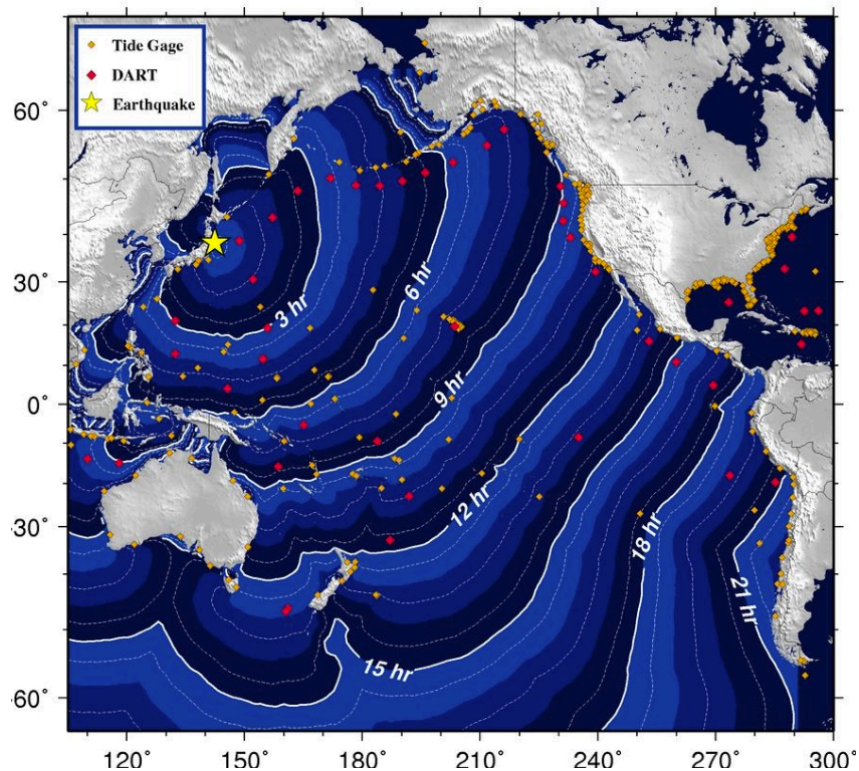


Institut supérieur d'électronique de Paris



2023 - 2024

Summary

1 Hypervisor	3
1.1 What is a hypervisor ?	3
1.2 Types of hypervisors	3
1.3 Architecture of a hypervisor ?	4
1.4 Resource management and Hardware restrictions ?	4
1.5 Comparison of security between the two types ?	5
1.6 Use case and hypervisor on the market ?	5
2 Research on IP addresses ?	6
	26
Conclusion	27

Chapter I

1 Hypervisor

1.1 What is a hypervisor ?

A hypervisor is a software used to create different virtual machines inside a physical machine. Each machine can be isolated from the others with their own environments with their own applications and own operating systems. The hypervisor allocates resources to the virtual machine by allocating parts of the hardware to each virtual machine like the core of the CPU and RAM.

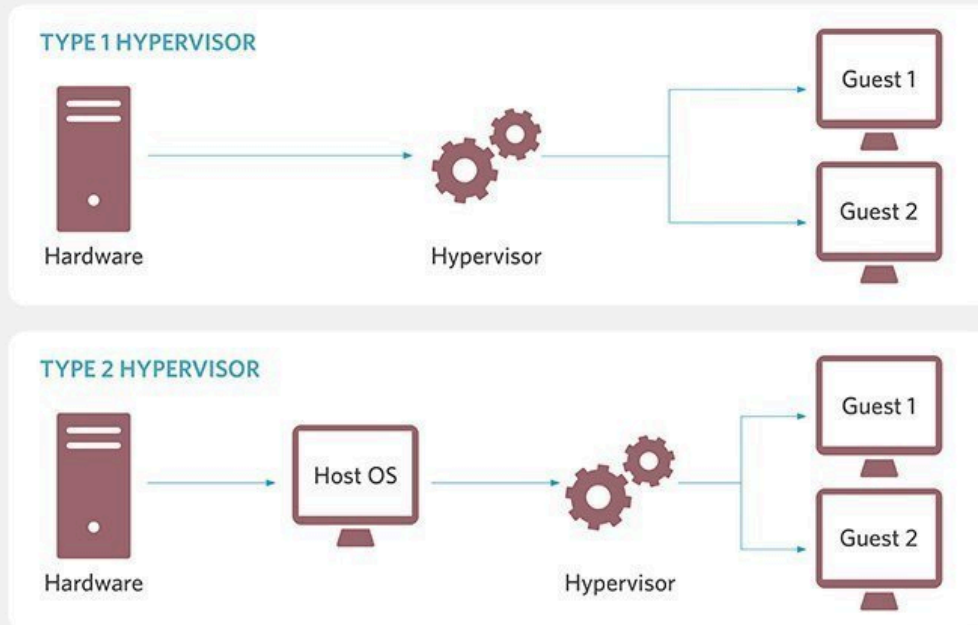
The use of a hypervisor has numerous advantages, one of them is that it offers a large flexibility. When you run a virtual machine on your computer, the virtual machine will be isolated and you can choose operating systems which are different from the one on your physical machine.

Another advantage of the hypervisor is that by creating multiple virtual machines on one physical machine, and allocating hardware resources efficiently, one machine can run multiple workloads, for a corporation, it can be time saving and money saving.

1.2 Types of hypervisors ?

The hypervisors have 2 categories, type 1 and type 2, The difference between them is that type 1 has direct access to the hardware resources, he is also named “bare metal hypervisor”. The type 2 hypervisor is an application installed directly on the host operating system, it is also named “embedded hypervisor” .

Hypervisor types



©2016 TECHTARGET. ALL RIGHTS RESERVED TechTarget

1.3 Architecture of a hypervisor ?

The architecture of a hypervisor plays a significant role in determining its performance, scalability, and flexibility. Type 1 hypervisors, being closer to the hardware, have direct control over system resources and can implement custom resource allocation strategies adapted to the specific requirements of virtual machines. On the other hand, Type 2 hypervisors are run on the host operating system for resource allocation, which can introduce issues and irregular performance in function of the operating systems.

In terms of features, both types of hypervisors offer a wide range of capabilities, including live migration, snapshotting, and resource pooling. However, the implementation and performance of these features may vary depending on the hypervisor type and vendor.

1.4 Resource management and Hardware restrictions ?

Each type of hypervisor has the same goal in the end but they do not get there in the same way, so there must be a difference between the two.

When the type 1 hypervisor directly communicates with the hardware resources, the type 2 needs to ask to borrow their resources from the operating system so by doing that, it slows down the process and reduces the efficiency of the operation.

The use of a type 2 hypervisor is much easier than a type 1 hypervisor, because type 2 is an application run on the operating system while the type 1 directly interferes with the hardware devices so requires a system administrators level knowledge.

The type 1 is much more performant than the type 2 because he has no intermediary, the type 2 has to pass by the application, the operating system when the type 1 is directly allocating the resources.

Type 1 and Type 2 use something called hardware acceleration support, this allows them to divide the task by sending data to specialized components instead of only relying on the CPU, like sending all video and image processing to a GPU (Graphic Process unit), it's like having co-workers, it allows you to gain time and have better results. Type 1 doesn't function without these technologies in the BIOS while Type 2 can use it if it's available but it's not an obligation.

1.5 Comparison of security between the two types ?

The type 2 hypervisor is more secure in our mind due to the fact that we can clearly see the separation between our physical machine and the virtual one on our screen but hypervisors (type1) that run directly on physical hardware are also highly secure. Virtualization mitigates the risk of attacks that target security flaws and vulnerabilities in OSES because each guest has its own OS. This ensures an attack on a guest VM is logically isolated to that VM and can't spread to others running on the same hardware. Type 1 hypervisors provide a higher degree of isolation for each virtual environment. There is no shared layer as there is with the operating system of a type 2. This makes virtual machines running on the type 1 hypervisor inherently more secure.

1.6 Use case and hypervisor on the market ?

Type 1 hypervisors are more often used in large enterprises who have a lot of workloads and need a lot of virtual machines with an optimal use of the resources like in data centers or web servers for example.

Type 2 have less knowledge requirements and a lower price, they are more efficient, they are used when you need a few virtual machines.

The most known and popular hypervisor type 1 is VMware VSphere, Microsoft HyperV and Xen.

VMware VSphere is essentially sold to enterprises who run data centers, and the high price (1000\$ to 4000\$ per machine) make it harder for small enterprises.

Microsoft HyperV is capable of running different virtual machines inside an admin virtual machine, it is used by developers to make tests on software by creating Virtual machines for each test.

For the hypervisor type 2, there is VMware Workstation, VirtualBox and Parallels Desktop.

VirtualBox is an open source hosted hypervisor that supports guest virtual machines. He can use a variety of operating systems for his virtual machine such as windows, Linux or Apple mac OS.

I choose to use Oracle VirtualBox for the following reasons:

- VirtualBox is an Open Source hypervisor so it's equal to free
- It's a Type 2 hypervisors so it's easier to use than a Type 1
- He offers a huge variety of Os support which in our project could be useful in the creation of our network.
- I have already used it a bit so I'm familiar with it even if it's been long since I have used it.

2 Research on IP addresses ?

An IP (Internet Protocol) address is an address that will make your device recognizable from the others, a unique address, this address can be different from network to network, your devices can be connected to internet and local network, and have a different IP address. An IP address contains location information and makes your devices accessible to communication. It allows us to make a difference between computers, routers, and switches. Every address is composed of 4 numbers separated by a dot and each number goes from 0 to 255, so it goes from 0.0.0.0 to 255.255.255.255 for example 192.168.1.68. The generation of the IP address is regulated by the Internet Assigned Numbers Authority (IANA) who produced them mathematically.

2.1 Understanding Data Transmission on the Internet

Description of the process of data transmission from one computer to another on the Internet.

The process of data transmission is mainly separated in two categories: the packet and the protocols.

When a computer wants to send data to another computer, he cannot just send the data in one block but the data will be divided in a small part named packet and will be reunified at the end. This packet contains two pieces of information: the data that we want and information about the data. The information about the data is being read before the data itself, because when the packet is being received by the receiving machine, she needs to know where to put the data like when we need to build Ikea furniture, the pieces are the data and the manual, the data information. On the internet, packets are composed of bits . The packets get routed to their destination by various networking devices such as routers and switches. When the packets arrive at their destination, the receiving device reassembles the packets in order and can then use or display the data.

They are a standard way to communicate between computers. It's what the protocols are, like IP addresses where every device has one. All ways of communication on the internet are common, that is why Internet-connected computers and other devices can interpret and understand these protocols, the Internet works no matter who or what connects to it.

Role of IP addresses in packet routing and delivery.

2.2 Functionality of Routers and Switches

The packets and protocols are not the only one who does all the job, there are also physical devices who have an important role like the routers and the switches. The routers guide the data packets to their IP addresses and allow multiple devices to use the same internet connection, it's most used on a large scale. The switches are used to interconnect devices; it's more used in internal or private networks.

2.3 Structure and Format of IPv4

- Detailed explanation of IPv4 addressing structure, including network and host portions.

Since his creation, the protocols IP have been upgraded multiple times but the most used nowadays is the IPv4 and resist to is new concurrent IPv6. IPv4 (Internet Protocol version 4). IPv4 addresses are 32-bit numbers that are typically displayed in dotted decimal notation. A 32-bit address contains two primary parts: the network prefix and the host number. In a single network, all the hosts share the same network address and each host has an address that represents themselves.

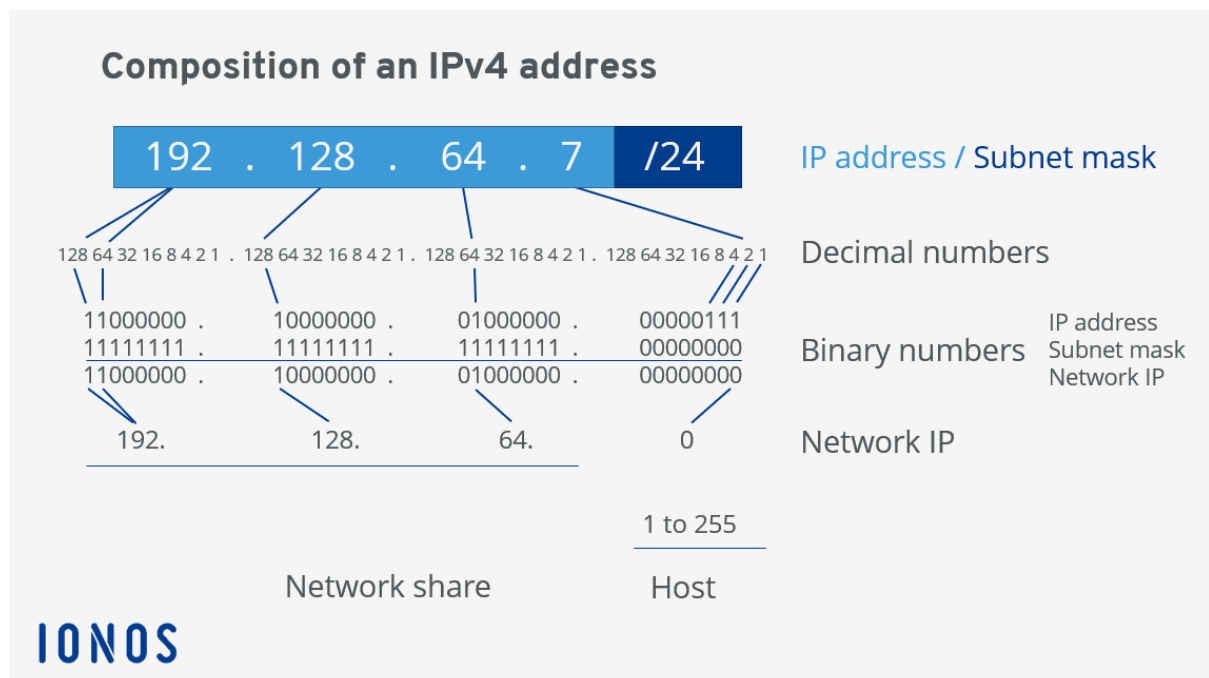
Depending on the scope of the network and the type of device, the address is either globally or locally unique. If the devices are connected to the Internet, he needs to have globally unique IP addresses and instead the ones who are visible only in the network need to have locally unique IP addresses.

- Discussion on the format of IPv4 addresses and subnet masks.

The IPv4 format is 32 bits where each octet (8 bits) is treated as a separate number and each octet is a number in binary that can be converted to decimal. I will explain with an example, the following IPv4 Addresses in bits: 00000001.00000010.00000100.00001000

In decimal will be: 1.2..4.8

The rightmost bit represents 2^0 (or 1), increasing to the left until the first bit in the octet is 2^7 (or 128).



The subnet mask is a 32 bits number to distinguish the networks and host part of an IPv4 address. It work with the IP address to know part of the address is dedicated to the network and which part is dedicated to the host

- Explanation of Classful and Classless addressing.

The classful address method was that IP addresses were originally divided into three different categories to provide flexibility in the number of addresses distributed on function of the size of the network: class A, class B, and class C. Each address class specifies a different number of bits for its network prefix and host number:

- Class A addresses use only the first octet to specify the network prefix, leaving 3 octets to define individual host numbers.

- Class B addresses use the first 2 octet to specify the network prefix, leaving 2 octets to define host addresses.

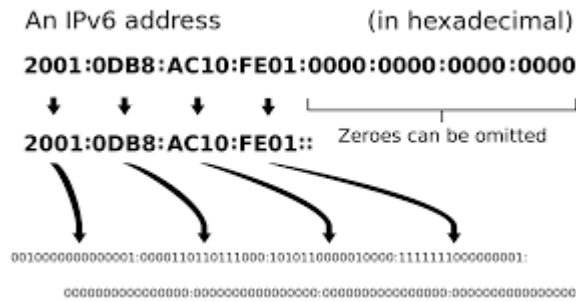
- Class C addresses use the first 3 octets to specify the network prefix, leaving only the last octet to identify hosts.

But this method was quite restricted; the size of the network was fixed and left no room to an expansion or a restriction so the classless addressing method appeared, decoupling IP address ranges from a default subnet mask, allowing for variable-length subnet masking (VLSM). With the VLSM and classless addressing the network admin could adjust the network mask to fit the right size for the network.

2.4 Structure and Format of IPv6

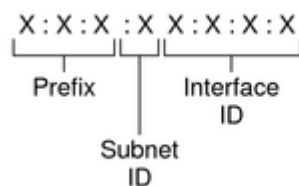
- Description of IPv6 addressing structure and its advantages over IPv4.

By the time passing there are more and more devices who need an address and slowly IPv4 will show its limit so that's why IPv6 with the same principal functionality that made IPv4 popular will replace it one day. IPv6 addresses will be on 128 bits instead of 32 bits. The IPv6 address is constituted of 8 sections of 16 bits, each section is a number in hexadecimal separated by “:”. Hexadécimale can be converted in decimal like in binary, The rightmost number represents 16^0 , increasing to the left until the first bit in the octet is 16^3 , but in adding to that you need to multiply the 16^n you are at by the n numbers you are at. For “20AC”, with the number going from 0 to 9, and the letter starting by A representing 10 to F representing 15, it goes $2 \times 16^3 + 0 \times 16^2 + 10 \times 16^1 + 12 \times 16^0 = 8364$

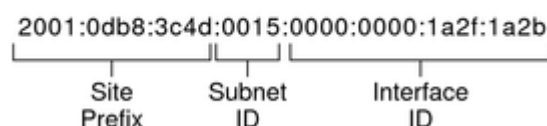


IPv6 has also other interesting features, it has different address types and can identify the type of applications it pertains to, IPv4 also has these features without .

Unicast address: It's an address which is specified for one individual like when you send a letter to someone, it's constituted of the prefix and the interface numbers (like the house number).



Example:



Multicast address: It's specified for a bunch of interfaces instead of one by selecting a certain interface ID

Anycast address: Like Multicast address, it will be sent to multiple interfaces but only one interface gets the data.

- Comparison between IPv4 and IPv6.

The IPv6 takes what makes IPv4 a good protocols by adding different features, here is what IPv6 has that IPv4 hasn't:

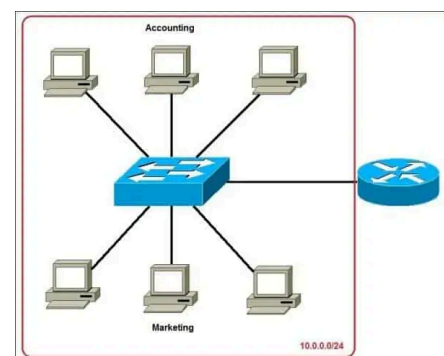
- Passing from 32 bits to 128 bits , it means a lot more addresses that can be provided
- When IPv4 has needed an extensions like NAT, IPv6 doesn't because it was reflect for the future
- A new type of address, Anycast

2.5 Subnetting

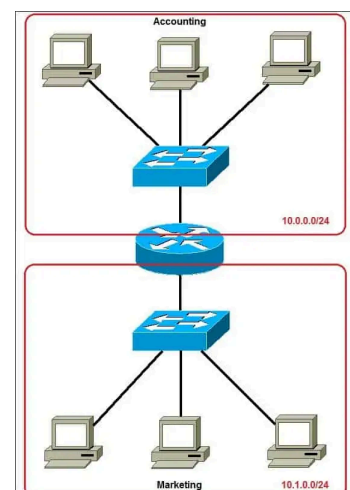
- Introduction to subnetting and its significance in optimizing IP address allocation.

The role of subnetting becomes more and more important by the size of a network. Subnetting has a role to streamline traffic in a network by dividing a network in multiple smaller ones strategically with giving subnet masks (devices with a submask can create new network) to devices, for them to take the shortest distance possible or a certain route to not have an overflowing traffic in the network. It's very useful in the organization of a network, IP addresses can be kept geographically localized meaning that a subnet can be used for specific staffing structures. For example:

Here we have just one huge network: 10.0.0/24. It has disadvantages like creating too much traffic or organization problems.



Here is what could be subnetting our network, dividing the network 10.0.0/24 in two network, 10.0.0/24 and 10.1.0/24. Now the traffic on the network should be good.



So subnetting is really important to IP address allocations, and other things need to be done for having efficient IP allocations like adding an IPAM tool to our network, with an IPAM you can plan, deploy, monitor and manage your IP address infrastructure, you can manage it all from a central interface. You can also add a DHCP that will automatically attribute a network IP address to a new device. Reviewing our IP scheme is important to optimize the traffic.

Testing and troubleshooting

There are a lot of testing methods to know if our network is working, one of them and the one that I will use to test my network is the Ping Test. The method is pretty simple, you just need to go to the cmd of one machine and type “ping and IP address in our network that we want to reach” for example “ping 192.168.0.1” and if we have a response then the link between our machine and the one we ping is done.

There is also other testing that can be done on a network:

Bandwidth testing : It's the test of the volume of information that can be sent over a connection in a measured amount of time, it's calculated in MegaBits per seconds (Mbps)

Packet loss testing: It's the measurement of the amount of data packets that don't arrive at their destination.

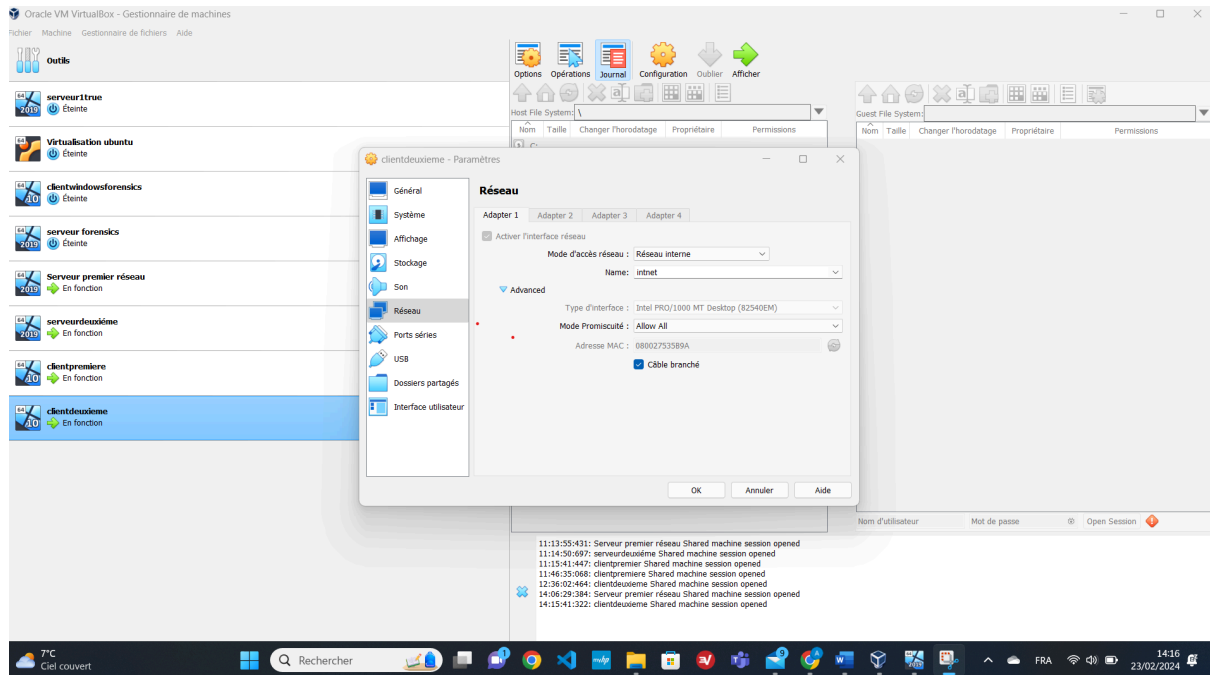
Security testing: Networking security testing is a holistic approach to finding security vulnerabilities and loopholes across a network.

For the creation of my network, I failed but I will explain how I have done. At first, I had succeeded on a smaller network with two devices and tried to do it on the scheme and it worked, but I have not done the right network scheme so I deleted all and started all again. So I created 3 internal networks:

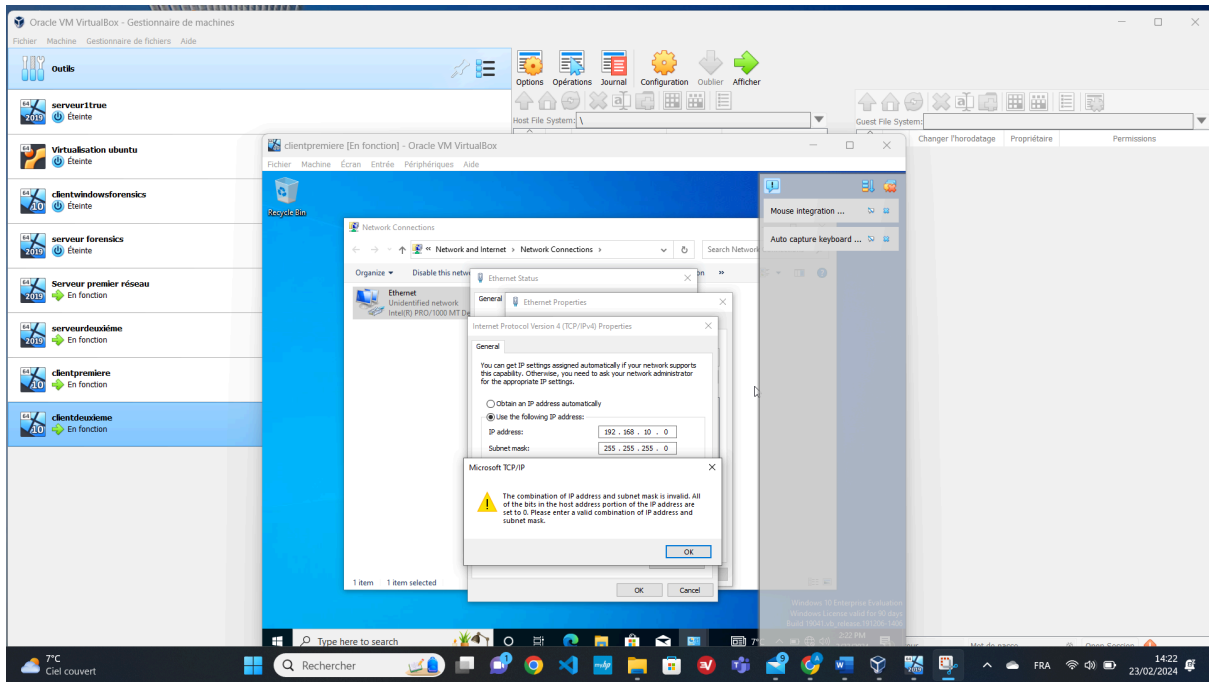
-Internal network 1: to connect server 1 et client 1

-Internal network 2: to connect server 2 et client 2

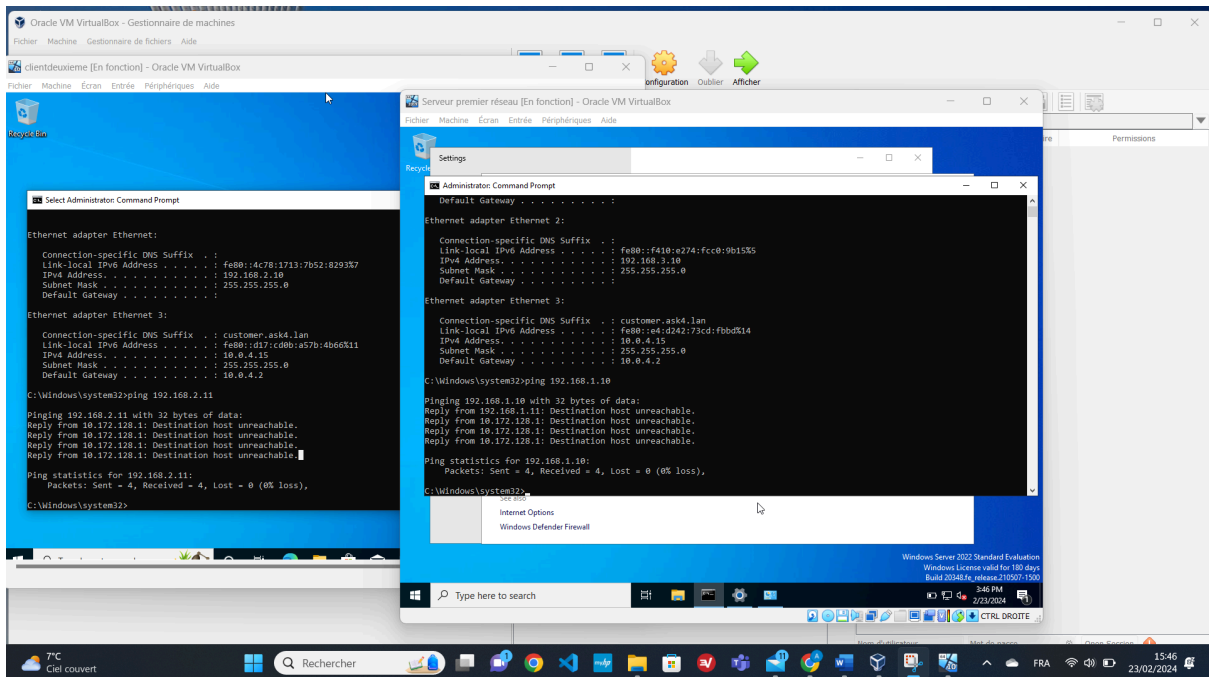
-Internal network server : to connect server 1 et server 2



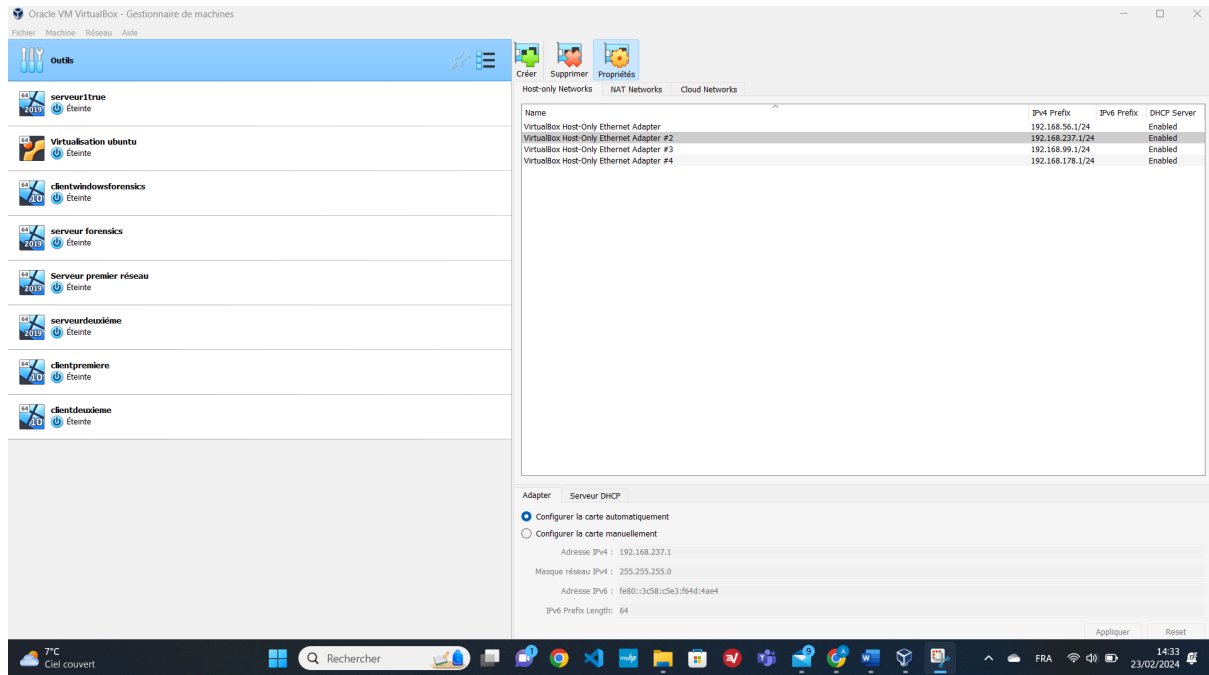
I changed the IP address manually of each client and server (servers are connected to 2 networks so they have 2 IP). But I have a error because the host part was wrong so I just changed all.



But when I typed ping the other machine, it was unreachable



So I have done my research, and tried to connect them to the internet, deactivate the fire all, change ping to automatic but nothing worked, so I tried to change the method. I created networks and assigned them to my machine but this time, the request was time out so I tried all that I tried before and it didn't work and I had no time left .



Conclusion

Even if I have failed to create my network, I learn a lot of things by researching IP addresses, Hypervisor, and I search things for my curiosity too ! I understand now, that troubleshooting skills are important.

Référence

<https://aws.amazon.com/fr/what-is/hypervisor/#:~:text=A%20hypervisor%20is%20a%20software,individual%20virtual%20machines%20as%20required.>

<https://www.techtarget.com/searchitoperations/tip/Whats-the-difference-between-Type-1-vs-Type-2-hypervisor>

<https://aws.amazon.com/fr/compare/the-difference-between-type-1-and-type-2-hypervisors/#:~:text=Type%201%20hypervisors%20directly%20access,process%20slower%20and%20less%20efficient.>

IP address

<https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address>

<https://www.cloudflare.com/en-gb/learning/network-layer/how-does-the-internet-work/>

<https://www.cloudflare.com/en-gb/learning/network-layer/internet-protocol/>

<https://www.juniper.net/documentation/us/en/software/junos/interfaces-security-devices/topics/topic-map/security-interface-ipv4-ipv6-protocol.html#:~:text=is%20IPv4%20Addressing-,IPv4%20addresses%20are%2032%2Dbit%20numbers%20that%20are%20typically%20displayed,addresses%20that%20uniquely%20identifies%20it.>

<https://gcore.com/learning/data-transmission-guide-everything-you-need-to-know/>

<https://www.cloudns.net/blog/what-is-ipv4-everything-you-need-to-know/>

https://www.cloudns.net/blog/ipv4-vs-ipv6-internet-protocol/#IPv4_vs_IPv6

<https://www.fieldengineer.com/skills/subnetting>

<https://study-ccna.com/subnetting-explained/>

<https://learn.microsoft.com/en-us/windows-server/networking/technologies/ipam/ipam-top>

<https://www.redswitches.com/blog/ip-address/#BestPracticesforAllocatingIPAddresses>

Chapitre I

Chapitre II

Chapitre III

