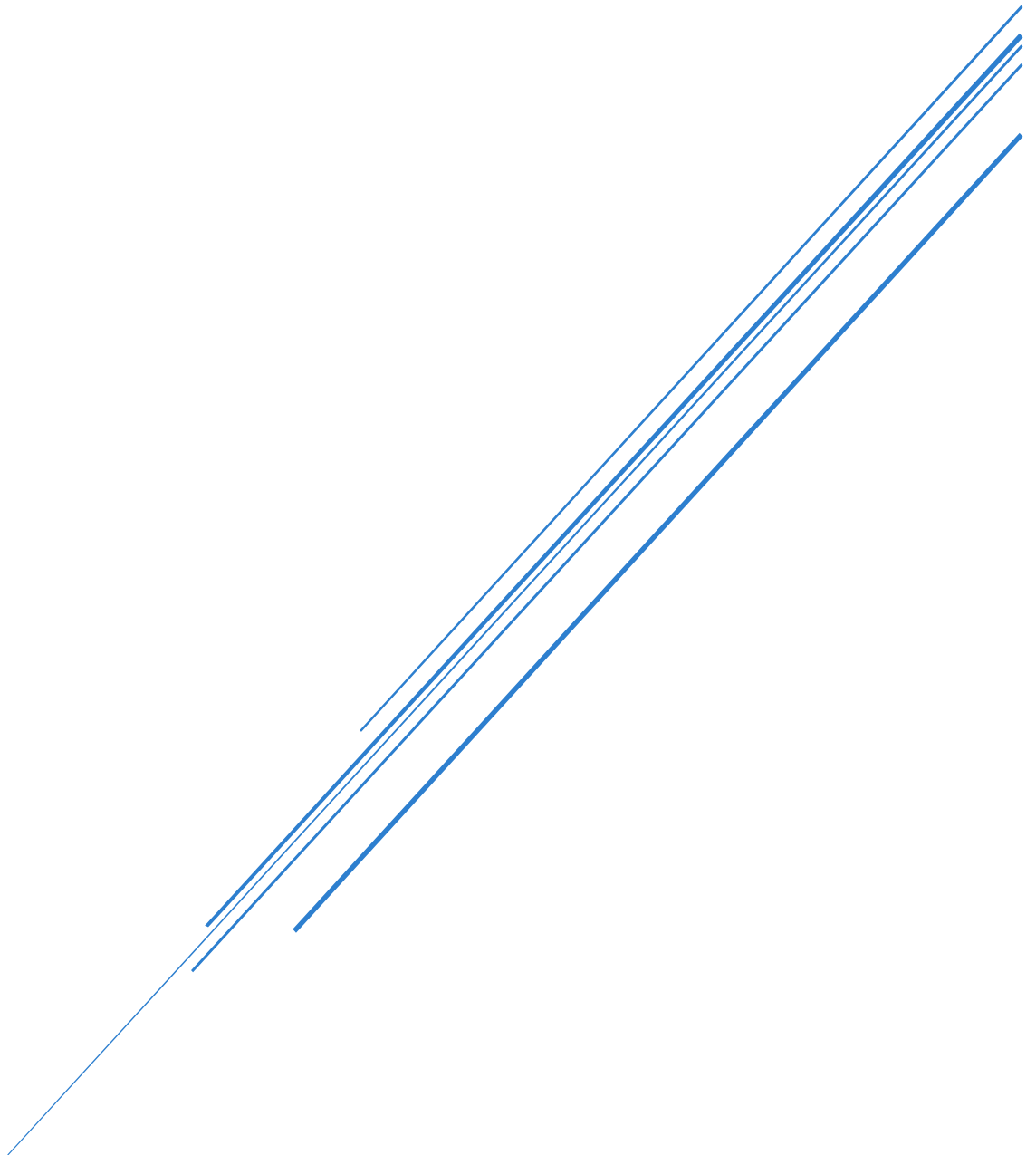


NETWORK OPERATING SYSTEMS AND SERVICES (ACCA5023)

Coursework 1 - Report



Che Morris - 2203458
Cybersecurity and Networks

Table of Contents

Research on Hypervisors	2
Type 1 Hypervisors	2
Type 2 Hypervisors	3
My choice of Hypervisor	3
Research on IP Addressing	4
Configuring the Network	6
SW-DC IP Configuration	6
LD-DC IP Configuration	7
SW-PC IP Configuration	7
LD-PC IP Configuration	8
Testing the Network	8
Research on Network Testing and Troubleshooting	8
Testing the Connectivity of my Network	10
SW-DC pinging SW-PC (and vice-versa)	10
SW-DC pinging LD-DC (and vice-versa)	10
LD-DC pinging LD-PC (and vice-versa)	11
Issues Faced	12

Research on Hypervisors

Over the last few decades, with the need for technology advancing so rapidly, there has been a need for systems to be easier to deploy, manage and use. To meet these demands, virtualization technology was developed to help manage infrastructure in modern day computing. The main part of this technology is the hypervisor (also known as Virtual Machine Monitors or VMMs), these come in different types that carry their own advantages, disadvantages, unique features, different architectures and their own distinct use cases. The two types of hypervisors are Type 1 hypervisors, also known as bare-metal hypervisors, and Type 2 hypervisors, also known as hosted hypervisors.

Type 1 Hypervisors

This type of hypervisor runs directly on the machine itself and does not need an underlying OS which would put it directly in control of all system resources, examples of type 1 hypervisors would be VMware ESXi and Microsoft Hyper-V [1]. Those hypervisors such as VMWare ESXi and Hyper-V are quite thin and don't take up much system resources, they take place of the OS on the machine. This type of hypervisor can be much more effective in terms of performance than other types for a few reasons, one of which being that with a type 1 hypervisor, the VMs have direct access to the hardware of the machine, this will be shared but due to the fact that it isn't limited by an underlying OS, the VM can be allocated resources dynamically and if it's in need of more it can be allocated more as and when needed [2].

Type 1 hypervisors offer many features that would be quite scalable within large corporations or data centres as the hypervisor is able to virtualize both desktop and server operation systems. Large organisations can utilize Virtual Desktop Integration (VDI) to let their employees access desktops on virtual machines running Windows and such from one central server which would be running the hypervisor, this can make it easier for IT staff within the organisation to monitor and maintain those desktops without having to physically go to a machine, making their job more efficient [3]. This also wouldn't be too resource intensive for the end user so they can access the desktop from anywhere on many devices, even mobile phones, as the client used to connect to the desktop can be quite light weight [3]. This could also be useful within data centres as it reduces the stress on employees there having to head to a certain server or machine and perform maintenance physically when it can be done from one central location. These also come with the benefit of the VMs being easily replaceable if something does go wrong, it would be extremely easy to spin up a backup of that VM or even deploy a completely identical VM that can take over from where the other left off [4].

The compatibility of type 1 hypervisors is generally quite expansive, but depending on your choice of hypervisor could potentially be quite limited and not all hardware may be supported [5]. These hardware limitations could be quite devastating depending on if you've bought your hardware before you've investigated which hypervisor you wish to use, which is why people may stay away from the use of type 1 hypervisors, especially if you only wish to use one or two virtual machines.

Type 2 Hypervisors

Type 2 hypervisors are slightly different to type 1, offering some of the same things but also coming with a lot more disadvantages. This type of hypervisor runs on top of a preexisting operating system that is installed on the host and will have to run by the 'rules' set by that host, leading to it being less dynamic as resources cannot be allocated on the fly, which also can lead to degraded performance [1]. Type 2 hypervisors are often used in cases where not many VMs are needed, they are quite convenient for this as there's no need to access a separate system to setup or manage your VMs, it's all done on one machine. This also means that type 2 hypervisors will not be as scalable when compared to type 1. Examples of type 2 hypervisors are Oracle's VirtualBox and VMWare's Workstation/Fusion, the first being free and the latter requiring a payment.

Type 1 hypervisors have the advantages of being able to setup machines quite easily and being easy to manage, convenient for cases where you need to test something (can be used to test something in multiple environments quite easily) and it can allow for users to access things on their own personal machine that might not be compatible with their host operating system [3]. This also makes it extremely compatible for the virtualised operating systems as most type 2 hypervisors have software which can be used to drag and drop from host to virtual machine and so on. It does come with the disadvantage of reduced performance when compared to the type 1 hypervisor as resource management isn't as easy and performance will be degraded due to both the host and the virtualised OSes needing resources [3].

My choice of Hypervisor

To build my network, I will be using the Type 2 Hypervisor. This is mainly because I have a lack of hardware to use a type 1 hypervisor as I only have my machine, which I need Windows to be installed upon for daily use. If I had a machine that I could install a type 1 hypervisor on, I would as it would come with the huge benefit of me being able to do things quicker and easier, but unfortunately that is not the case. My choice of type 2 hypervisor will be VMWare Workstation Pro as I've used it now for many years to use software that requires older operating systems and it's something that I'm extremely familiar with.

Research on IP Addressing

IP Addressing plays an extremely important part in communication within computing these days, it's a fundamental part of how our devices connect and communicate with each other. Each device that connects to a network will be assigned an IP address, this can be done either automatically or manually and this will let other devices know which device they're sending information to as it'll be addressed to a certain IP [6]. There are two types of IP addresses that are commonly used today, these are IPv4 and IPv6. IPv4 is short for IP version 4 and started being used in 1982, it is currently still in use and used more commonly than IPv6, but IPv6 had to be created due to its limitations since the amount of IP addresses we can get as IPv4 is much less than v6. [6].

IP addressing helps with the communication of data as it allows for data to be transferred between devices and the internet through the use of 'packets'. IP is used to send these packets from the sender of the information to the receiver, it will contain lots of information besides the data including the size of the information and will also include what is being sent within the packet which will be included within the header of the packet [7].

There are two types of IP addresses that are used within a network, these being, public IP addresses and private IP addresses. Public IP addresses are provided mainly to the routers within the network and are what devices outside of the network use to send information to devices connected to the network [6]. Private IP addresses are addresses assigned to devices within the network, these are assigned to each device so that the router can locate the devices and connect to them within the internal network, these cannot be reached from outside the network unless it's connected to the router [6]. These IP addresses can be assigned as either static or dynamic IP addresses. A static IP is assigned manually by the person configuring the network which cannot be changed automatically, and a dynamic IP address is automatically assigned to a device when it is connected to the network using the Dynamic Host Configuration Protocol [6]. See diagram below.

Four types of IP Addresses

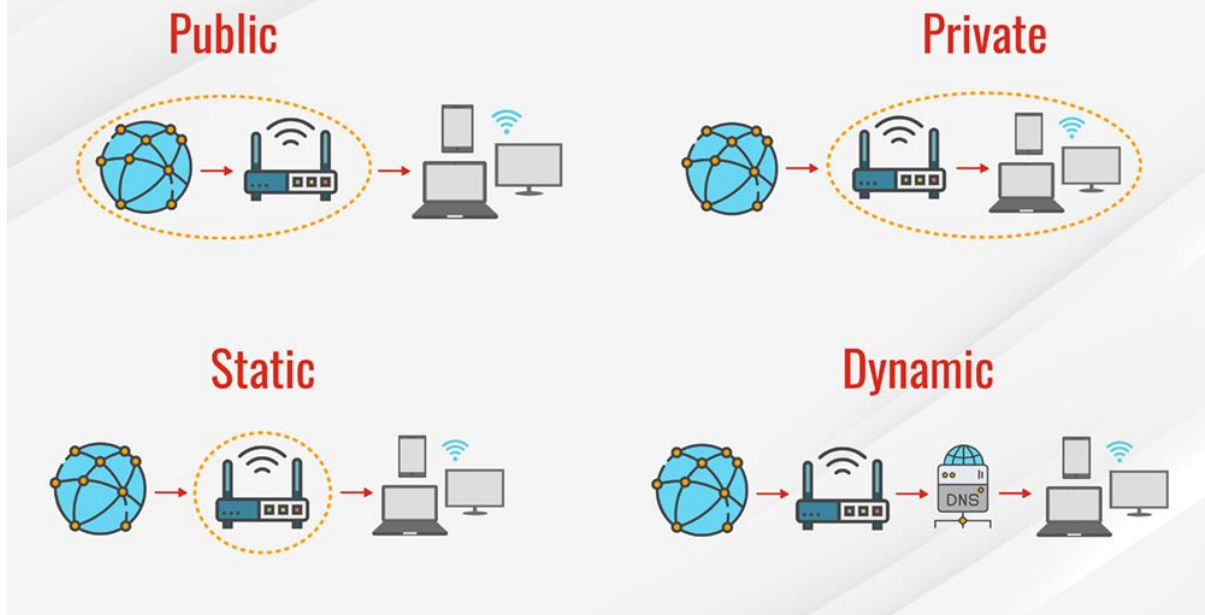


Figure 1 Types of IP addresses [6]

When creating a network, due to the limitations of IPv4, we don't want to waste IP addresses and we want to make it easy for our devices to communicate. This is where we utilize a process called 'subnetting'. Subnetting is when a 'subnet' is created within a network, they can make things within the network much more efficient as instead of data being sent through multiple places in the network to find its intended target, if it's within the subnet, it can find and talk to the destination device directly [8]. Subnetting can bring a few benefits to a network, it can lead to better network performance as it can "limit the scope of intranetwork broadcast messages to a specific subnet" [8]. This will lead to much better and much smoother communication between devices within that specific subnet, the packets will only search outside of the subnet if the destination IP address cannot be found within that subnet [8].

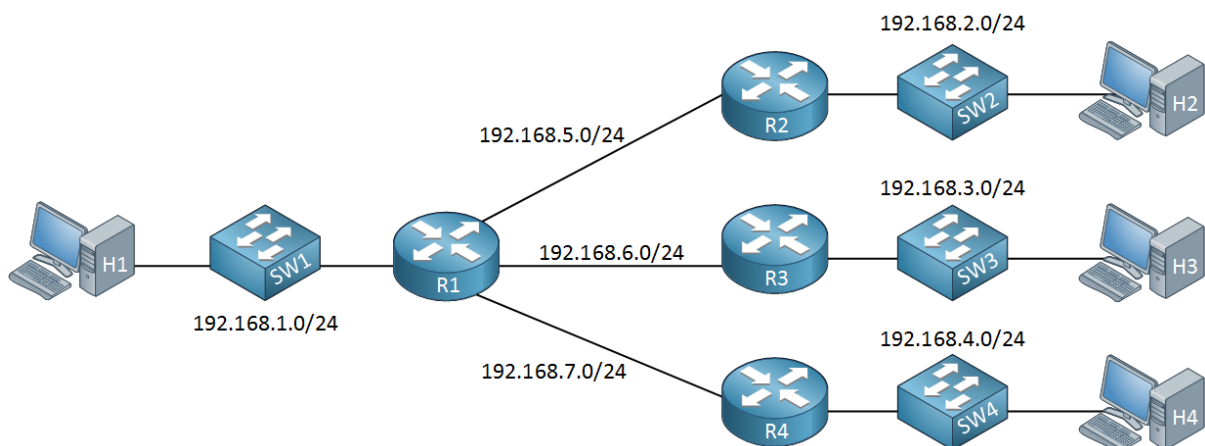


Figure 2 Diagram of Subnetting [9]

This is where routers can come in, when a packet has a destination that is outside of the local network, devices are used to direct that data between outside networks such as the internet or other local networks, they allow for routing to take place which helps forward packets to where they need to be inside of other networks [10]. Network administrators can create ‘routing tables’ within these routers that when a packet is received in a router, the router compares the IP to the routing table and sends the packet to the right place [10].

Configuring the Network

Following the given topology, I installed two servers running Windows Server 2022 and a client for each server running Windows 10. I followed the IP addressing scheme given on the topology and configured the SW domain with the IP 10.1.0.1 on the LAN on the client side and IP 192.1.1.1 on the server side. I did same for the LD domain with IP 10.2.0.1 on the client side and IP 192.1.1.2 on the server side. The PCs had IPs 10.1.0.2 for the SW-PC and 10.2.0.1 for the LD-PC respectively. I will provide screenshots of each machines IP configuration below. I also set the passwords to “Pa55w0rD!” as described on the topology.

SW-DC IP Configuration

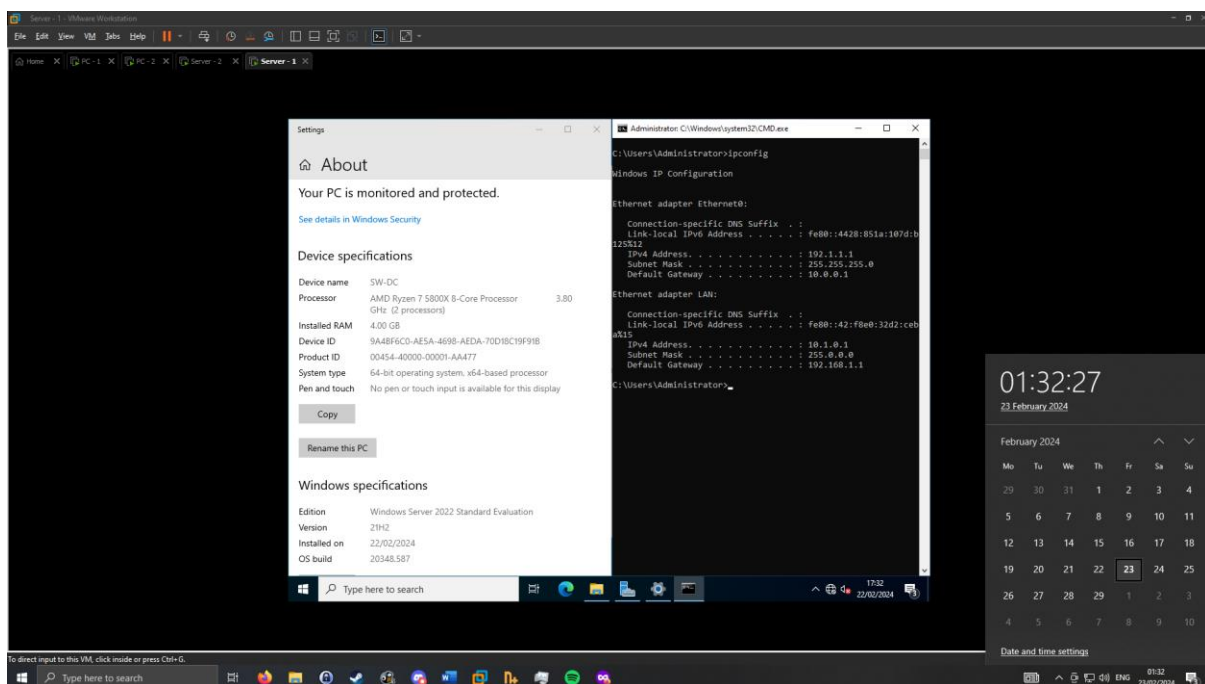


Figure 3 SW-DC IP Configuration

LD-DC IP Configuration

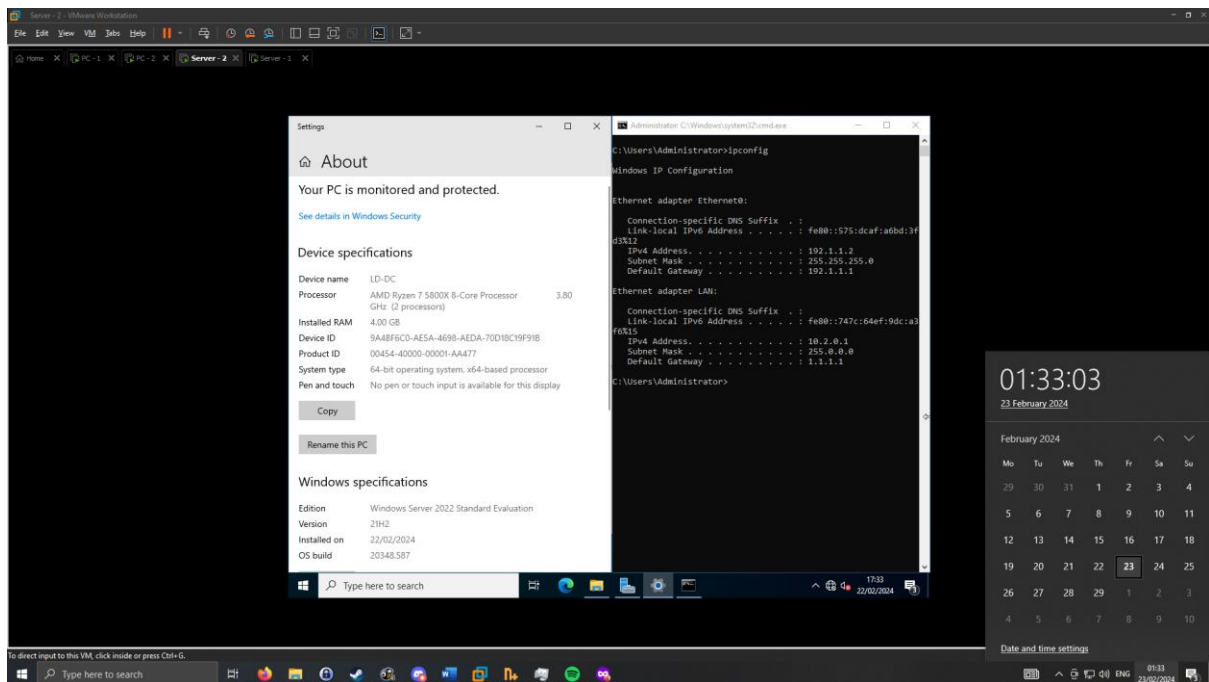


Figure 4 LD-DC IP Configuration

SW-PC IP Configuration

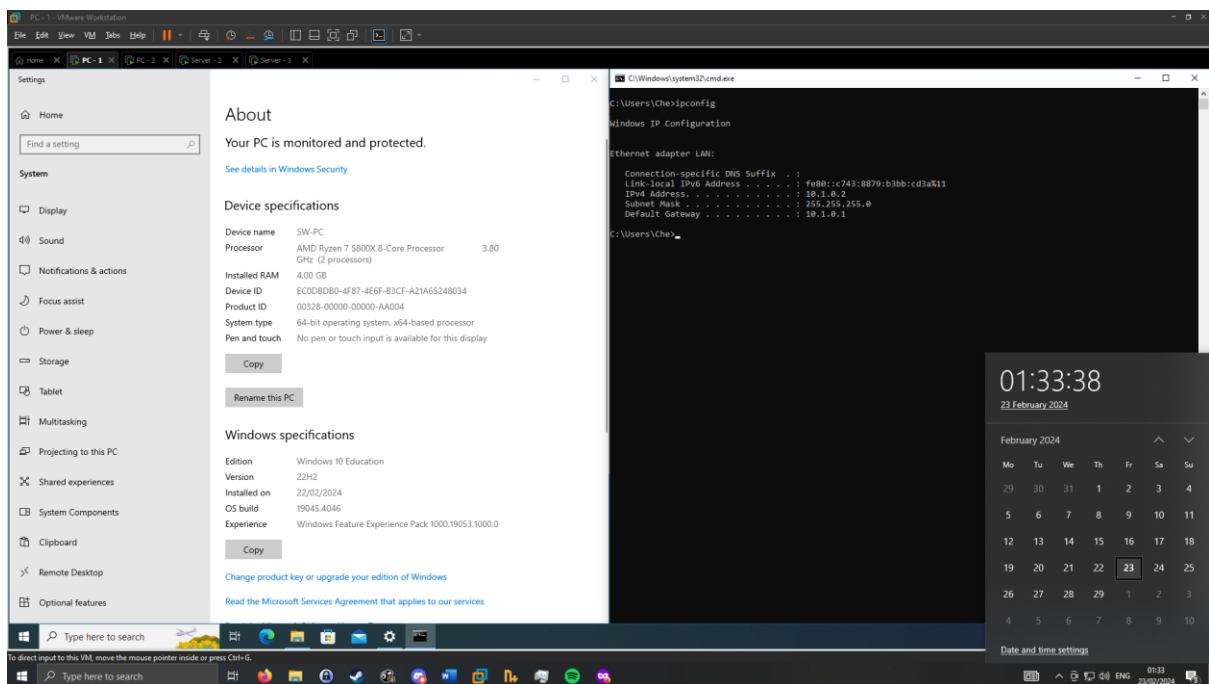


Figure 5 SW-PC IP Configuration

LD-PC IP Configuration

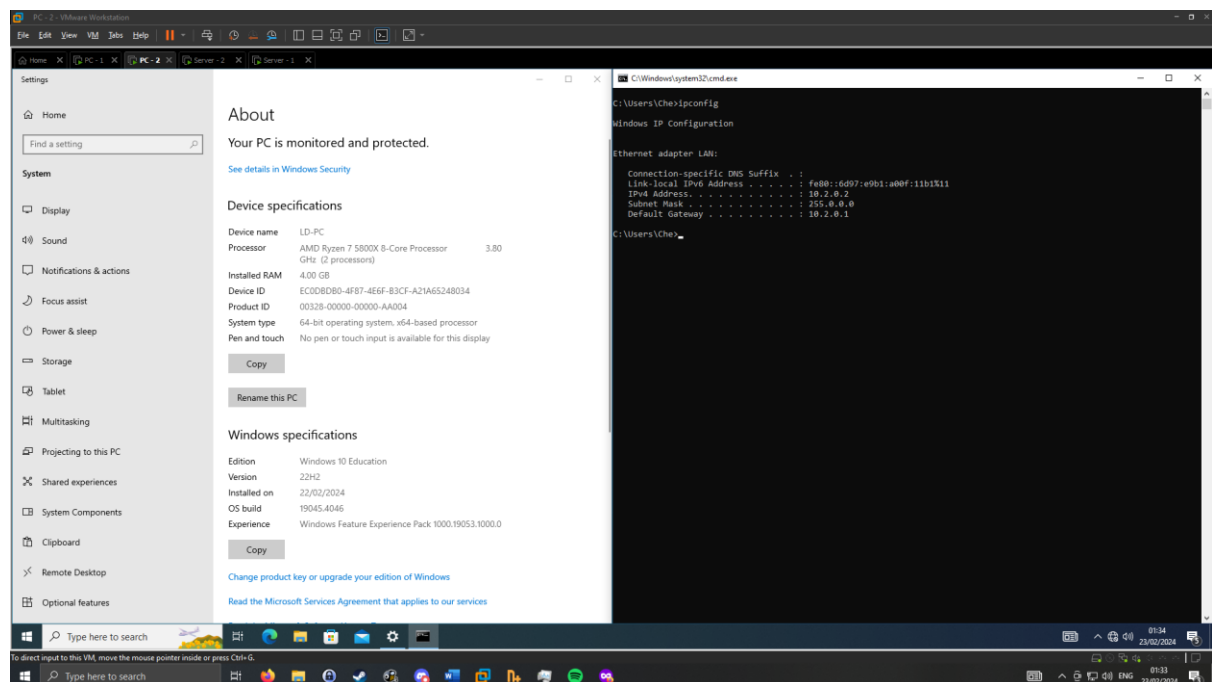


Figure 6 LD-PC IP Configuration

Testing the Network

Research on Network Testing and Troubleshooting

Network testing and troubleshooting can quite possibly be the most painful part of a network engineers' job, but none-the-less are something that need to be performed. Network testing defined is "the process of verifying the correct functioning and performance of a network infrastructure" [11]. Network testing is an imperative process as while some networks are setup automatically in modern times things don't always go as planned, some are still setup manually and can still suffer from human error leading to lack of connectivity and potential security risks within a network [12]. Focusing more on connectivity testing, there a few methods that a network engineer can go about completing this. One method is through direct inspection, this is a straightforward method that involves just checking that each part of the network can reach other parts, this can be done through pinging other parts of the network from each point and making sure that you get a successful response [12]. An example of this taken from my own network shown below shows that Server-1 can connect to Server-2 (192.1.1.2) and PC-1 (10.1.0.2).

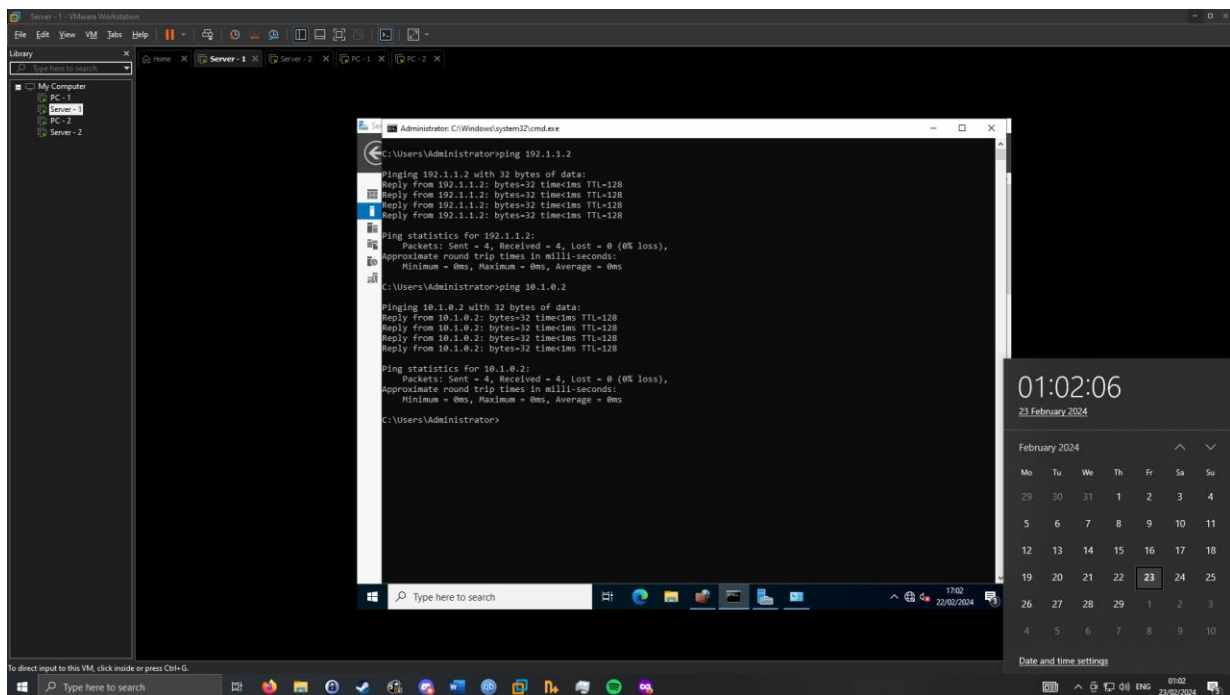


Figure 7 Server-1 pinging Server-2 and PC-1

Another way of testing network connectivity is through tracerouting. This process looks for all routers between a host where the command is performed, each router encountered along the way is called a “hop”, this process will allow the engineer to check that when traffic is sent, it follows the intended path [11].

Bandwidth testing is a process used to test “the data transfer rate or speed of a network or internet connection which evaluates both upload and download speeds” [13]. This process can provide the user with information on how fast or slow their internet connection is and can help them identify any issues with their network such as if their connection could be slower on Wi-Fi or Ethernet for example. It could also aid the user in seeing how capable their internet connection is.

Security testing is another important part of network testing. Network testing can allow organisations and users to identify any security vulnerabilities or risks within their network and can aid in these being patched as quickly as possible, these ideally should also be done on a regular basis as cyber criminals are always coming up with new ways to penetrate and harm networks [14]. There are multiple ways security testing can be performed, one of the most popular is through penetration testing. Companies can pay other companies who specialise in this to externally or internally pentest their system. External pentesting is where a tester starts from outside the network and attempts to breach the network using vulnerabilities or sometimes even social engineering, while internal pentesting is when someone starts from within the company and attempts to abuse their permissions to gain access to information that they should not have access to [14].

Testing the Connectivity of my Network

SW-DC ping SW-PC (and vice-versa)

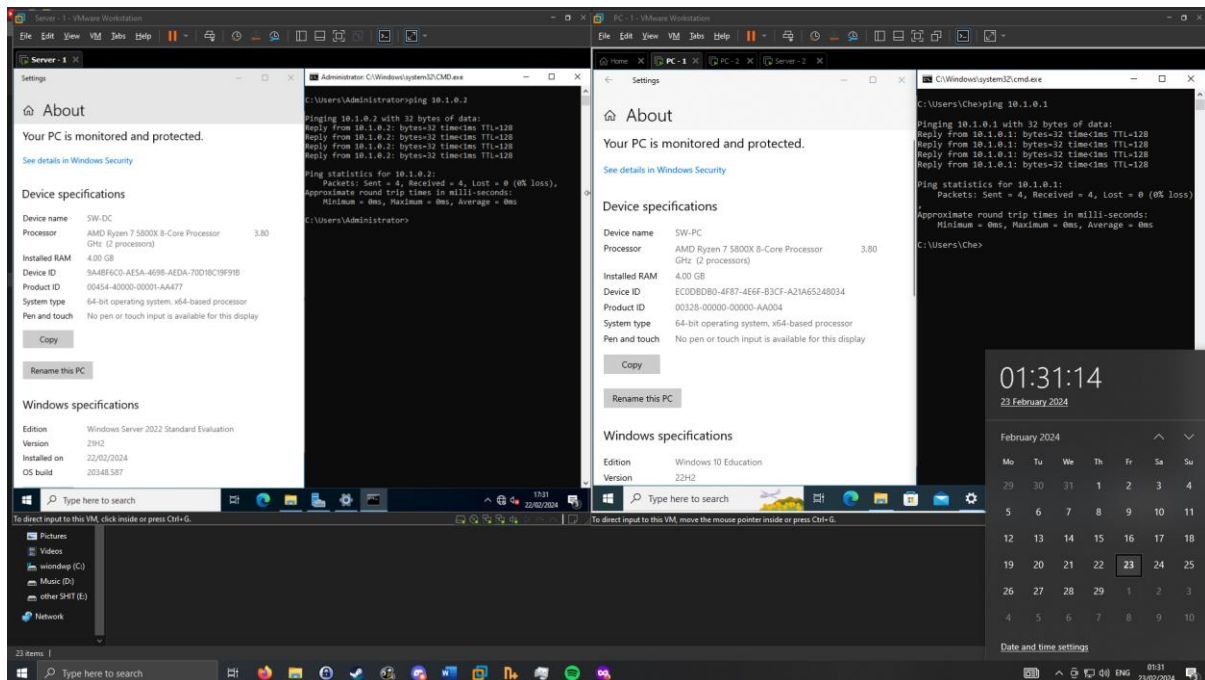


Figure SW-DC ping SW-PC (and vice-versa)

SW-DC ping LD-DC (and vice-versa)

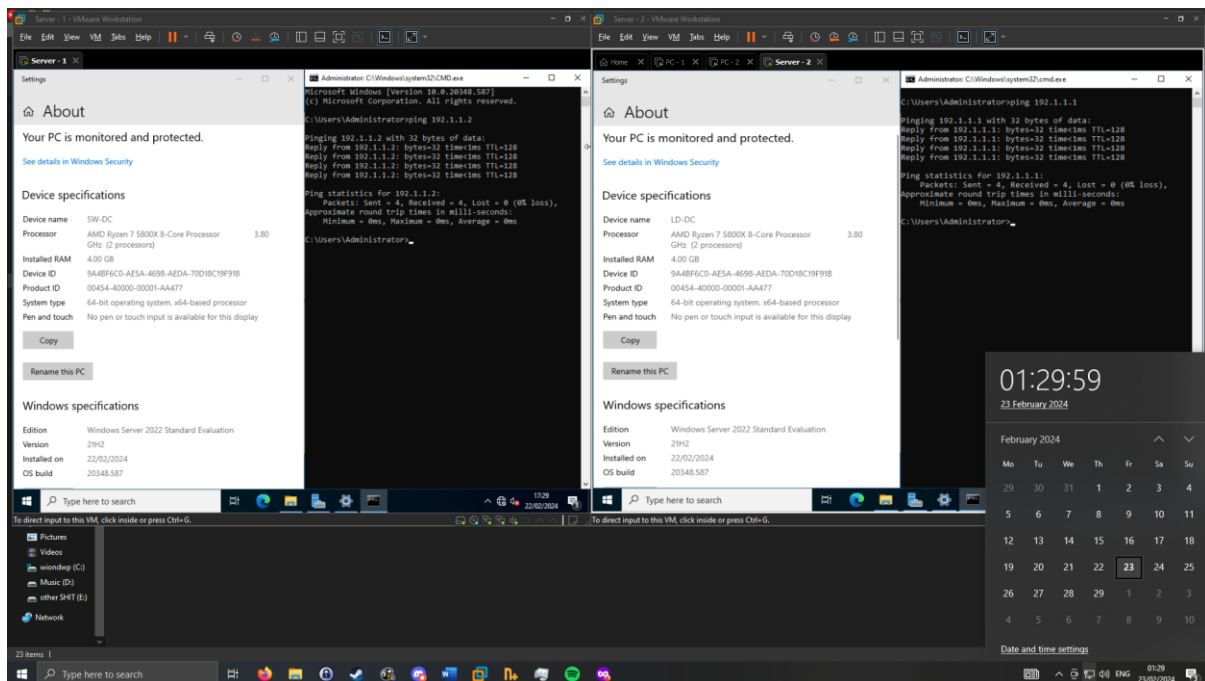


Figure 8 SW-DC ping LD-DC (and vice-versa)

LD-DC pinging LD-PC (and vice-versa)

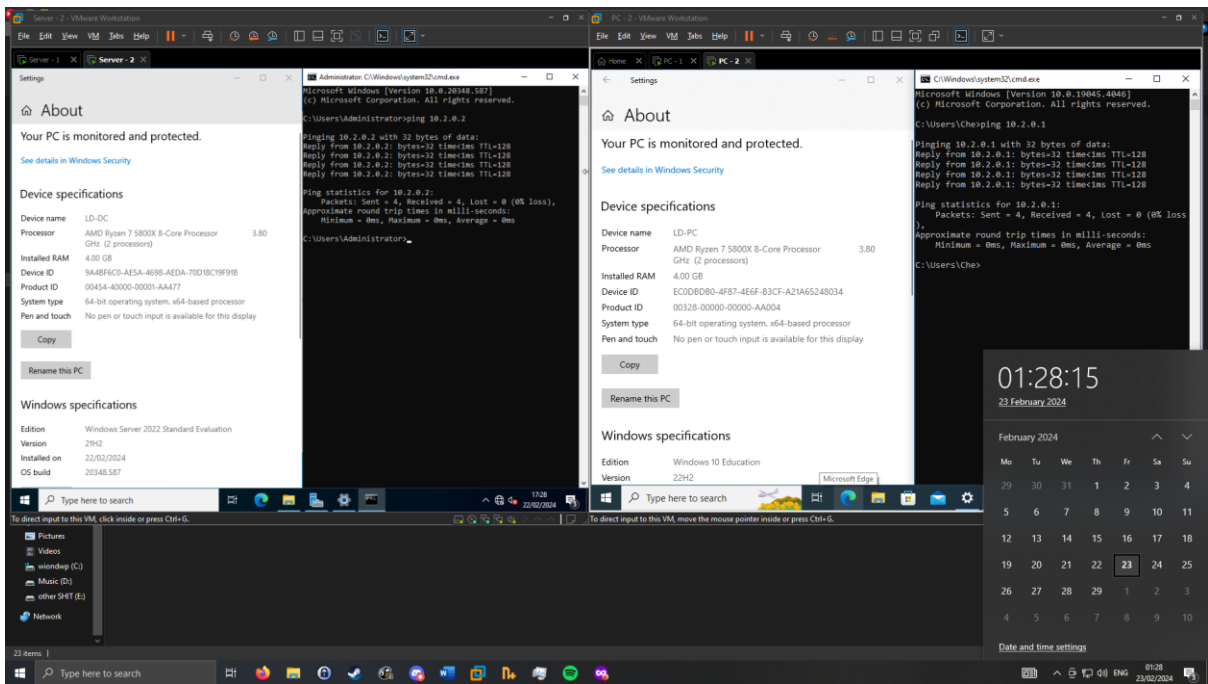


Figure 9 LD-DC pinging LD-PC (and vice-versa)

Issues Faced

I faced a few issues while configuring my network, mainly issues with the PCs pinging back to the servers and the servers pinging each other. I found that the servers could ping the PCs fine and that would work but if the PC tried to ping the server or the servers tried to ping each other, it would fail. I did some google searching as well as speaking to one of my friends who has some experience with networking and runs his own network hosting company online and it came down to the fact that there's a certain firewall rule on Windows Server that is disabled by default called "File and Printer Sharing (Echo Request - ICMPv4-In)" which completely blocks pings that are inbound to the server (shown in the screenshot on SW-DC). After enabling this inbound rule in the Windows Defender Firewall on both of the server machines, the pings went through fine, and we had excellent connectivity throughout the entire network.

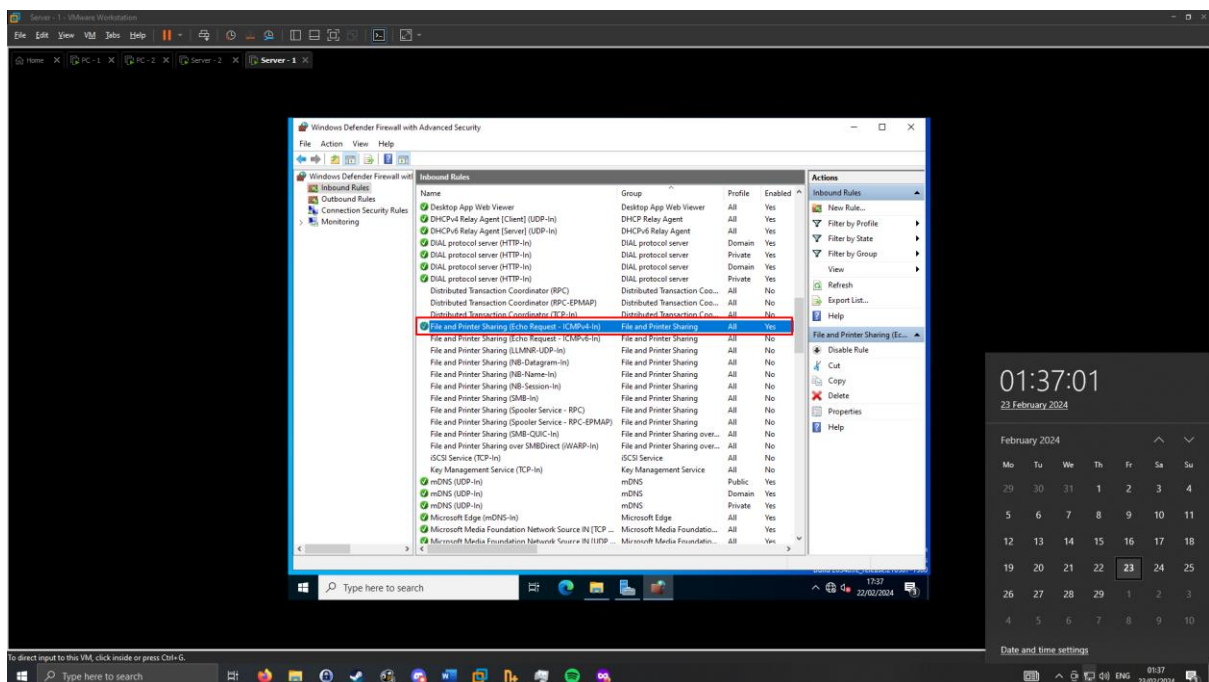


Figure 10 Firewall rules on SW-DC

References

- [1] E. Bugnion, D. Tsafirir and J. Nieh, *Hardware and software support for virtualization*, San Rafael, California: Morgan & Claypool Publishers, 2017. doi: 10.2200/S00754ED1V01Y201701CAC038
- [2] S. Meier, *IBM Systems Virtualization: Servers, Storage, and Software*, 2008.
- [3] S. Simic. "What is a Hypervisor? Types of Hypervisors Explained (1 & 2)." Knowledge Base by phoenixNAP. <https://phoenixnap.com/kb/what-is-hypervisor-type-1-2> (accessed Feb 18,).
- [4] P. K. Das and G. C. Deka, *Design and use of virtualization technology in cloud computing*, Hershey, PA: Engineering Science Reference, 2017. doi: 10.4018/978-1-5225-2785-5
- [5] "Type 1 vs. Type 2 Hypervisor: What Is The Difference?", *StarWind Blog*, <https://www.starwindsoftware.com/blog/type-1-vs-type-2-hypervisor-what-is-the-difference> (accessed Feb 18, 2024).
- [6] "What is an IP Address? How it works? How to Locate it?" Fortinet. [/uk/resources/cyberglossary/what-is-ip-address.html](https://www.fortinet.com/resources/cyberglossary/what-is-ip-address.html) (accessed Feb 18,).
- [7] Open University, "Data networks and IP addresses: View as single page | OLCreato," Accessed: Feb 18, 2024, [Online]. Available: <https://www.open.edu/openlearncreate/mod/oucontent/view.php?id=129584&printable=1>
- [8] "What Is Subnetting? How Subnets Work - IT Glossary | SolarWinds." <https://www.solarwinds.com/resources/it-glossary/subnetting> (accessed Feb 18,).
- [9] R. Molenaar, "What is Subnetting?", *NetworkLessons.com*, <https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/what-is-subnetting> (accessed Feb 23, 2024).
- [10] "How Does a Router Work?" Cisco. <https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/how-does-a-router-work.html> (accessed Feb 23,).
- [11] S. Gridelli. "Network Testing Tools and Best Practices." NetBeez. <https://netbeez.net/blog/network-testing-tools/> (accessed Feb 23,).
- [12] T. Sochi, "Testing the Connectivity of Networks," vol. 9, no. 2, pp.239, 2014. doi: 10.4304/jnw.9.2.239-243.
- [13] "Bandwidth Test", *DevX*, <https://www.devx.com/terms/bandwidth-test/> (accessed Feb 23, 2024).
- [14] "Network Security Testing." Check Point Software. <https://www.checkpoint.com/cyber-hub/cyber-security/cyber-security-testing-types-of-cybersecurity-testing/network-security-testing/> (accessed Feb 23,).