

LEVEL 5 ASSESSMENT SPECIFICATION



Student name:	DURYE Clement	Student ID number:	2325578
Programme:	Computing/ Isep exchange		
Module:	Network Operating Systems and Services		
Module code:	ACCA5023	Contribution to Overall Module Assessment (%):	50%
Lecturer:	Dr. Nitheesh Murugan Kaliyamurthy	Internal Verifier:	Munyaradzi Murira
Assignment Title:	Build, and deploy, a Type 2 Hypervisor platform based Virtualised network	Word count (or equivalent):	2500 words
Submission deadline:	23/02/2024	Return date of provisional marks & written feedback:	20 Working Days
Submission method:	All written assessments, where practical and possible, must be submitted via Turnitin unless otherwise instructed by the Lecturer. (Please DO NOT put this assessment specification into Turnitin or it will match many similarities with other students' submissions.) Alternative submission method (if applicable): b Late submission of the assessment will result in a late penalty mark. Penalties for late submission: Up to one week late, maximum mark of 40%. Over one week late, 0%. Only the Extenuating Circumstances Panel may approve a change to submission dates.		
Academic honesty / referencing:	Academic honesty is required. In the main body of your submission, you must give credit to authors on whose research and ideas your work is based. Append to your submission a reference list that indicates the books, articles, etc. that you have used, cited or quoted in order to complete this assessment.		

Table of Content

Chapter 1: Exploring the Hypervisor Technology..... 3

1. Research Hypervisor
2. Choosing the most suitable hypervisor
3. Downloading
4. Setting up servers and clients

Chapter 2: The Network Communication and role of IP addresses.....5

5. Data Journey on Internet
6. Configurations of IP

Chapter 3: Network testing and troubleshooting.....9

7. Connectivity of my Network

Chapter 1: Exploring the Hypervisor Technology

1. Research Hypervisors

First of all, a hypervisor is a virtualisation tool that is often known as a Virtual Machine Monitor (VMM). If you research hypervisors, you'll find that there are two types, called type 1 hypervisors and type 2 hypervisors. The difference between the two is explained very well on the VMware site, which produces type 1 and type 2 hypervisors; type 1 is the most common and is installed on the hardware layer of a server and then, like any other type 2 hypervisor, you can run several virtual machines on it; type 2 hypervisors are installed on an operating system that is already installed on a hardware layer. On a type 2 hypervisor you can therefore compare the hypervisor to a simple application that you launch on a machine and unlike a type 1 hypervisor you can have several hypervisors on the same OS. Once installed, the hypervisor has the same role as on a type 1. We can therefore find advantages and disadvantages on each type of hypervisors, first of all on a type 1 the advantages are that, a maximum of resources can be allocated to virtual machines because this type of hypervisor is directly linked to the hardware layer and there is not really a disadvantage that can be identified, for a type 2 hypervisor, it is advantageous to be able to run several hypervisors at the same time because they do not install directly on the hardware layer, and their disadvantage is that they can't allocate much less resources than a type 1 hypervisor because the OS on the hardware layer already consumes resources. It is also important to mention the scalability of hypervisors which is a vital feature in cloud computing, because scalability facilitates the migration of VMs by exchanging data and other possible operations. Then, by doing research on the safety of hypervisors, we find forums warning about the dangerousness of data theft, about the stability of the system. The forums explain that this often occurs when one seeks to run unnecessary services on their machine. Many forums specify that not updating your hypervisor can end up becoming a security flaw, because older versions of hypervisors can leave security flaws fixed in the most recent versions. Finally we can finally give some examples that we find different types of hypervisors, first in types 1 the most known is VMware vSphere and we can also take as an example Citrix XenServer, in types 2 there are also many of them including VMware Workstation or VirtualBox. In both types there are many others which are quoted are just often used.

2. Choosing the most suitable hypervisor

The last question allowed us to study the different types of hypervisor, their functionalities and to evaluate their advantages and disadvantages. It has therefore made it possible to identify that to carry out the submitted project, it would have been more efficient to use a hypervisor type 1 because it is directly on the hardware layer of the machine, but given our situation and that we only have a computer with an OS already installed on our hardware we will therefore use a hypervisor type 2. We must then choose that it would be best to use for our project. Better, one that will be cheap or even free, so our research leads to VMware Workstation or Oracle VirtualBox. Oracle VirtualBox being an open source software advantage our choices and already finding it on our machines. To realise the design architecture, we will use Oracle VirtualBox to create our two Windows 2022 ISO servers and our two Windows 10 clients.

3. Downloading

So I chose to download VirtualBox from Oracle, to then add the different requested servers and different clients. The servers were downloaded using the Windows 2022 ISO found on the Internet and the clients were downloaded as Windows 10 clients. As can be seen in the photo (Image 1) there are several download options

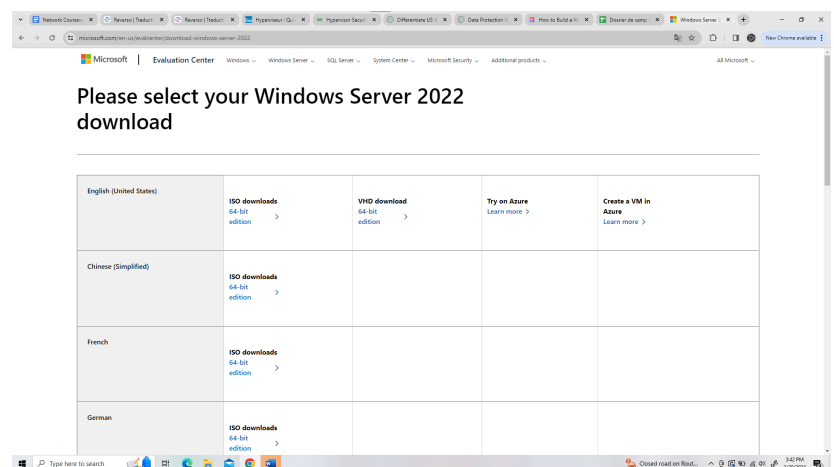
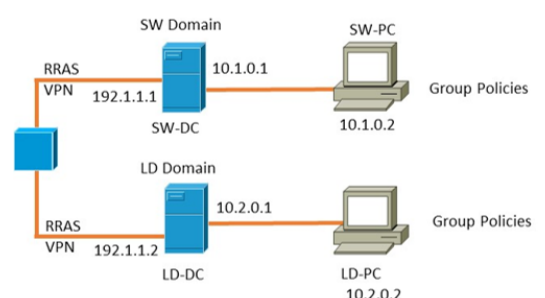


Image 1

for the Windows 2022 server, there are VHD, ISO and test options on Azure, so it was necessary to choose the ISO and obviously in English.

4. Setting up servers and clients

Image 2



I then did the setup according to the topology we had (Image 2). So I had to install the named servers for one Swansea Domain (SW) and the other London Domain (LD). This was complicated especially because I had trouble setting up both servers because in the application of the Hypervisor, VirtualBox at the beginning of the server setup steps once the ISO of Windows 2022 add several launch type options are possible, the first option is to launch it as I did in computer mode and therefore have a Windows interface, but my mistake at the beginning was to launch it as a basic launch which does not give us this interface. Then in the setup I had to create a second server once I understood how to do the first one. For the second server a faster option was possible, so I realised it, it was enough to clone the server to have two similar. Then setup the Windows 10 clients was a similar step this was done without much problem, again, the first step was to find the right iso and then the setup with in particular, choose the number of cores to add for the startup of the VM. So I put two cores on the clients and all the servers being necessary enough to succeed in then linking the clients to the domains and to link the two servers between them.

Chapter 2: The Network Communication and role of IP addresses

5. Data journey on Internet

Transferring data across the Internet, from one computer to another, is a process involving many steps. I found resources to understand this phenomenon on the Cloudflare website. The first step in the data transfer process is to break down the data into small parts, the different small parts are called "packets". Packets contain a lot of information, for example the content of the sent message from the sender and the receiver, but it also contains the IP of the sender and the receiver, in order to know where to go the packets. Once the packets have left the sender's computer, they cross the computer networks arriving at routers, the routers themselves are like traffic directors, they will choose the most efficient way so that the packets reach the recipient's computer in the least given time. Generally, the data also passes through switches that have the same purpose as a router in short, guided the data to the receiver. Packets thus pass from routers to routers and each time the destination IP address is checked to redirect it to another router until the packets reach the receiving computer. I also learned in my research and through the *howstuffworks* website, that each packet can contain up to 1500 bytes of information, moreover all the information of a packet is contained in what is called the header, it contains, in particular, the information of the originating

computer and the receiving computer (IP addresses of Both). It is also important to specify that once the packets arrive in the computer receiving the message, there are other data that are sent including the response of the recipient to the sender to confirm whether or not all the packets were received, because it can happen that packets do not arrive at the reception of the message and therefore that the computer which receives the message asks the sender to send back the missing packets always according to the information of the website: *howstuffworks*, once all packets received the recipient confirmation is sent to the sender. One can thus see the sending of the data, as the sender creating the cutting of a puzzle and the recipient must rebuild it. I mentioned several times the term IP address in my explanation of crossing data between two computers. The IP address in a data transfer is surely the most important. First of all, you should know that any device connected to the internet, therefore mobile phone, laptop, server and any object on internet networks has a unique IP address. So in a data transfer like sender and recipient are unique thanks to their IP, we can identify the source and how far packets must travel in the network to reach the recipient. The IP address is also an important factor in the transfer of data because in the header of the packets is present the IP address of the starting computer but also of the receiving machine which makes it possible to identify their path from the source to the recipient. In my research I noticed that there are two types of IP addresses, IPv4 and IPv6. There are obviously differences between these two versions of IP, the first that we notice is the length of both, for version 6 we have a length of 128 bits and for version 4 it will be much shorter with 32 bits. Thus with an IPv4 we obtain 255^4 possibility or about 4.3 billion possible IP address and for IPv6 we have 2^{128} possibilities thus much more than for version 4 allowing to have a real single address compared to the machine numbers on the market. The second difference is the notation of the 2 versions of the protocol, for version 4 it is a series of 4 numbers varying between 0 and 255 separated by points (example: 192.0.2.146). For version 6 instead of continuing to increase in numbers it was decided to make a notation in hexadecimal with 8 sets of 2 numbers in hexadecimal and each series is separated by colons (example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334). In short, we can conclude that IPv6 was created to address the shortcomings of IPv4.

6. Configurations of IP

With the topology we had I had to configure my clients and servers to assign them IP addresses according to the version 4 protocol. Having configured Internal network connections for my 2 servers and my 2 clients so that they can communicate with each other I

DURYE Clement
2325578

just had to go and impose on the clients and the servers to have their IP according to the topology for the server of Swansea and London the IPs to communicate with the clients were respectively: 10.1.0.1 (SW) and 10.2.0.1 (LD). As for the clients, the IPs to the servers were 10.1.0.2 for Swansea and 10.2.0.2 for London (Image 3).

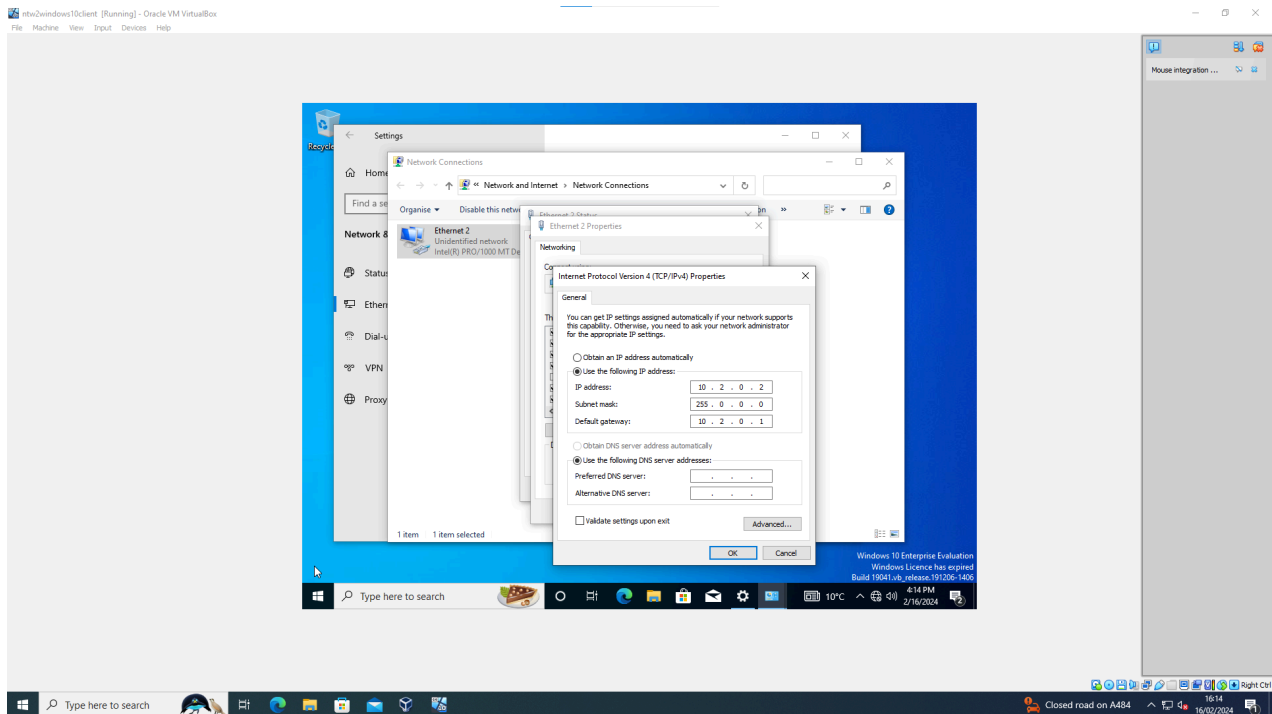
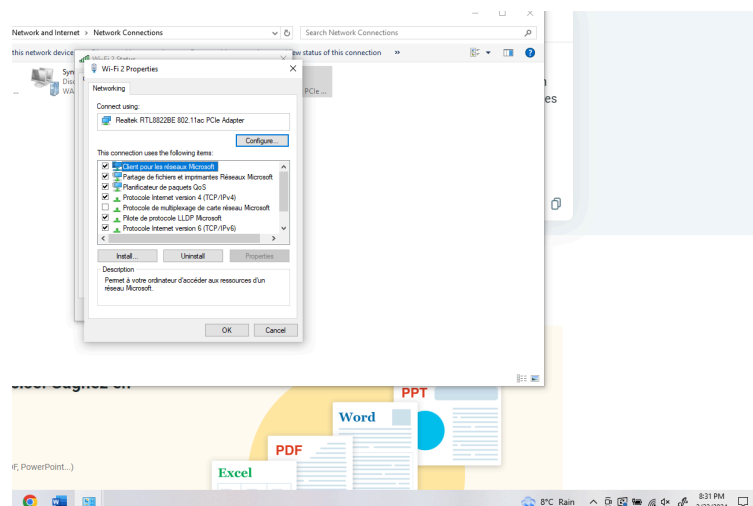


Image 3

In addition to these connections between server and client it was necessary to create another Internal Network connection between the two servers to complete the topology scheme with IP addresses that were, for Swansea 192.1.1.1 and for London the IP address was 192.1.1.2. Moreover to configure this it was necessary to go in the control panel (Image 4) and to modify manually in Internet Protocol version 4 the framework IP address (Image 5).



Moreover for the connection of the clients to their server it was necessary to create the connection to the server in the default gateway section by manually writing the IP of the server.

Image 4

[illegible]

Image 6

Chapter 3: Network testing and troubleshooting

7. Connectivity of my Network

a) Today several ways are known to test its connectivity, we find the ping test, which is used via the prompt command of Windows by typing on a ping machine and behind it the IP of the server we want to reach. This is a fairly basic test which consists in sending ICMP echo request in the form of packets to the machine to which one tries to test its connectivity, after that we wait for the response of the machine that received our packets and that returns us other packets it will show us if the device that we want to reach is accessible and will also measure the round trip time, so the time between sending and receiving packets on the machine that sent first. However sometimes the connectivity test does not work and we refer to errors that we will see. First the most common error is "request timed out" which means that the destination that tries to be reached is unreachable, which can be seen in Image 7 this is often due to either a problem in the configuration of the firewall but also can be due to the destination that makes dropping packets. The second option is also known as packet loss, this happens for various reasons such as delays, disruptions, or errors in network communication. To check where this problem comes from several ways are possible, test its bandwidth with websites such as speedtest.net or local with prompt command and iperf command. In addition, connectivity errors can also come from other issues such as IP Address conflicts, DNS resolutions. IP address conflict is a problem that occurs when in a network several machines have the same IP address this is noticed with ping test failed and also Inconsistent Traceroute Results. For DNS resolution issues, this happens when the DNS fails to translate domain names into IP addresses or resolves to incorrect IP addresses, preventing successful communication between devices. This results in the same problem as the previous Issues and these three previous problems are the main network connectivity problem.

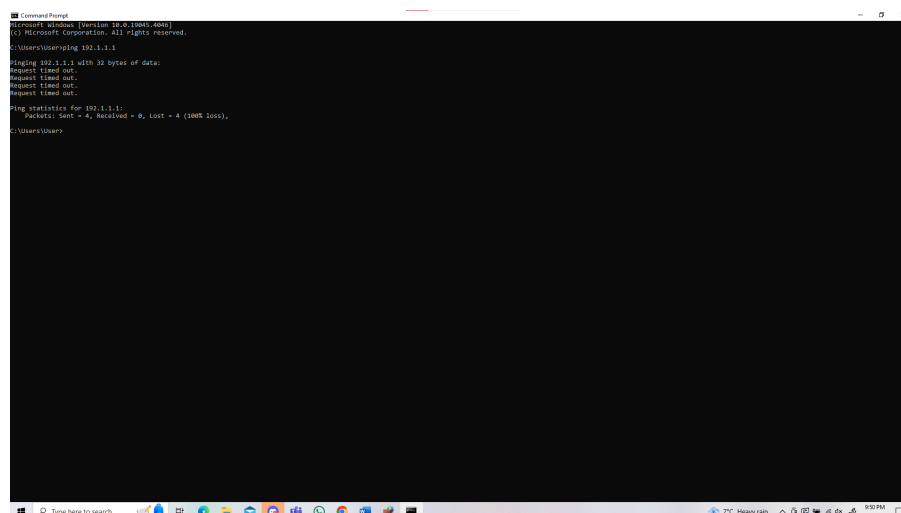
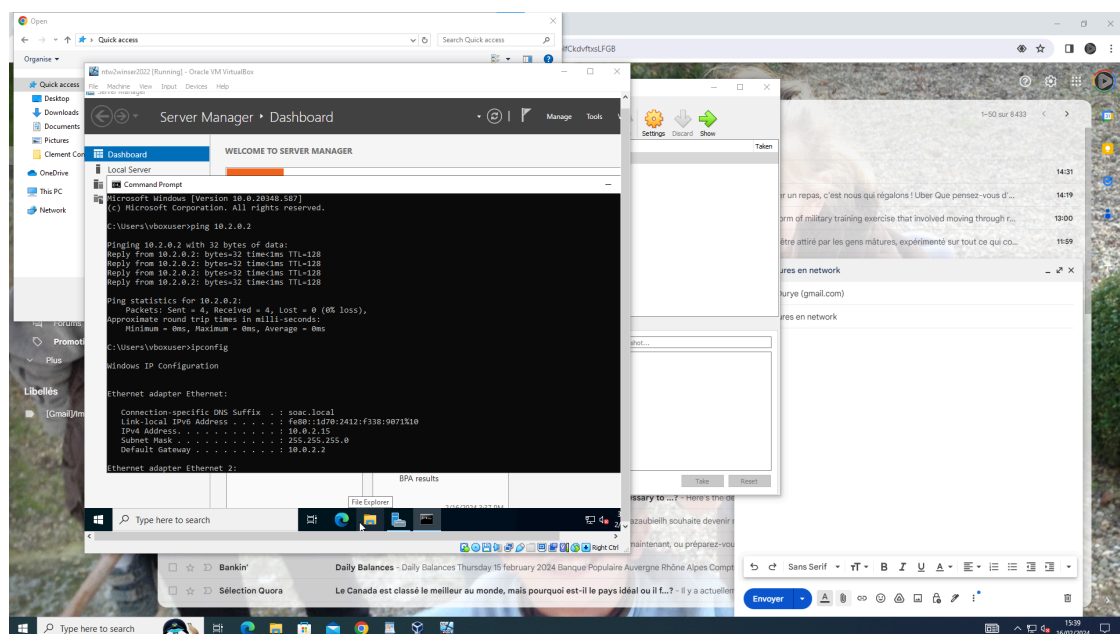
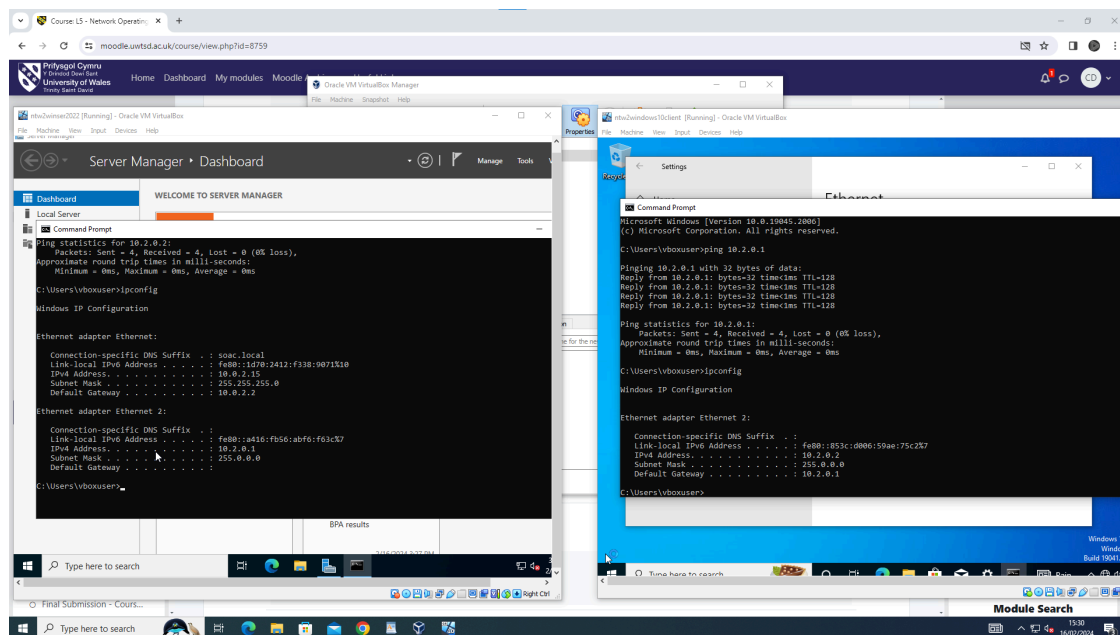


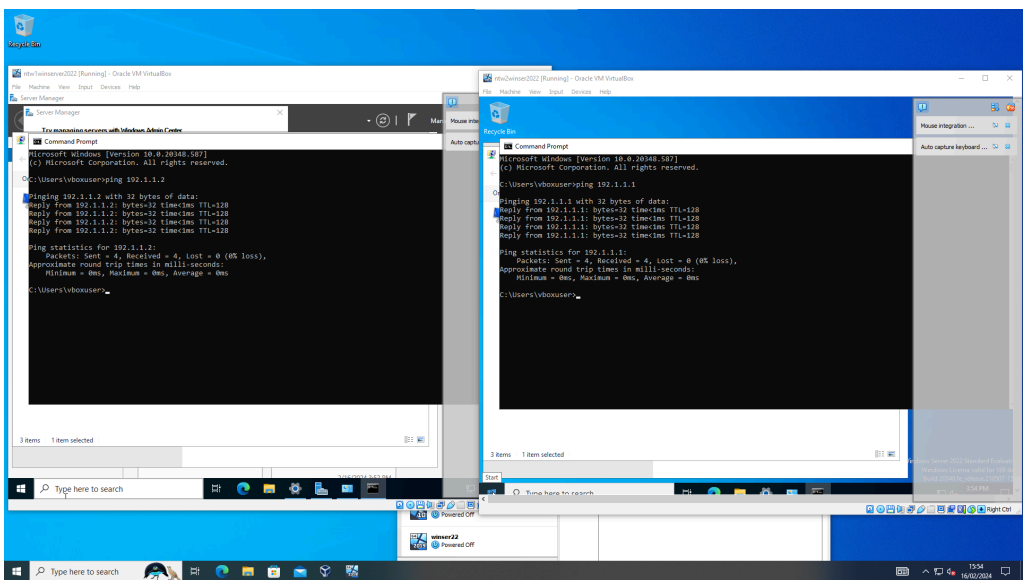
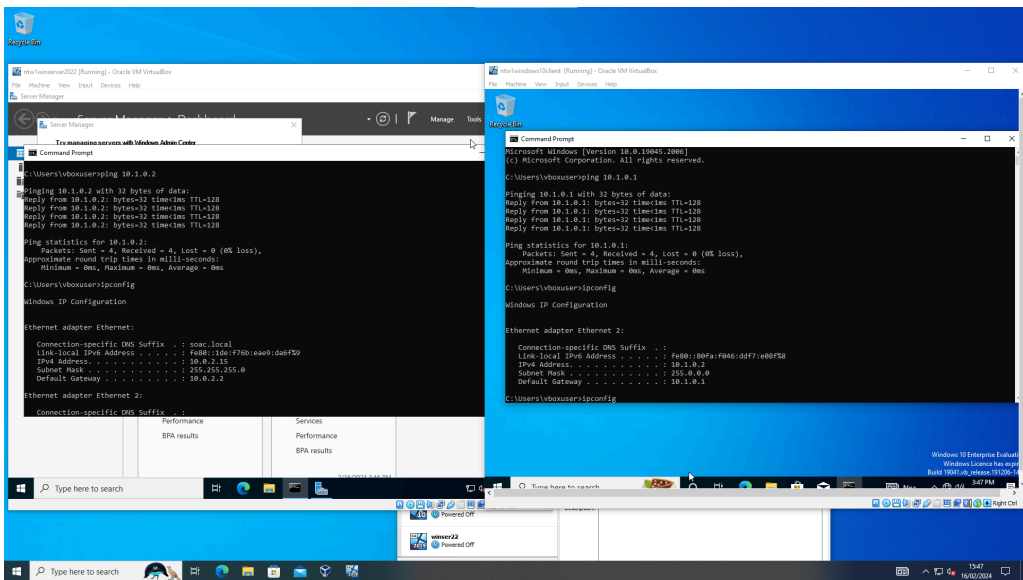
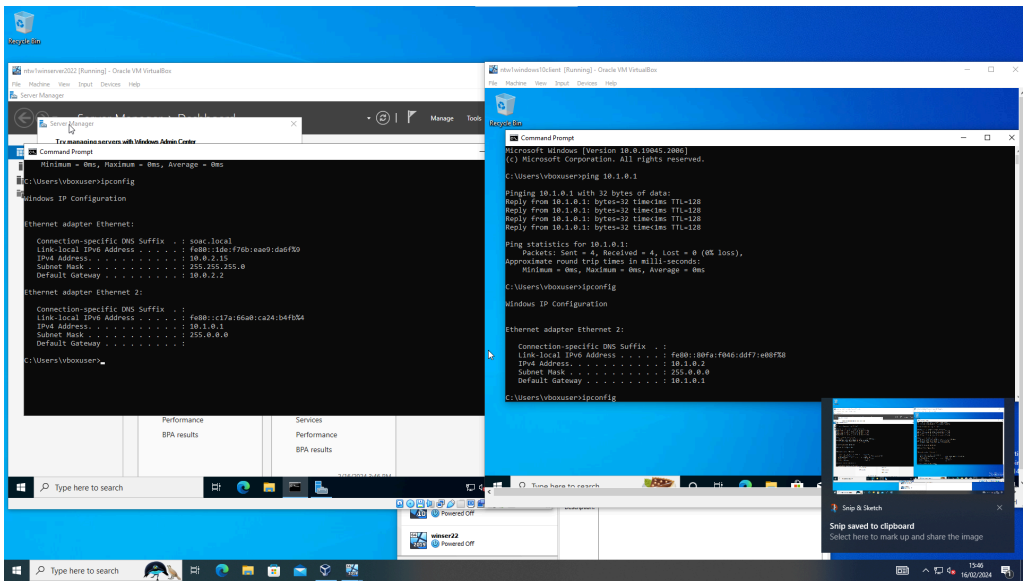
Image 7

DURYE Clement
2325578

b)

To validate my topology I therefore checked with a ping test each of the connections between servers and clients in both directions and server to server (Image 8-12), these images show the connectivity that is successful between each of my servers and clients and also showing the valid configuration of each of the IP addresses according to the topology.





DURYE Clement
2325578

Appendix

Chapter 1

<https://www.vmware.com/uk/topics/glossary/content/hypervisor.html#:~:text=There%20are%20two%20main%20hypervisor.system%2C%20like%20other%20computer%20programs.>

<https://www.datamation.com/applications/hypervisors/>

<https://www.geeksforgeeks.org/hypervisor-security-in-cloud-computing/>

Chapter 2

<https://www.cloudflare.com/learning/network-layer/what-is-a-packet/>

<https://computer.howstuffworks.com/ip-convergence2.htm>

<https://www.juniper.net/gb/en/research-topics/what-is-ipv4-vs-ipv6.html#:~:text=IPv6%20offers%20these%20improvements%20over,from%2032%20to%20128%20bits>

<https://kinsta.com/blog/ipv4-vs-ipv6/>

Chapter 3

<https://www.pagerduty.com/resources/learn/ping-network-testing-connectivity/#:~:text=A%20ping%20network%20test%20transmits.connectivity%20between%20IP%2Dnetworked%20devices.>

<https://www.youtube.com/watch?v=59RhHsvNK44&t=164s>

<https://www.ir.com/guides/what-is-network-packet-loss>

<https://www.makeuseof.com/tag/whats-ip-conflict-resolve/>