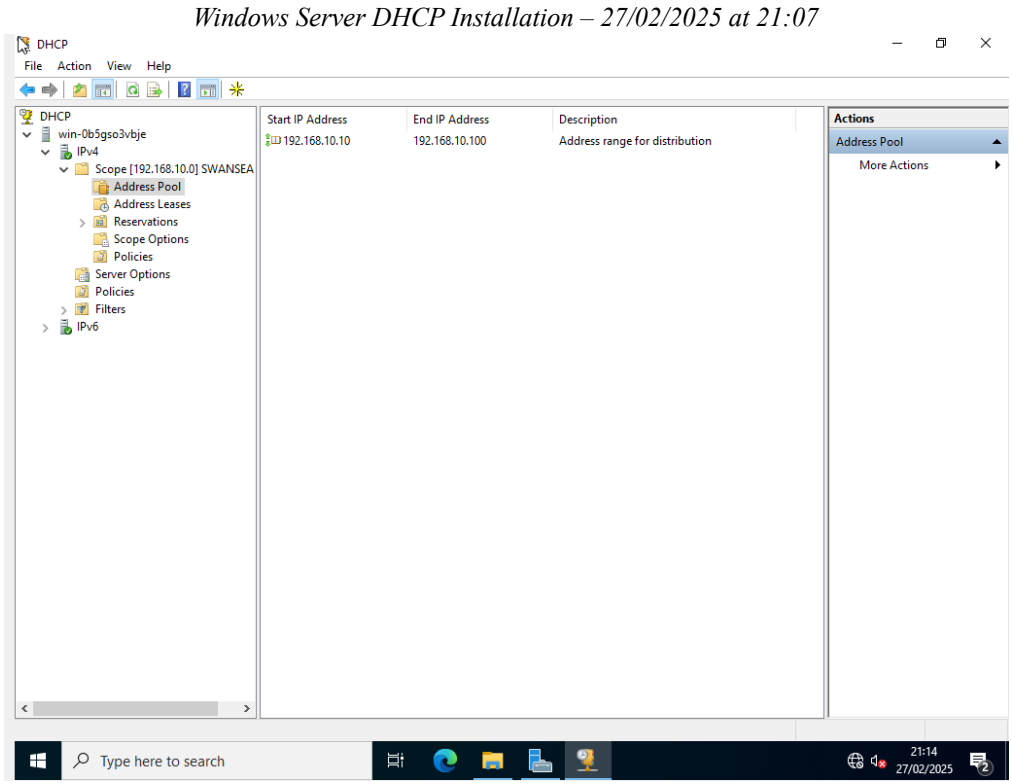
Windows Server IPv4 manual configuration – 27/02/2025 at 21:10

We have a **Swansea LAN (192.168.10.0/24)** composed of a Windows Server (192.168.10.1) and a Windows Client (192.168.10.10). It was configured manually inside LAN properties in Windows, by changing both IPv4 addresses.**Cardiff LAN (10.9.94.0/24)** is composed of a Debian Server (10.9.94.1) and an Ubuntu Client (10.9.94.10) . Both LAN are connected on their respective servers : Swansea's LAN on its local server (210.94.10.1) and Cardiff's on it Server (210.94.10.2) are both connected on the wider network **WAN (210.94.10.0/30)**, that links all the centers together to the Internet.

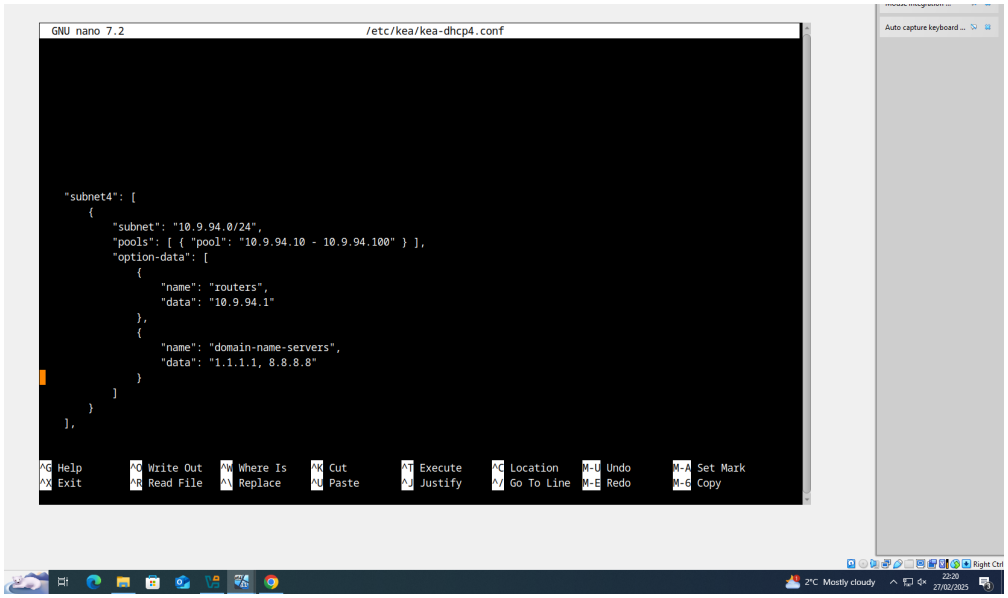
Here, our servers acts with a DHCP protocol even if we manually changed (Static) and gateway towards the clients that are still connected to their networks, where their IP are defined. That's the case for both Windows and Ubuntu clients, here's the given IP after the protocol defined. In our case, DHCP aministrator allowed us to give addresses from a range of 192.168.10.10 to192.168.10.100 for Windows clients, where Debian used a package called "kea-dhcp4-server" to be configured. Similarely, Cardiff's network got to use addresses from 10.9.94.10 to 10.9.94.100.



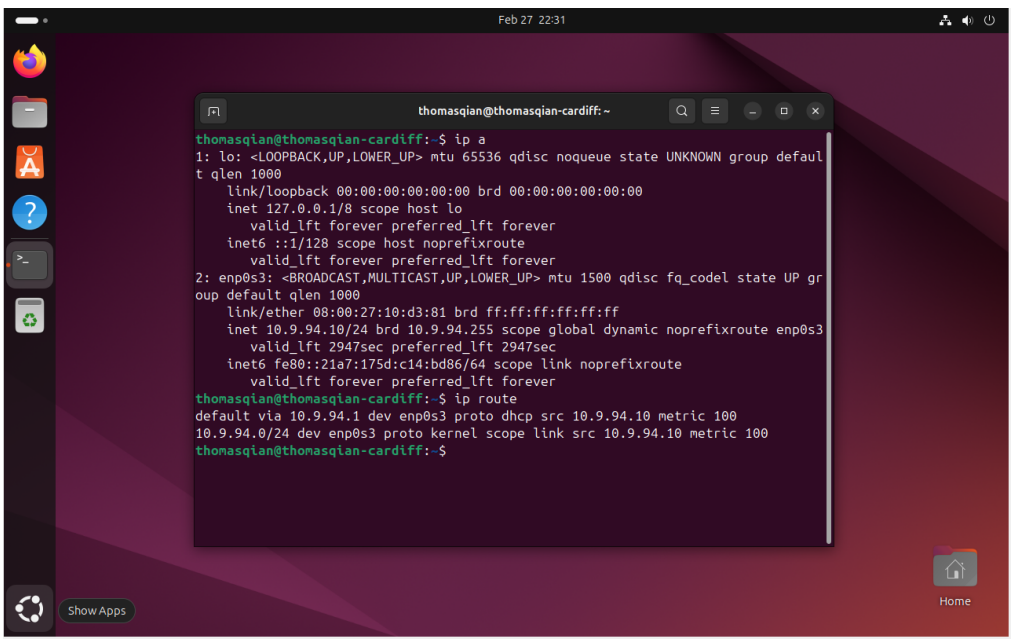
Windows Server DHCP Installation – 27/02/2025 at 21:07



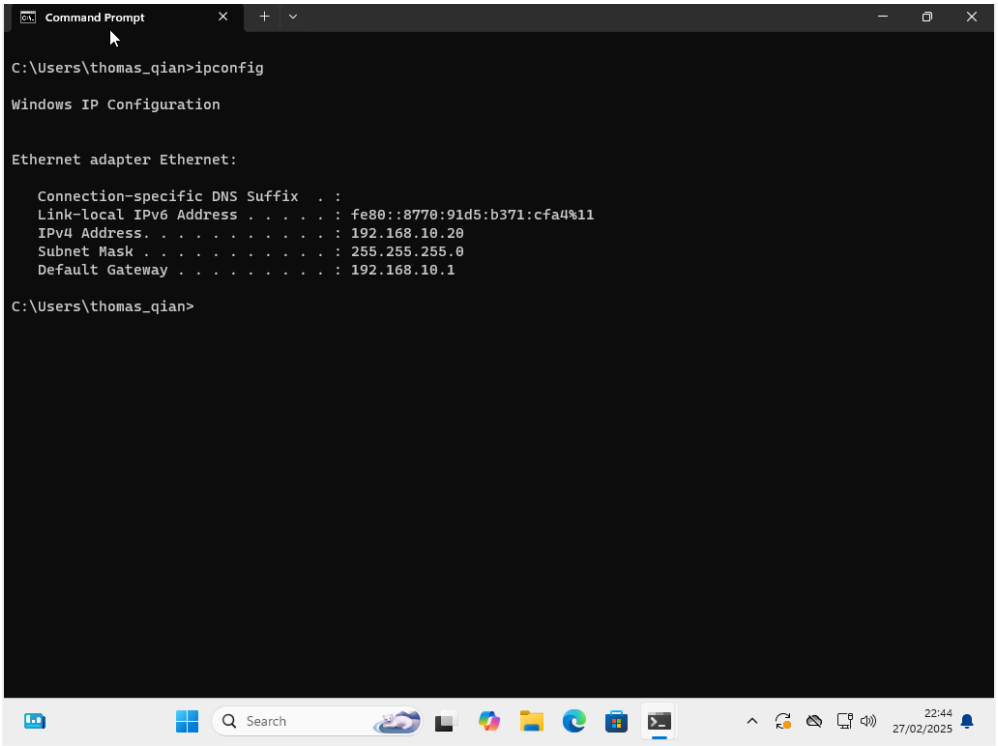
Windows Server DHCP Configuration – 27/02/2025 at 21:14



Kea-dhcp4 on Debian configuration – 27/02/2025 at 22:20



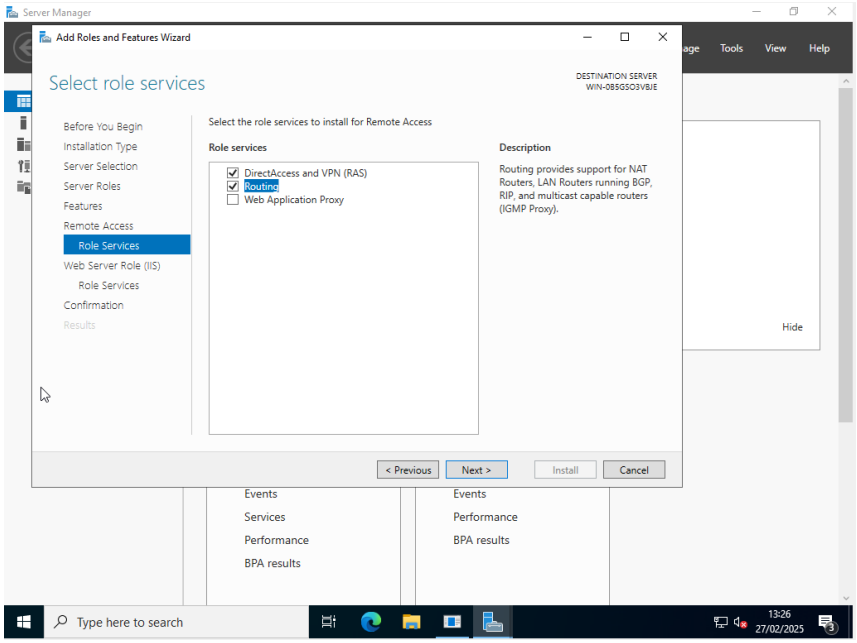
Ubuntu given IP after DHCP configuration – 27/02/2025 at 22:31



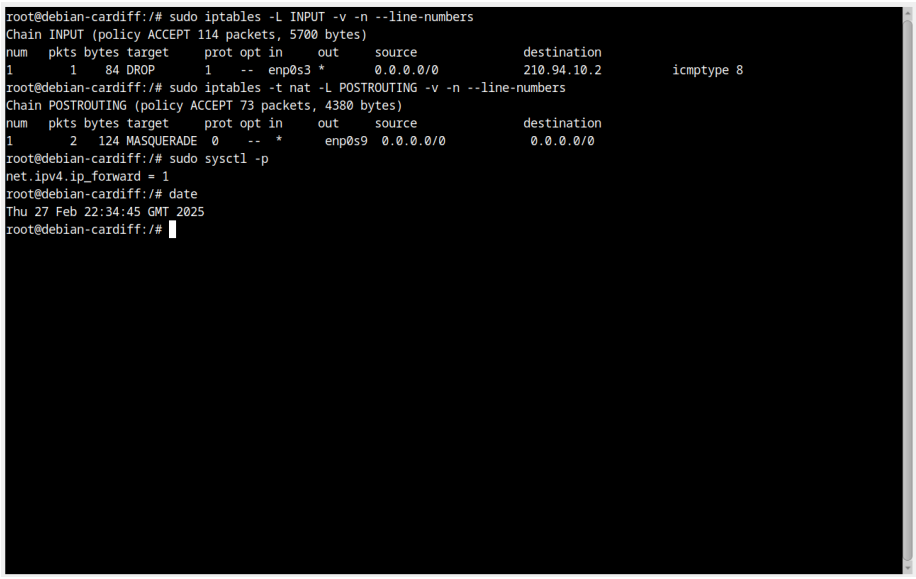
IP configuration automatically attributed via DHCP – 27/02/2025 at 22:44

The advantages to use a DHCP in our situation is the fact that we gain time because we won't have to configure manually for future clients and reduces human errors when there will be an editing in the future.

Then, we start to install a NAT on both servers to allow Internet connection for the clients (Gateway). On Windows Server, we give access to users connected to Swansea's network. Debian Server got configured thanks to IPtables and IP forwarding/netting techniques. The objective here is to allow access to all machines to naviguate on Internet by keeping a fluid and safe connexion on the whole server.



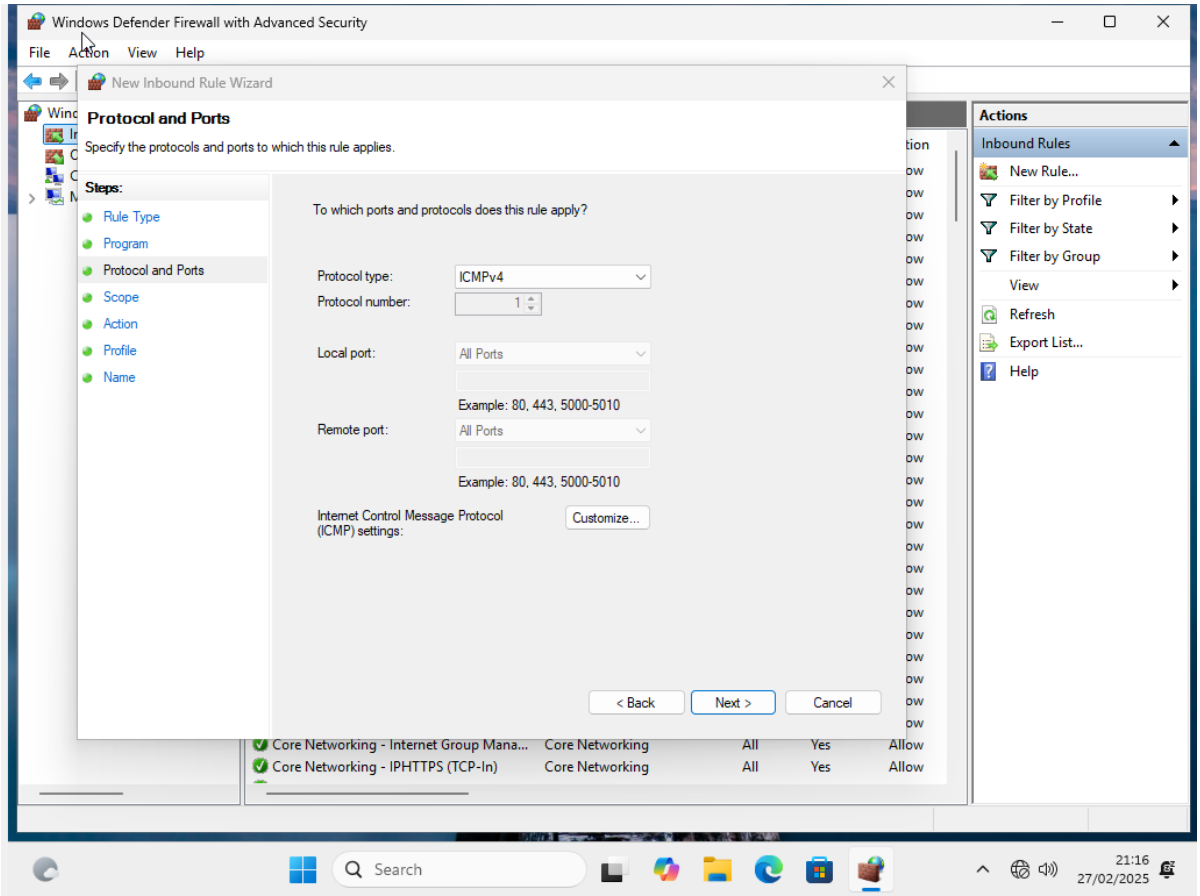
NAT installed on Windows Server – 27/02/2025 at 13:26



```
root@debian-cardiff:/# sudo iptables -L INPUT -v -n --line-numbers
Chain INPUT (policy ACCEPT 114 packets, 5700 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        1    84 DROP       1    --  enp0s3 *       0.0.0.0/0            210.94.10.2          icmptype 8
root@debian-cardiff:/# sudo iptables -t nat -L POSTROUTING -v -n --line-numbers
Chain POSTROUTING (policy ACCEPT 73 packets, 4380 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        2   124 MASQUERADE  0    --  *      enp0s9  0.0.0.0/0            0.0.0.0/0
root@debian-cardiff:/# sudo sysctl -p
net.ipv4.ip_forward = 1
root@debian-cardiff:/# date
Thu 27 Feb 22:34:45 GMT 2025
root@debian-cardiff:/#
```

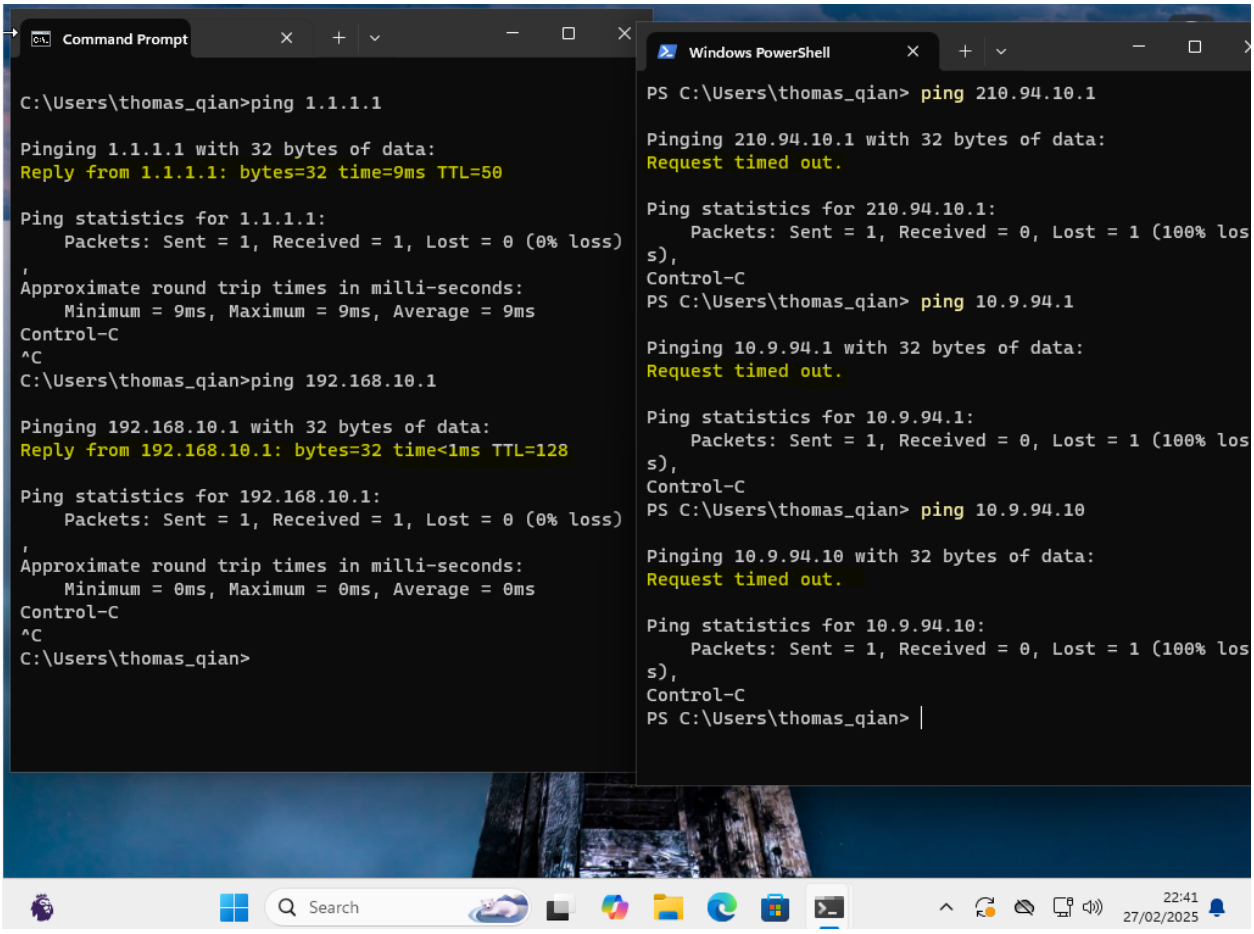
NAT configuration on Debian (Internet on Cardiff) & IP forwarding – 27/02/2025 at 22:34

The configured firewall was also necessary to allow ICMPv4 to emit pings from the machines on Windows server, where Debian and Ubuntu can have a temporary firewall disabling.



Firewall Configuration for Windows Server, ICMPv4 Protocol Ruling – 27/02/2025 at 21:16

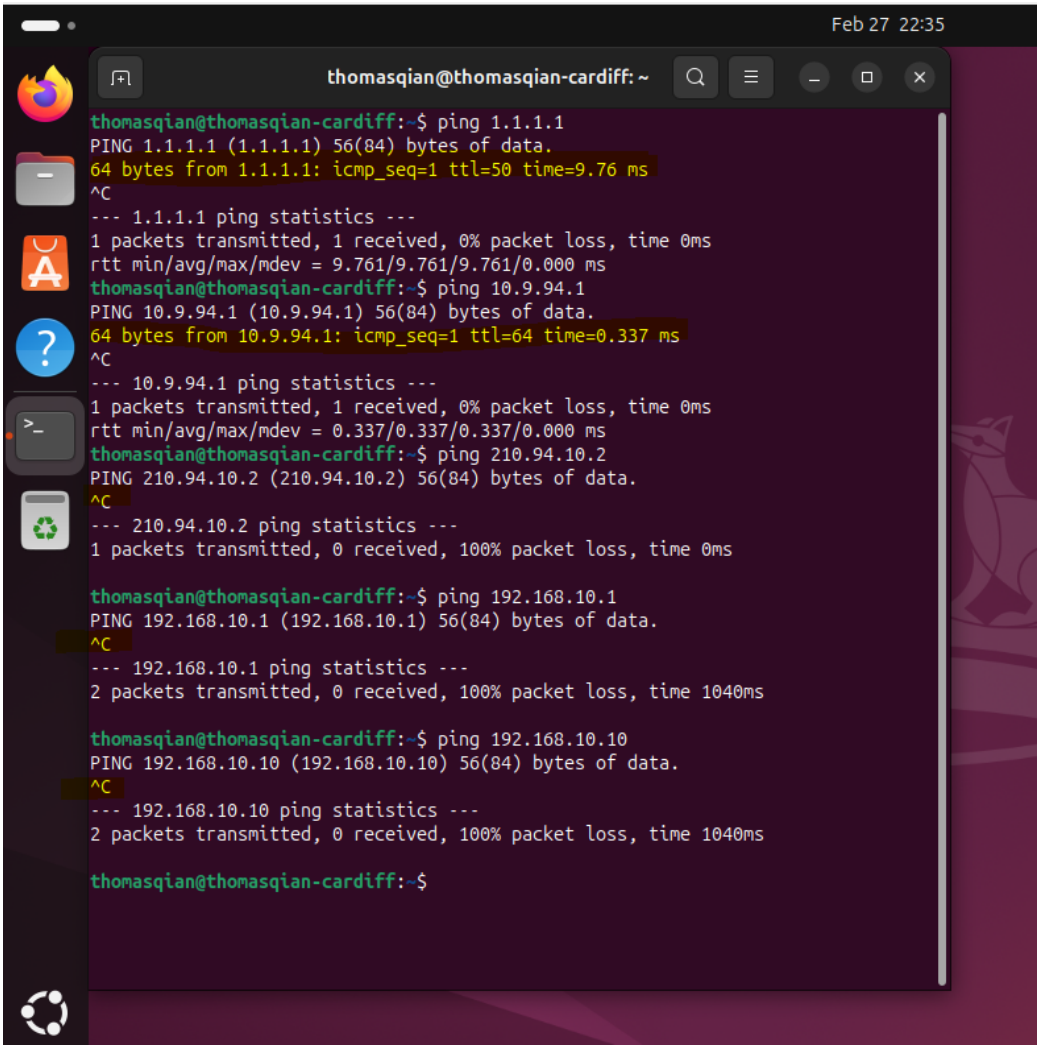
2.4. Connectivity Tests & Troubleshoot



Windows Final successful pings – 27/02/2025 at 22:41

Here's the results of the pings: we have successfully ping 1.1.1.1, a public IP address commonly used to test Internet connection. It shows that our client can access to it and that the NAT on Swansea's server works correctly at that the firewall allows traffic towards outside the local network. Ping towards its server 192.168.10.1 is working since they are in the same subnet (LAN), and Windows firewall is correctly configured to allow pings.

For the unsuccessful pings, 210.94.10.1 is not working since it's Swansea's server address on the WAN, but that's not the case of the client that is not directly connected to it, and the Windows server does not allows those kind of request between LAN and WAN. It's same case for 10.9.94.1's ping fail since Swansea and Cardiff's LANs are not routed to each other, same situation for the Ubuntu client where there's not routing between the networks.



Ubuntu Final Successful pings – 27/02/2025 at 22:35

Here, we can see that Ubuntu also successfully send packages to 1.1.1.1, meaning a good NAT configuration on Cardiff's server and its firewalls. It can also ping its server 10.9.94.1 (Debian) since they are in the Cardiff LAN. Packets are lost for the same reasons as Windows when it tries to ping 210.94.10.2, where it does not directly go from the LAN to the WAN and the not-shared subnet when it tries to ping Windows server and client.

We see that the connectivity in the network is successful thanks to a correct configuration of DHCP, of the NAT, and of the firewall. The tests that were done show that clients have a correct automatically designated IP addresses and that they can communicate with their servers. Some in-networks are unsuccessful but shows that security as network isolation is working.

TASK 3

I found that Task 2 was not easy to understand at first when we are not used to the subject. A part of the work was done a few weeks ago just to get a basic understanding of Linux and Windows' system settings, since it's not something that I usually do as activity on those kinds of devices. About the configurations, without DHCP protocol I was lost during the first configurations since it happened that I use some incorrect IPs. I got help about the firewall since I did the mistake to totally turn them off.