

Build, Deploy, Configure and Manage a Type 2 Hypervisor Platform Based Virtualised Network

1st Given Edward Patch
Software Engineer Student (of HND Year 2)
Network Operating Systems and Services
University of Wales Trinity St. Davids (of Nitheesh Murugan Kaliyamurthy)
 Swansea, Wales
 Student ID: 1801492

CONTENTS

I	Introduction	1
II	Worksheet One - Practical	1
II-A	Windows Server - Creation	1
II-B	Windows Server - Installation	2
II-C	Windows Server - User Setup	3
II-D	Windows Server I - Networking	4
II-E	Windows Server I - Security	4
II-F	Windows Server II - Networking	5
II-G	Windows Server II - Security	5
II-H	Windows 10 Client - Creation	6
II-I	Windows 10 Client - Installation	6
II-J	Windows 10 Client - User Setup	8
II-K	Windows 10 Client I - Networking	8
II-L	Windows 10 Client I - Security	9
II-M	Windows 10 Client II - Networking	9
II-N	Windows 10 Client II - Security	10
II-O	Server I to Client I - Ping Test	10
II-P	Client I to Server I - Ping Test	10
II-Q	Server II to Client II - Ping Test	10
II-R	Client II to Server II - Ping Test	11
III	Worksheet One - Observational	11
III-A	Differences Between Hypervisors	11
III-B	IPv4 Addressing	11
III-C	Cloud-Computing	11
III-D	Terminologies	11
IV	Evaluation	12
IV-A	Firewall	12
V	Conclusion	12
VI	References	12

Abstract—Type 2 hypervisor platform-based virtualised network documentation.

Index Terms—Type-1, Type-2, Hypervisor

I. INTRODUCTION

This report separates into two sections:-

- Worksheet One - Practical.
- Worksheet One - Observational.

Resources required to complete the listed resources:-

- Type 2 Hypervisor Management Software.
- Server based Network Operating System and intrinsic services and features.
- Client based Network Operating systems and suitable, intrinsic/external features.

Worksheet One requires a virtual network configuration.

II. WORKSHEET ONE - PRACTICAL

A. Windows Server - Creation

Step One

Figure 1 displays VirtualBox's Create Virtual Machine window. The following information is set:

Type: Microsoft Windows **Version:** Windows 2019 (64-bit)
Memory Size: 4096 MB

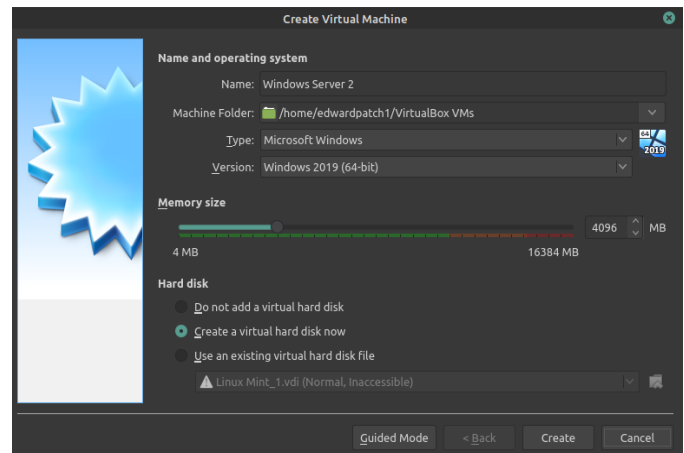


Fig. 1. Figure of Windows Server Creation.

Step Two

Figure 2 shows the VirtualBox's Create Virtual Hard Disk window. As shown in the figure, the hard drive is assigned a max of 30GB on a dynamically allocated drive. VirtualBox Disk Image (VDI) default file type is chosen.

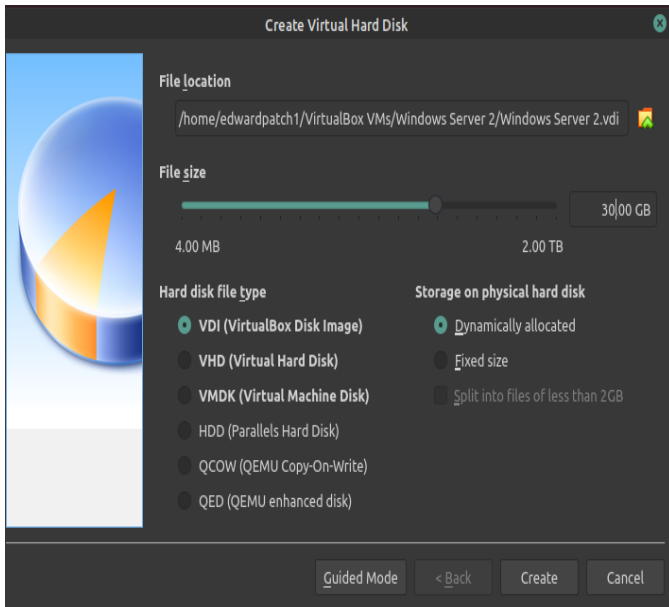


Fig. 2. Figure of Windows Server Creation.

Step Three

Figure 3 shows the Settings - Storage window. The storage option enables the user to add boot images or storage methods to the virtual machine. Shown in this screenshot, is the Windows Server 2019 image. Windows Server 2019 image was fetched from [Azure Software](#).

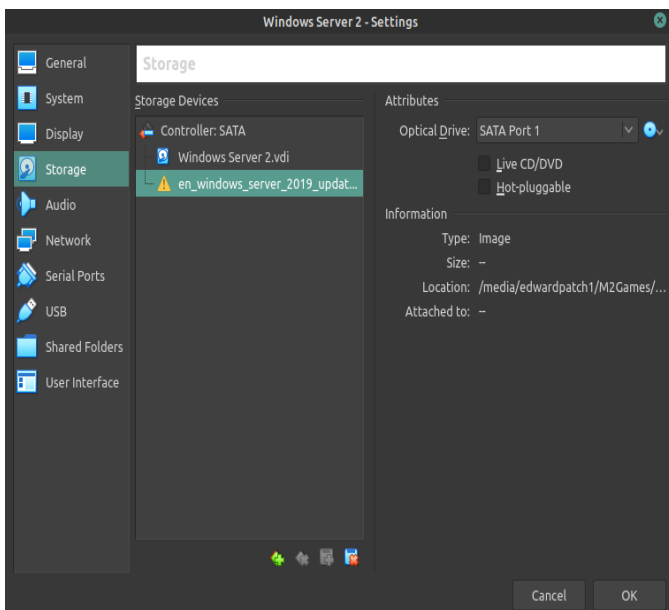


Fig. 3. Figure of Windows Server Creation.

B. Windows Server - Installation

Step One

Figure 4 shows the startup screen of the Window Server start-up window. This menu enables the user to choose their language, regional and keyboard settings.

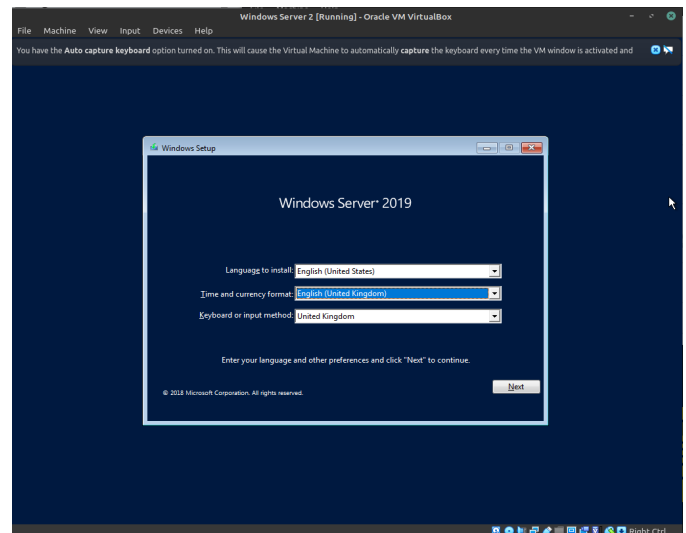


Fig. 4. Figure of Windows Server Installation.

Step Two

Figure 5 shows the Activate Windows window. Product key displayed as evidence is obtained from [Azure Software](#).

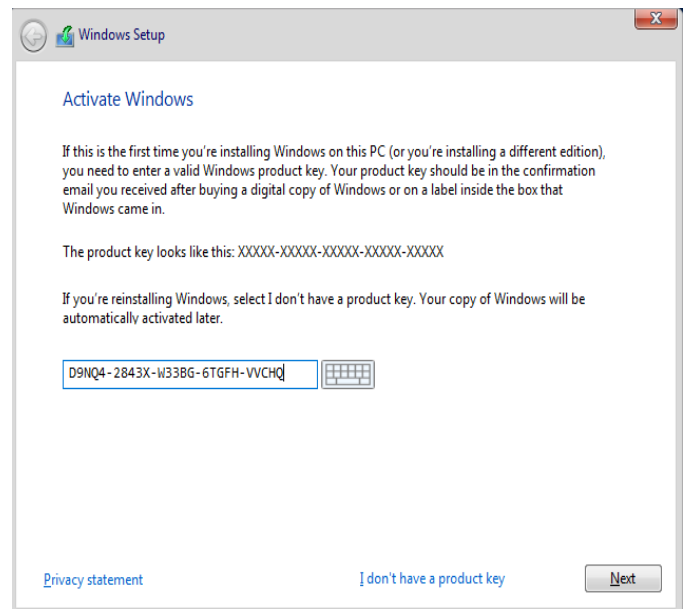


Fig. 5. Figure of Windows Server Installation.

Step Three

Figure 6 shows the Operating System Selection. Here the user can choose which operating systems are offered. In this case, **Windows Server 2019 Standard** is command-line only. Whereas the **Windows Server 2019 Standard (Desktop Experience)** offers Graphical User Interface (GUI) to manage the server. The second option is chosen for this setup.

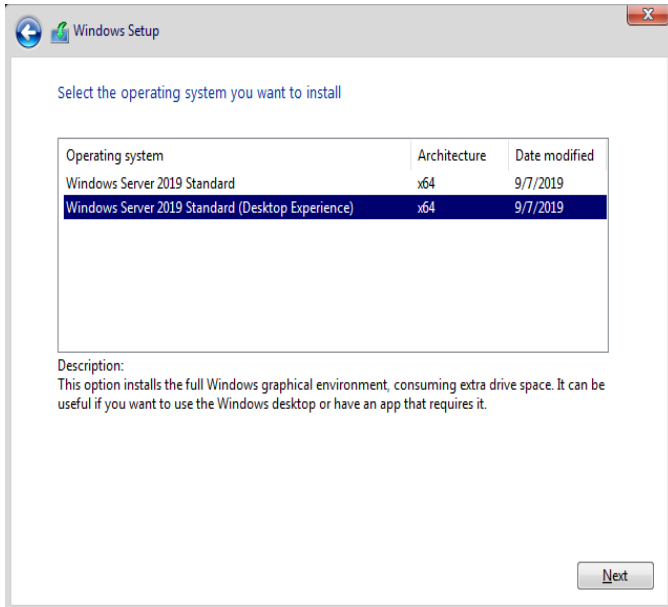


Fig. 6. Figure of Windows Server Installation.

Step Four

Figure 7 shows a window that offers the types of installations. The two options included are **Upgrade: Install Windows and Keep files, settings and applications** and **Custom: Install Windows only (advanced)**. As there is no operating system previously installed, the second option is selected in this case.

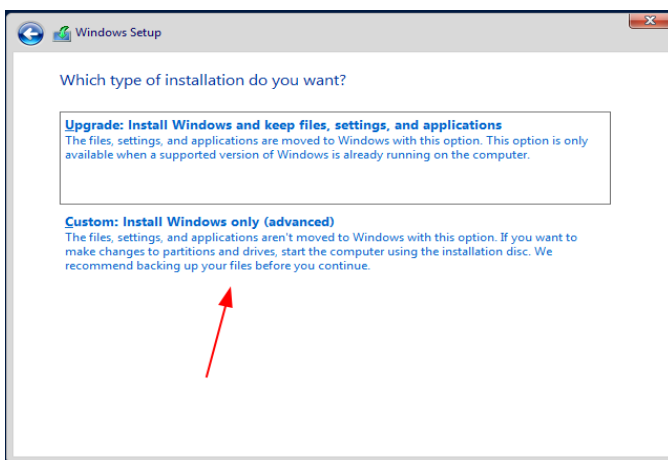


Fig. 7. Figure of Windows Server Installation.

Step Five

Figure 8 shows the Partition window. The purpose of this window, allows the user to create, delete, format partitions. The unallocated space is selected and next is pressed to choose the main unformatted drive. The installation wizard process will format and create system partitions accordingly.

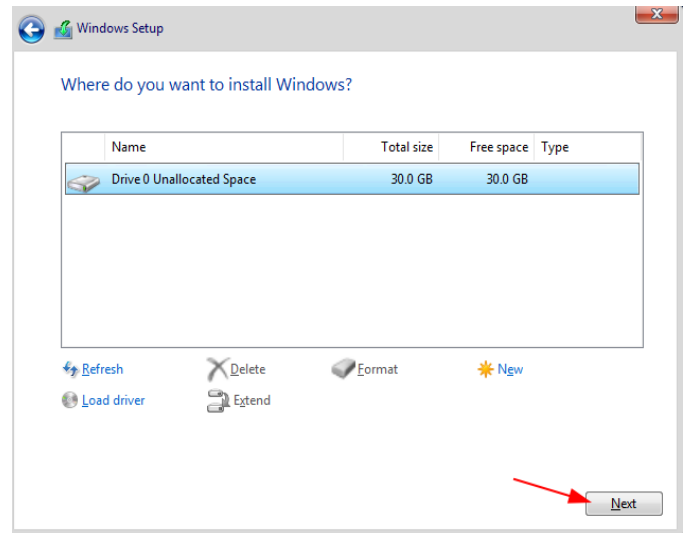


Fig. 8. Figure of Windows Server Installation.

C. Windows Server - User Setup

Figure 9 shows the Customise Settings window, which allows the user to set a password. The chosen password is *P@ssw0rd*. Read about why this is not a strong password. Refer to article [Password Security: How to Avoid the Most Common Password Mistakes](https://zapier.com/blog/password-security/) by Larry Tremblay [1]. URL: <https://zapier.com/blog/password-security/>.

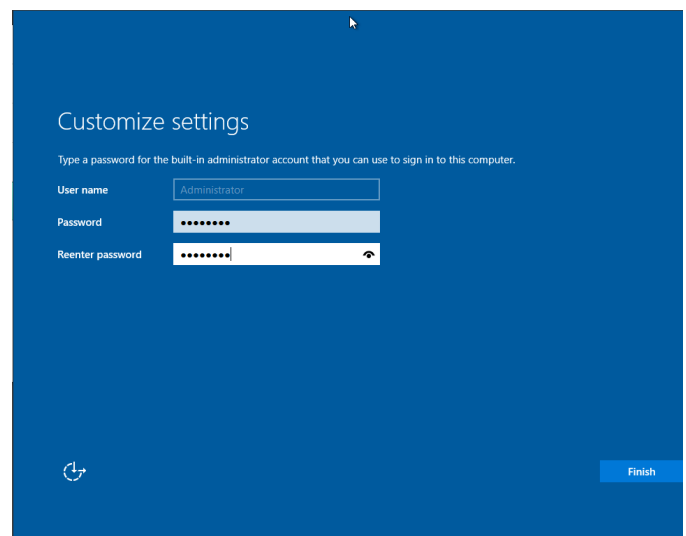


Fig. 9. Figure of Windows Server User Setup.

D. Windows Server I - Networking

Step One

Figure 10 displays the first network adapter renamed to *PrivateNet2* and second network adapter to *PublicNet*.



Fig. 10. Figure of Windows Server I Networking.

Step Two

Figure 11 shows PrivateNet1 adapter's IP address and subnet mask set to *IP:192.168.100.1 — Subnet Mask: 255.255.255.0*.

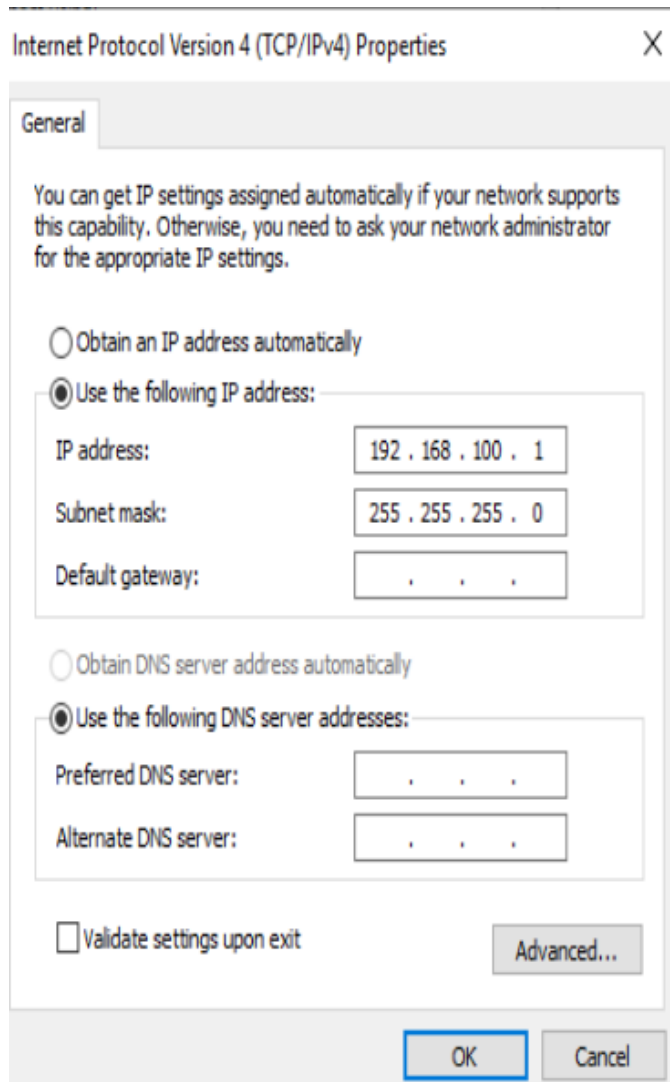


Fig. 11. Figure of Windows Server I Networking.

Step Three

Figure 12 shows PublicNet adapter's IP address and subnet mask set to *IP:192.168.1.100 — Subnet Mask: 255.255.255.0*.

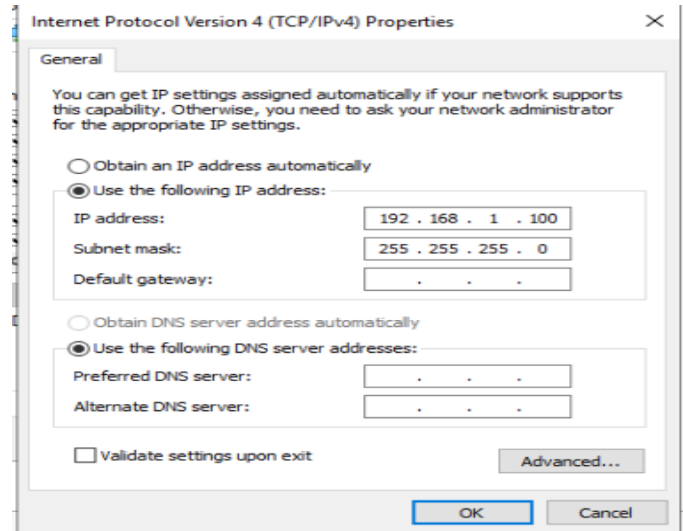


Fig. 12. Figure of Windows Server I Networking.

E. Windows Server I - Security

Screenshot shows the firewall of the system being disabled. This method allowed for the demonstration of Server I to communicate with Client I and vice versa. However, this process is **not recommended** under professional use, read more from the article [Why do I need a firewall?](https://www.netstar.co.uk/why-do-i-need-a-firewall-business/) by net-star [2] to understand why. URL: <https://www.netstar.co.uk/why-do-i-need-a-firewall-business/>

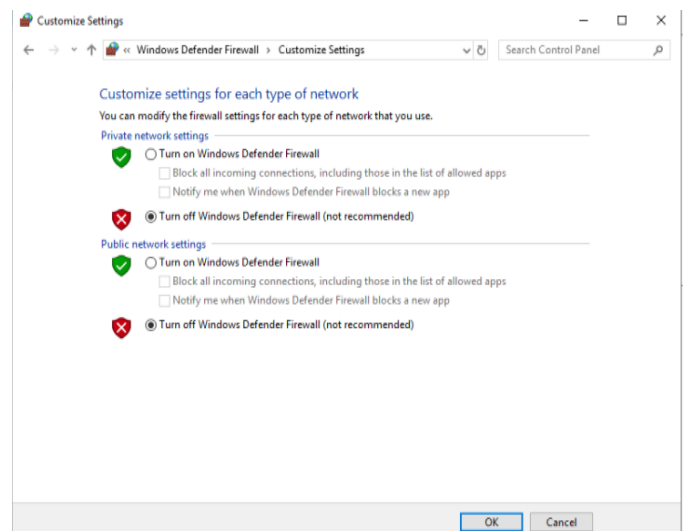


Fig. 13. Figure of Windows Server I Security.

F. Windows Server II - Networking

Step One

Figure 14 displays the first network adapter renamed to *PrivateNet1* and second network adapter to *PublicNet*. The reason to rename the adapters, is to help the Administrator know what adapter connects to which network.

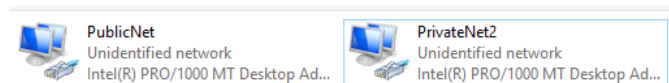


Fig. 14. Figure of Windows Server II Networking.

Step Two

Figure 15 shows PrivateNet2 adapter's IP address and subnet mask set to *IP:192.168.101.1 — Subnet Mask: 255.255.255.0*.

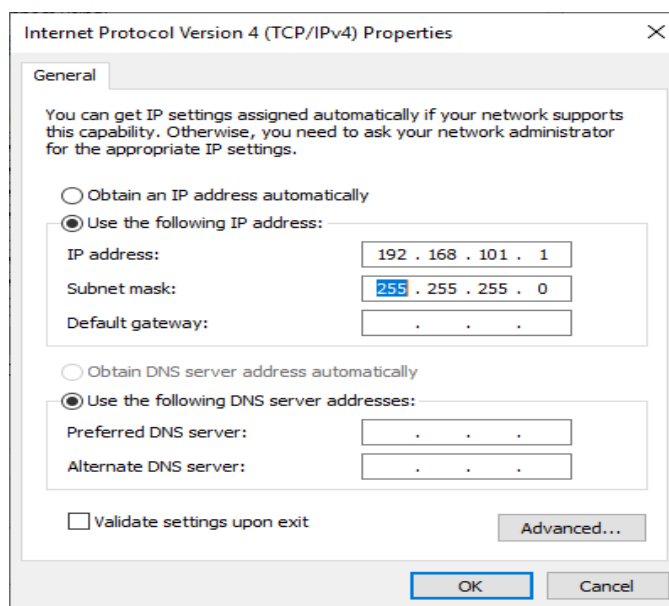


Fig. 15. Figure of Windows Server II Networking.

Step Three

Figure 16 shows PublicNet adapter's IP address and subnet mask set to *IP:192.168.1.101 — Subnet Mask: 255.255.255.0*.

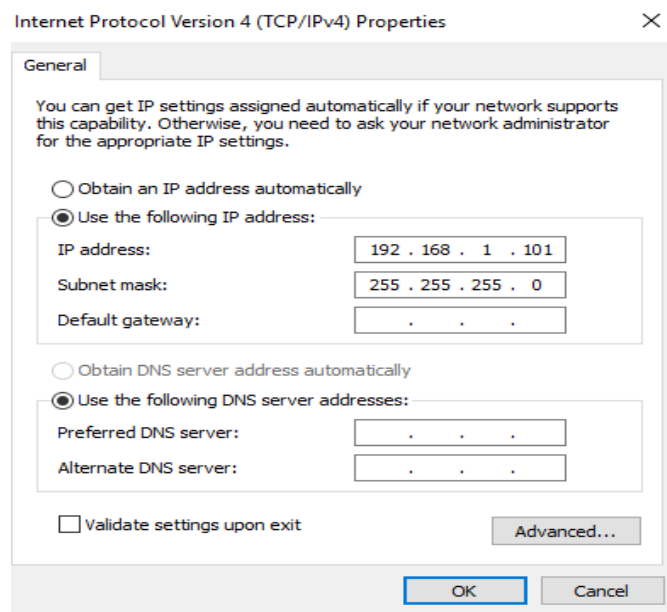


Fig. 16. Figure of Windows Server II Networking.

G. Windows Server II - Security

Screenshot shows the firewall of the system being disabled. This method allowed for the demonstration of Server II to communicate with Client II and vice versa.

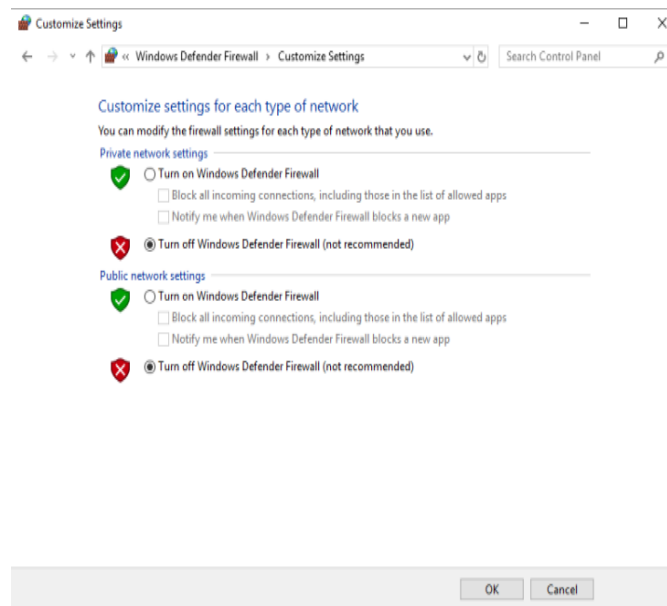


Fig. 17. Figure of Windows Server II Security.

H. Windows 10 Client - Creation

Step One

Figure 18 displays VirtualBox's Create Virtual Machine window. The following information is set:

Type: Microsoft Windows **Version:** Windows 10 (64-bit)
Memory Size: 4096 MB

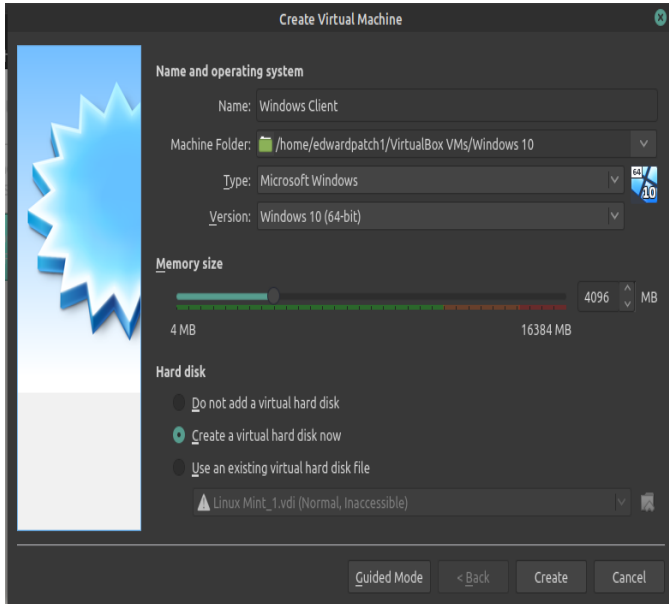


Fig. 18. Figure of Windows Client Creation.

Step Two

Figure 19 shows the VirtualBox's Create Virtual Hard Disk window. The file size is set to 30.00 GB. The rest of the properties are set as default.

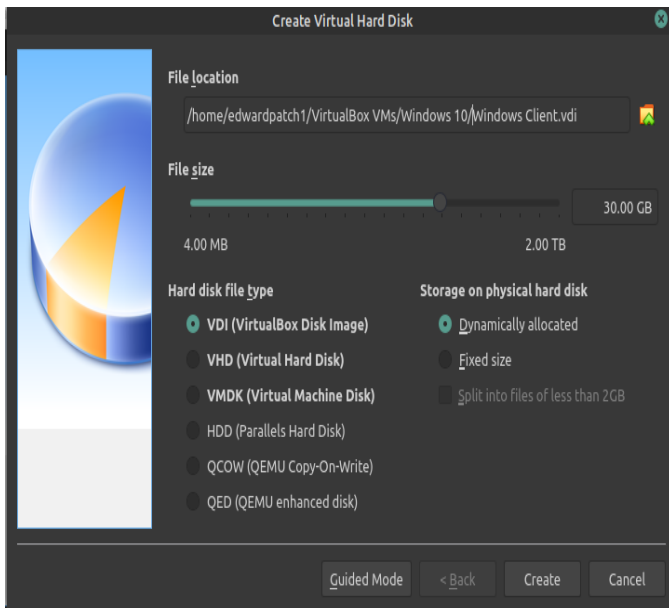


Fig. 19. Figure of Windows Client Creation.

Step Three

Figure 20 shows that VirtualBox's Settings - Storage window. Winndows 10 image file is chosen. This file has the boot image of Windows 10.

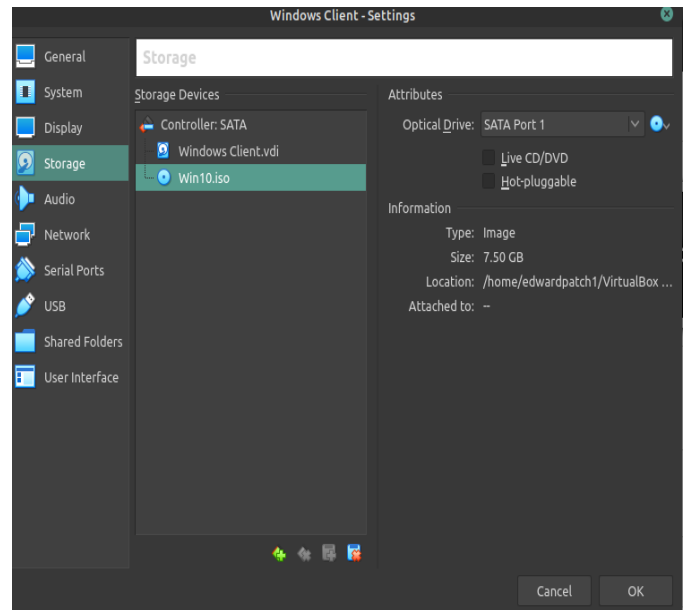


Fig. 20. Figure of Windows Client Creation.

I. Windows 10 Client - Installation

Step One

Figure 21 shows the startup window, similar to Windows 2019 server. This enables the user to select their language, region and keyboard method.

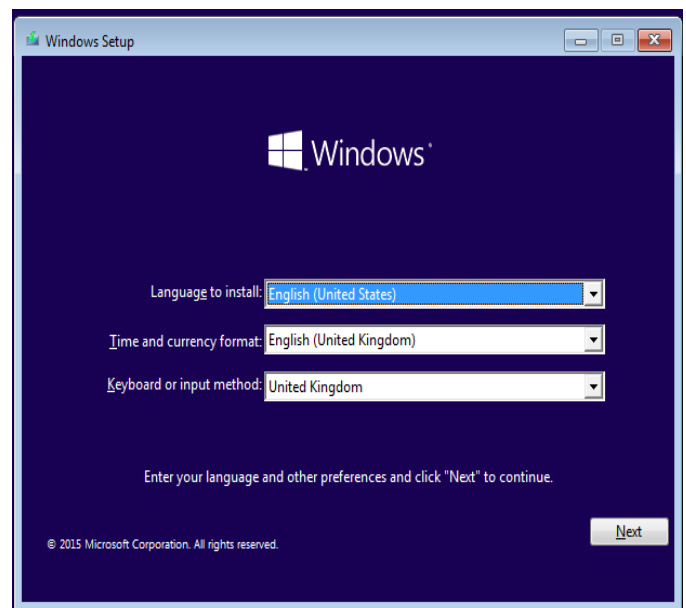


Fig. 21. Figure of Windows Client Installation.

Step Two

Figure 22 shows the next window. This window gives two options, **Install Now** and **Repair your computer**. The main option, Install Now, is chosen.

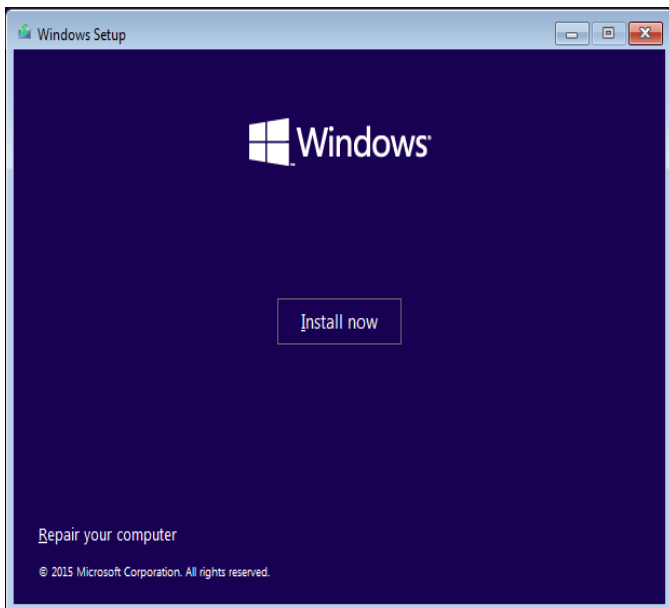


Fig. 22. Figure of Windows Client Installation.

Step Three

Similarly to the Windows Server 2019 windows installation, a operating system choice is given. Windows 10 Pro is selected.

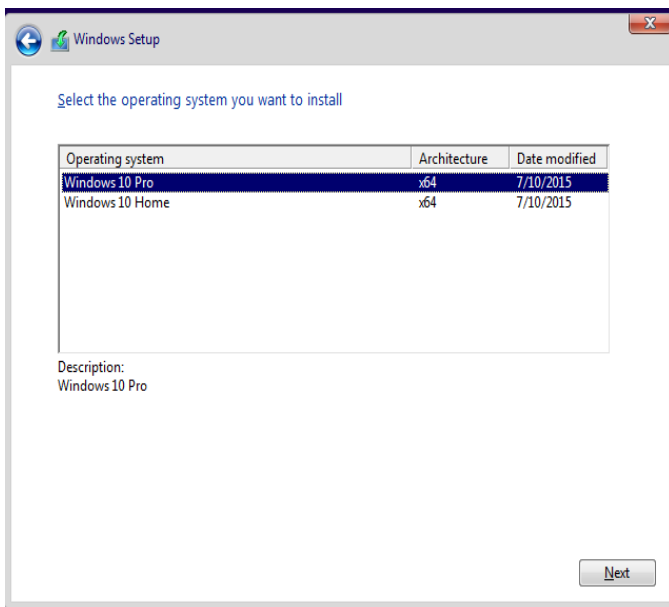


Fig. 23. Figure of Windows Client Installation.

Step Four

Figure 24 displays the terms and conditions of software use, with an empty checkbox. Make sure to read through the terms and conditions and click “I accept the license terms.” if agreed to. Next is then pressed.

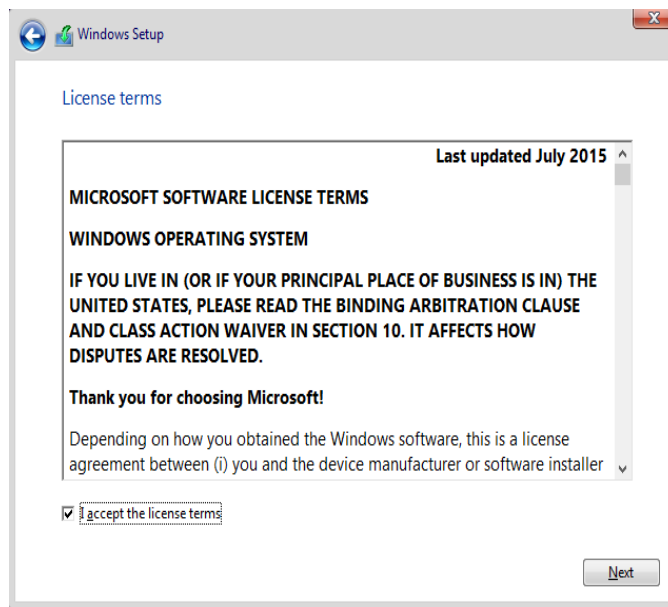


Fig. 24. Figure of Windows Client Installation.

Step Five

Figure 25 shows **Custom: Install Windows only (advanced)** is chosen.

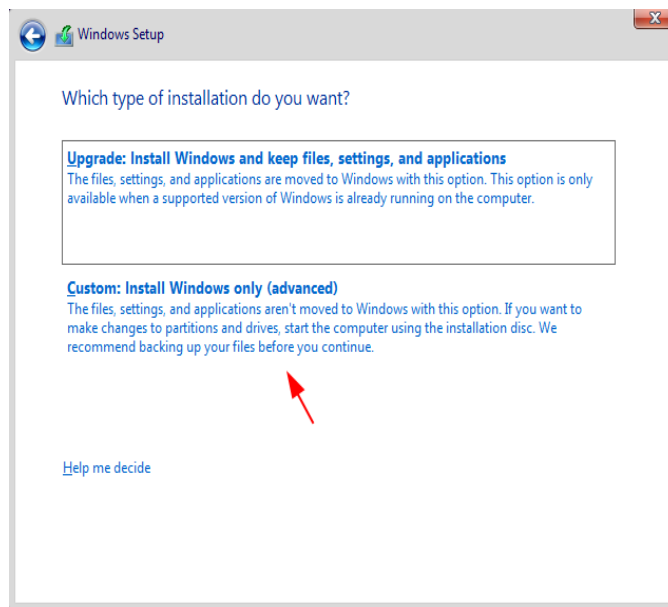


Fig. 25. Figure of Windows Client Installation.

Step Six

Drive 0 Unallocated Space is selected is chosen and next button is clicked.

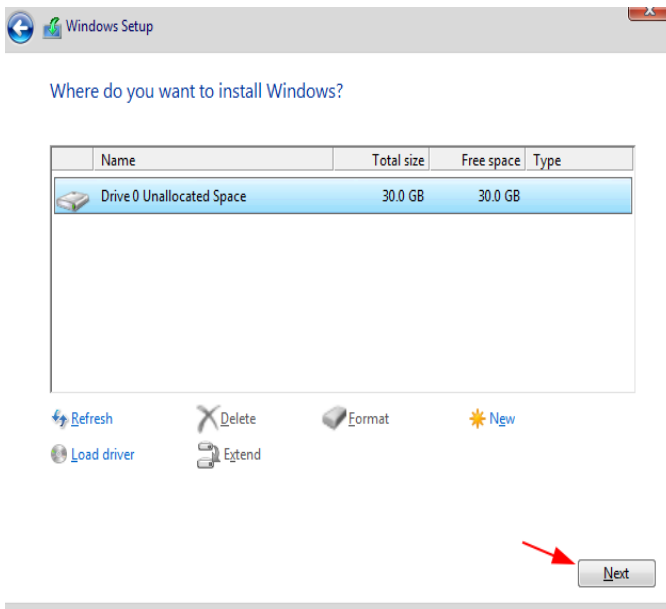


Fig. 26. Figure of Windows Client Installation.

J. Windows 10 Client - User Setup

The following information for the user setup is given:

Username: Edward **Password:** P@ssw0rd

Next is clicked.

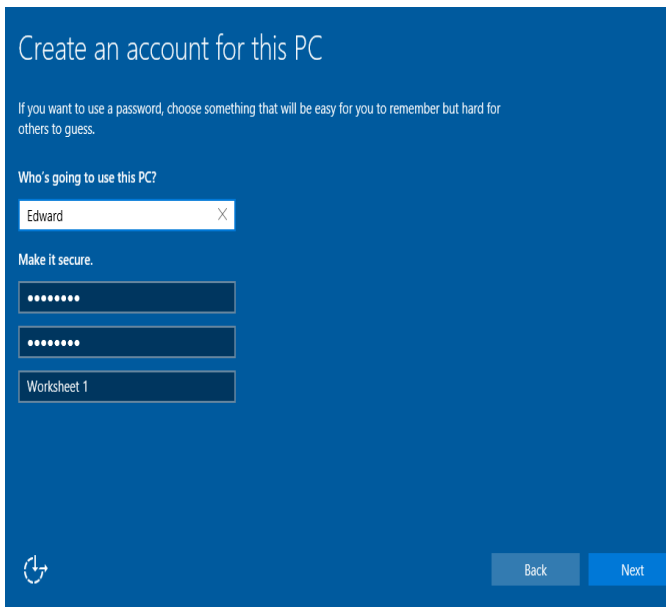


Fig. 27. Figure of Windows Client User Setup.

K. Windows 10 Client I - Networking

Step One

Renamed adapter 1 to *PrivateNet1*.

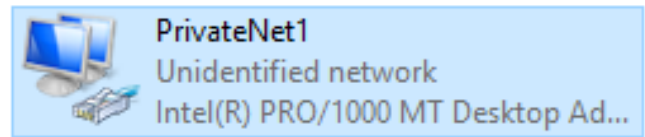


Fig. 28. Figure of Windows Client I Networking.

Step Two

Set IP of PrivateNet1 to *192.168.100.2* and subnet mask to *255.255.255.0*.

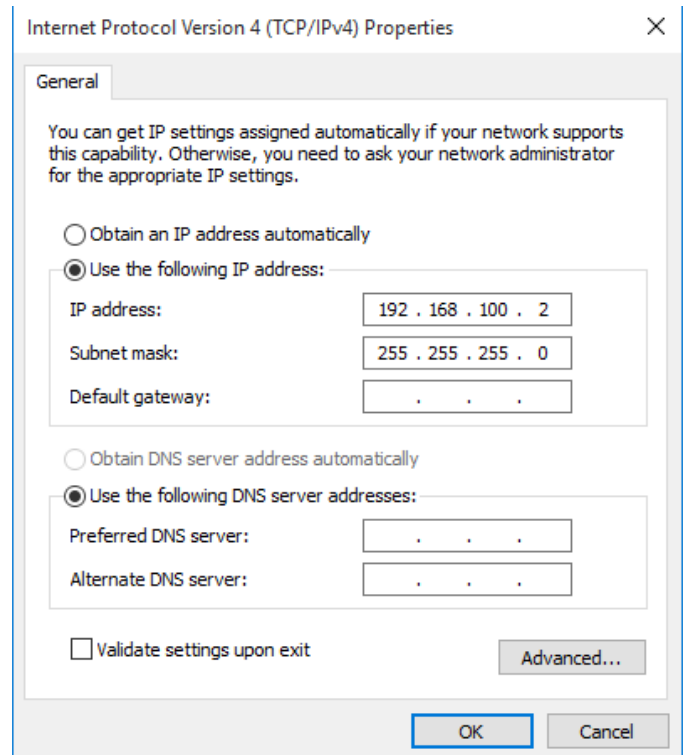


Fig. 29. Figure of Windows Client I Networking.

The figure 30 shows that the firewall is turned off. This allows the communication for Client I to communicate with Server I.

L. Windows 10 Client I - Security

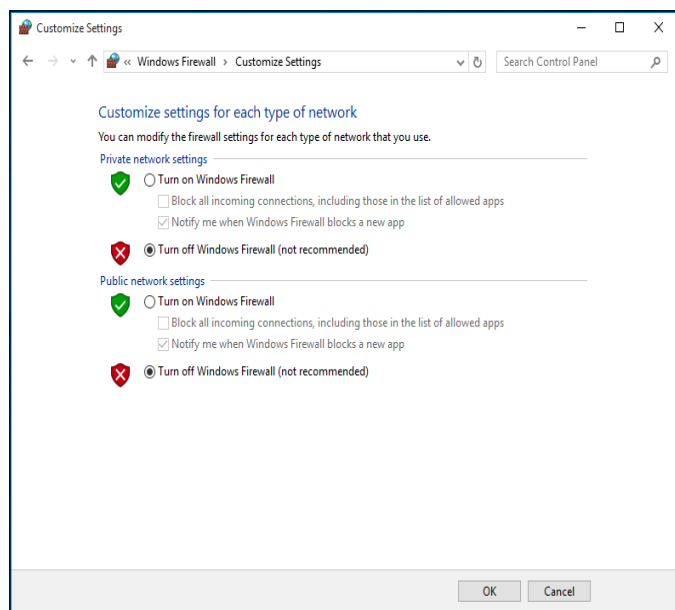


Fig. 30. Figure of Windows Client I Security.

M. Windows 10 Client II - Networking

Step One

Renamed adapter 1 to *PrivateNet2*.

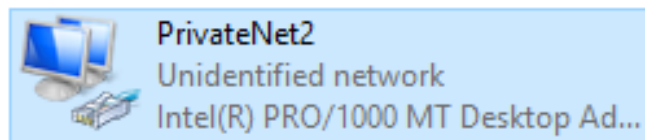


Fig. 31. Figure of Windows Client II Networking.

Step Two

Set IP address of PrivateNet2 to *192.168.101.2* and subnet mask to *255.255.255.0*.

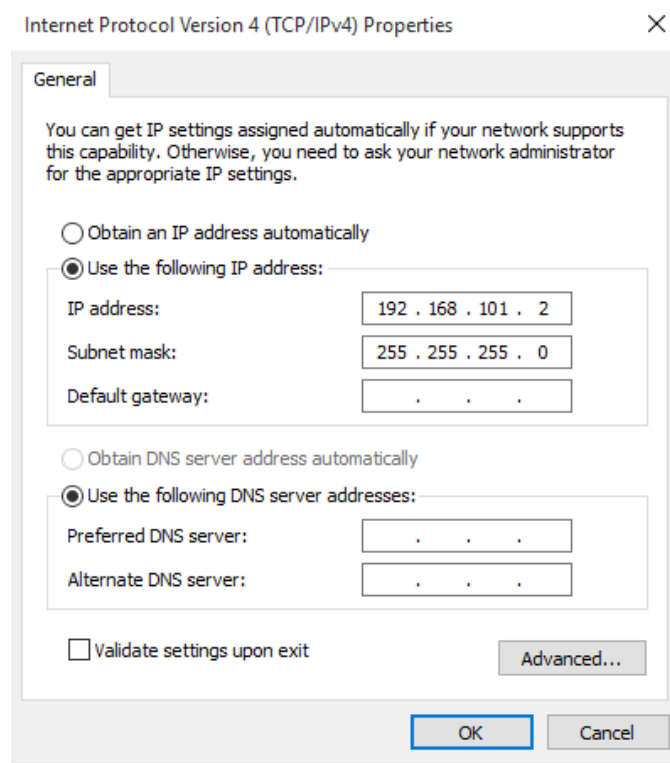


Fig. 32. Figure of Windows Client II Networking.

N. Windows 10 Client II - Security

Disabling the firewall allows Client II to communicate to Server II, without further configuration.

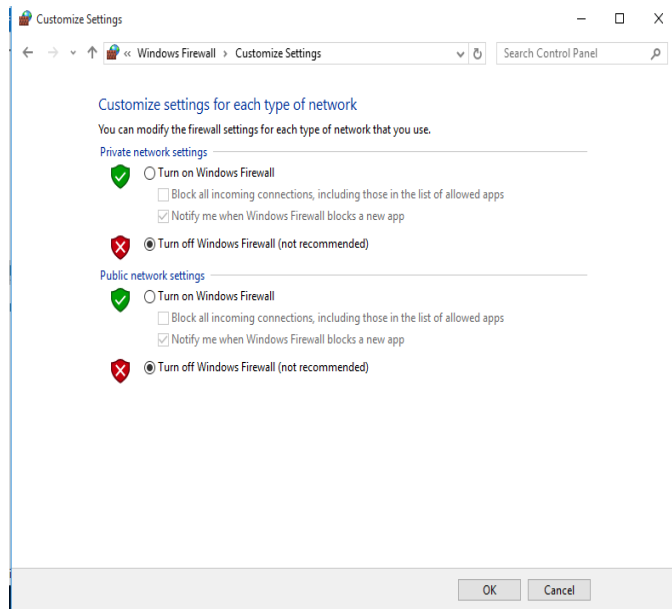


Fig. 33. Figure of Windows Client II Security.

O. Server I to Client I - Ping Test

The figure 34 shows a ping to Client I. Evidence displays successful pings.

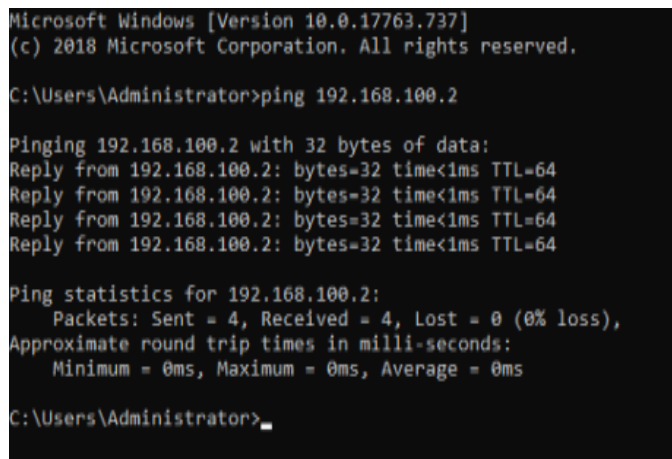


Fig. 34. Figure of Server I Ping to Client I.

P. Client I to Server I - Ping Test

The figure 35 shows a ping to Server I. Evidence displays successful pings.

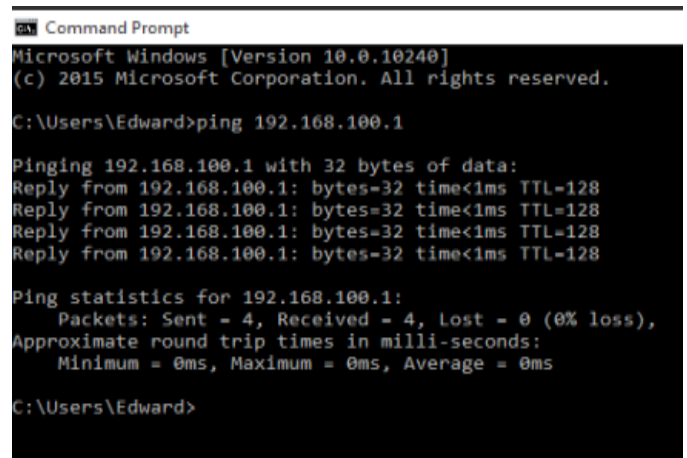


Fig. 35. Figure of Client I Ping to Server I.

Q. Server II to Client II - Ping Test

The figure 36 shows a ping to Client II. Evidence displays successful pings.

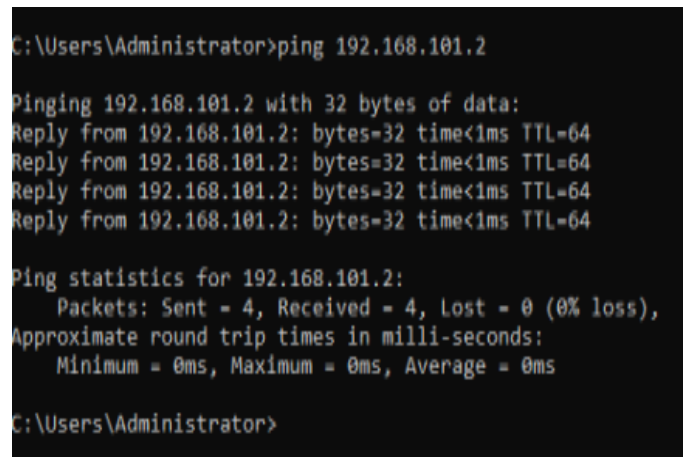
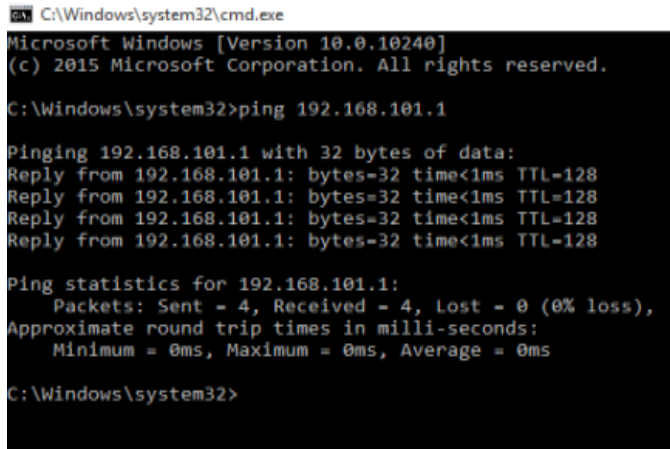


Fig. 36. Figure of Server II Ping to Client II.

R. Client II to Server II - Ping Test

The figure 37 shows a ping to Server II. Evidence displays successful pings.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 192.168.101.1

Pinging 192.168.101.1 with 32 bytes of data:
Reply from 192.168.101.1: bytes=32 time<1ms TTL=128
Reply from 192.168.101.1: bytes=32 time<1ms TTL=128
Reply from 192.168.101.1: bytes=32 time<1ms TTL=128
Reply from 192.168.101.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.101.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>
```

Fig. 37. Figure of Client II Ping to Server II.

III. WORKSHEET ONE - OBSERVATIONAL

A. Differences Between Hypervisors

Based on the article What is a Hypervisor? Types of Hypervisors 1 and 2, written by Sofija Simic [3], the main difference is type 1 hypervisor is a type of operating system. Whereas type 2 is a software-based application. A disadvantage of a type 2 hypervisor is that the software would share resources from the host operating system. An advantage of a type 2 hypervisor would be that it runs conveniently on any operating system, such as Windows, Linux and Mac.

A few vendors of Type 1 Hypervisors sourced from VapourApps [4] are listed:

- VMware.
- Microsoft Hyper-V.
- Citrix XenServer.

A few vendors of Type 2 Hypervisors sourced from VapourApps [4] are listed:

- Oracle VM VirtualBox.
- Microsoft Virtual PC.
- VMware Server.

B. IPv4 Addressing

The importance of subnet masking in IPv4 addressing is that it dictates how many hosts can use the network. The standard subnet masks that were used in practical exercises was slash 24. This specific mask enables 254 hosts and 256 addresses.

C. Cloud-Computing

Cloud-Computing services such as Microsoft Azure, Amazon AWS and Google Cloud, offers a remote virtual machine. These machines can be configured with different forms of specifications depending on the task ahead. These can be accessed via methods supplied by the cloud-computing company.

However, when configuring a remote virtual machine, the costs of the service may rise drastically. These services are not usually used by individuals but from a company stand point. Performance of the cloud-computing virtual machines can still vary on the internet speed uplink-downlink.

D. Terminologies

- **Firewall** - Protects outgoing and ingoing communications. Protects the user from unauthorised access.

Linux Distributions' (distro for short) are usually open-source. Any security issues found within the code can be reported or patched up by the operating system users. They can either upload their findings through official channels or keep their code for their usage. Therefore, because of Linux's constant patches from user input, having a firewall on personal systems are slim. However, user-made or custom company firewall applications usually made to suit the user/company needs.

List of a few open-source firewall applications for Linux Distributions from the article, Best free Linux firewalls of 2021: go beyond iptables for desktops and servers by Martin Meredith, Nick Peers, Nate Drake and Brian Turner [5]:-

- IPFire.
- OPNSense.
- ClearOS.
- OpenWRT.

Some open-source software is controlled by releasing older versions of code without exposing the current version. With this nature, it prevents hackers from being able to find vulnerabilities with the code. However, some open-source software is managed differently, which can prove a security risk. Finding closed-source or ordered open-source firewall products is recommended to keep your system safe from outside attacks.

- **PAE/NX** - Based on Oracle [6] PAW stands for Physical Address Extension. This option enables the virtual machine to access the full potential of the Host's CPU. This feature is only available on VirtualBox. However, other type 2 hypervisor software may offer other features.
- **NAT** - NAT stands for Network Address Translation. Cisco [7] NAT FAQ explains how NAT functions, "Basically, NAT allows a single device, such as a router, to act as an agent between the Internet (or public network) and a local network (or private network), which means that only a single unique IP address is required to represent an entire group of computers to anything outside their network."

IV. EVALUATION

The evaluation covers the importance of points mentioned throughout the setup and other security issues that a user needs to be mindful of when setting up a server.

A. Firewall

Why is it important?

Without a firewall on a server system, can cause further problems down the line. Issues vary from connections being made to a client within the network by accessing the server's permissions. Even if the client's firewall is off, the hacker could gain access to the client's system by providing themselves a false identification.

However, without firewall on a client system but with a firewall on a server would prove less challenge to the hacker to find vulnerabilities to the network. Regardless of the type of operating systems, in a network designed for professional and commercial use, it is important to have a **trusted** firewall in place. This is to protect confidential data such as company, staff and client data.

V. CONCLUSION

The Type 2 Hypervisor Management software, Oracle VM VirtualBox, now has four operating systems, Windows 2019 Server (Server I/II) and Windows 10 (Client I/II).

VI. REFERENCES

- [1] L. Tremblay, "Password Security: How to Avoid the Most Common Password Mistakes," Mar. 2019. [Online]. Available: <https://zapier.com/blog/password-security/>
- [2] netstar, "Why do I need a firewall? | Netstar IT Support London," Feb. 2021. [Online]. Available: <https://www.netstar.co.uk/why-do-i-need-a-firewall-business/>
- [3] S. Simic and PhoenixNAP, "How to Implement Validation for Restful Services with Spring," Jan. 2019. [Online]. Available: <https://phoenixnap.com/kb/what-is-hypervisor-type-1-2>
- [4] VapourApps, "What is Hypervisor and what types of hypervisors are there?" May 2016. [Online]. Available: <https://vapour-apps.com/what-is-hypervisor/>
- [5] M. Meredith, N. Peers, N. Drake, B. T. December 22, and 2020, "Best free Linux firewalls of 2021: go beyond iptables for desktops and servers," Dec. 2020. [Online]. Available: <https://www.techradar.com/uk/best/best-free-linux-firewalls>
- [6] Oracle, "Chapter 3. Configuring Virtual Machines." [Online]. Available: <https://www.virtualbox.org/manual/ch03.html>
- [7] Cisco, "Network Address Translation (NAT) FAQ - Cisco," Nov. 2020. [Online]. Available: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html>