

IT Technology
Networking Assignment 2



.....

University College

Authors

Aleksis Kairiss
Alexander Bjørk Andersen
Dainty Lyka Bihay Olsen
Daniel Rasmussen
Jacob Suurballe Petersen
Nikolaj Hult-Christensen
Sheriff Dibba

alka28793@edu.ucl.dk
aban28821@edu.ucl.dk
dlbo28887@edu.ucl.dk
dara28918@edu.ucl.dk
jspe28926@edu.ucl.dk
nihu28952@edu.ucl.dk
shdi28860@edu.ucl.dk

Wednesday 07 October 2020

Table of Contents

| | |
|---|----|
| Introduction | 1 |
| Audience | 1 |
| Inventory | 1 |
| Layer 3 network diagram | 2 |
| Setup VMnet3 in Virtual Network Editor | 2 |
| Explain what a host-only network is, and how to connect the host to it. | 4 |
| How to set static IP addresses on Linux hosts | 6 |
| Show the connectivity between virtual and physical hosts via ping | 7 |
| Show how to use TCP dump/wireshark to monitor traffic | 8 |
| Wireshark installation | 8 |
| Monitoring traffic | 8 |
| Extra: How to set up file sharing between two Linux hosts | 10 |
| Conclusion | 13 |

1 Introduction

This report will demonstrate the students' capability to set up a host-only network with 2 virtual machines inside VMware. The host/hypervisor computer must also be connected in this setup.

The student will also demonstrate setting static IP addresses, the connectivity between machines, the result of a TCP dump and how to set up file sharing between two Linux hosts.

2 Audience

This document is meant for teachers and fellow students alike, with the intention of receiving peer review from these parties.

3 Inventory

Software:

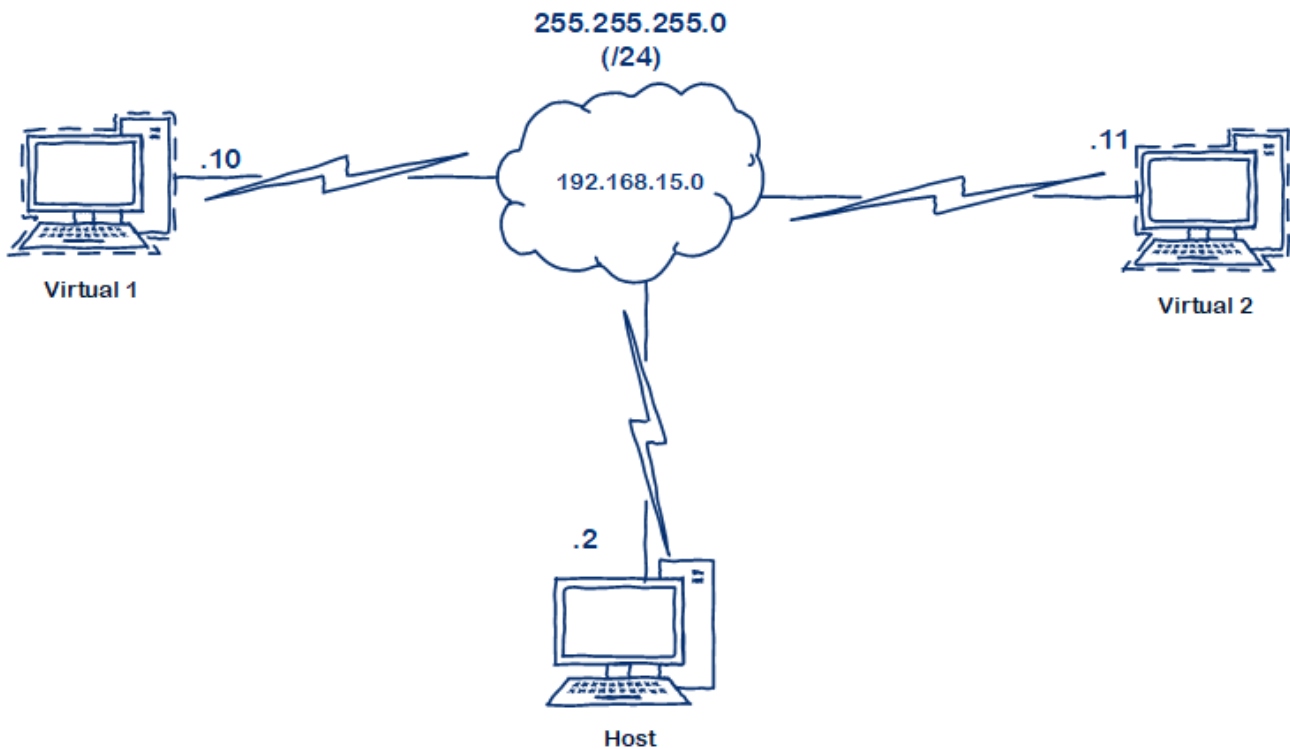
- VMware Workstation
- Wireshark
- Command Prompt
- Terminal
- Visio

Hardware:

- Host computer

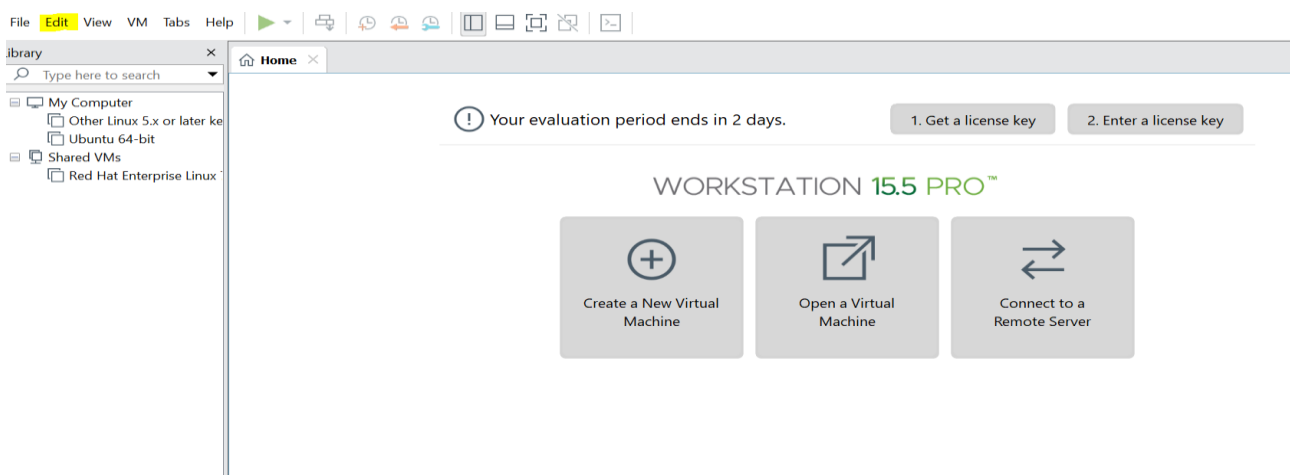
4 Layer 3 network diagram

In the picture below, we see a simple virtual network, with two virtual machines (192.168.15.10 and 192.168.15.11) hosted on a host machine (192.168.15.2). The virtual machines are on the /24 subnet.



5 Setup VMnet3 in Virtual Network Editor

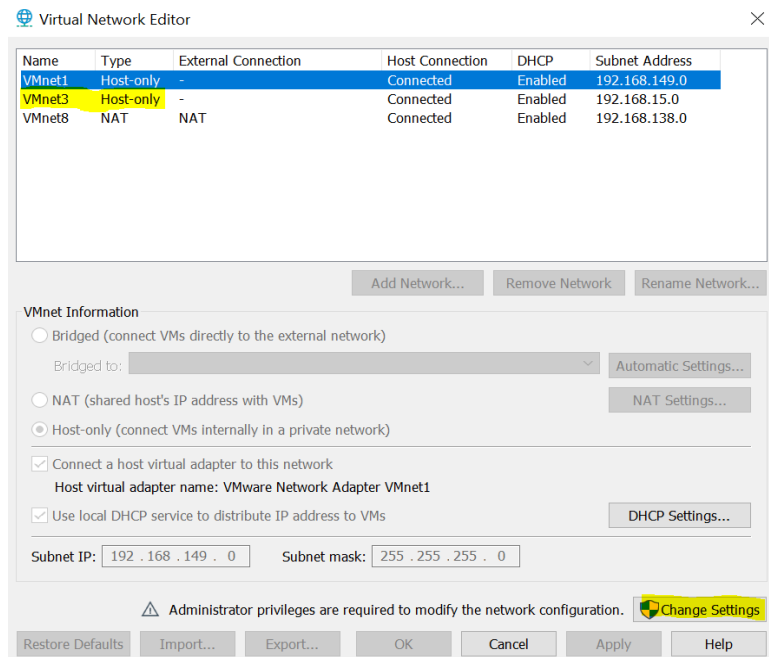
1) Go to VMware Workstation and click on “edit” in the left top corner.



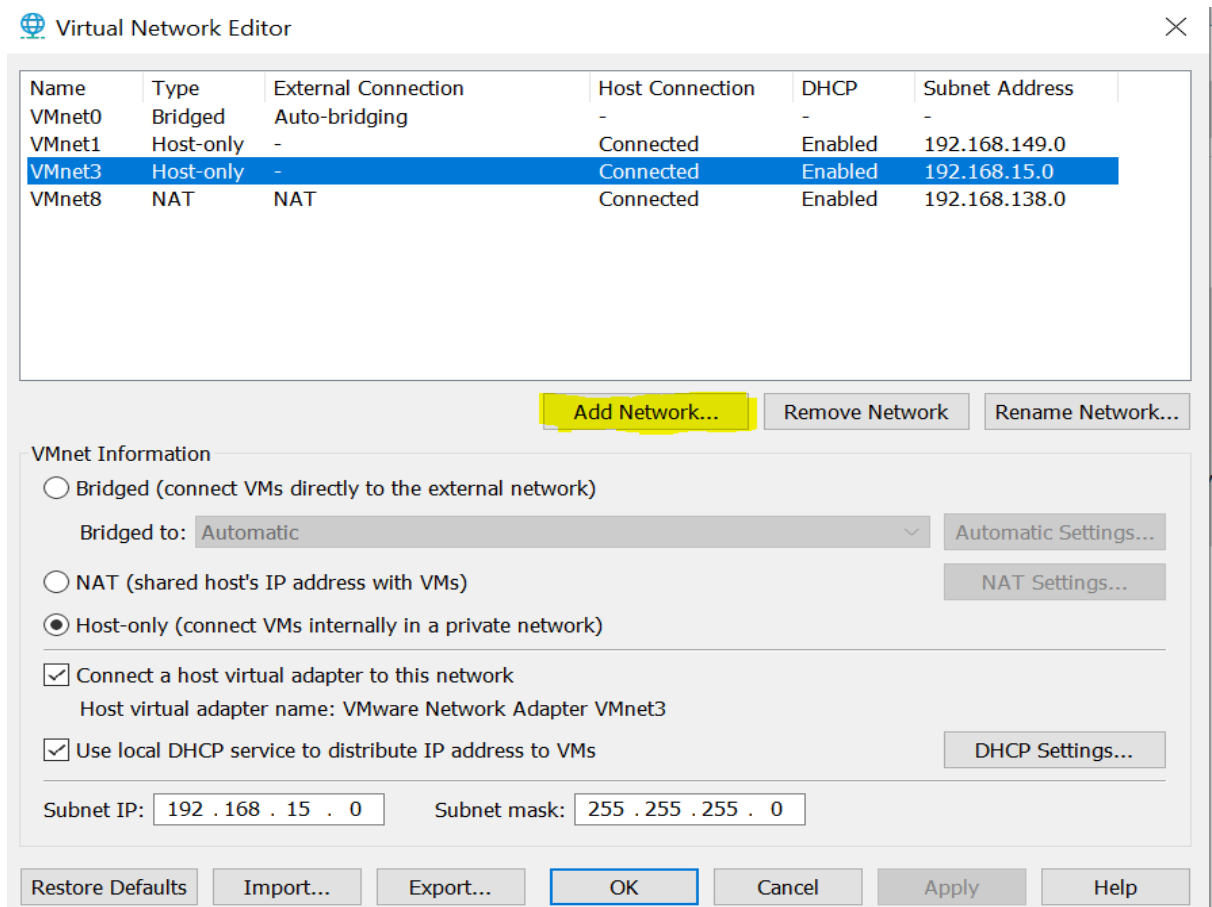
Click on “Virtual Network Editor” and you should see a screen which should be similar to this picture.

It is important to click on “Change settings” and grant administrator privileges, otherwise your computer will not have access to change anything.

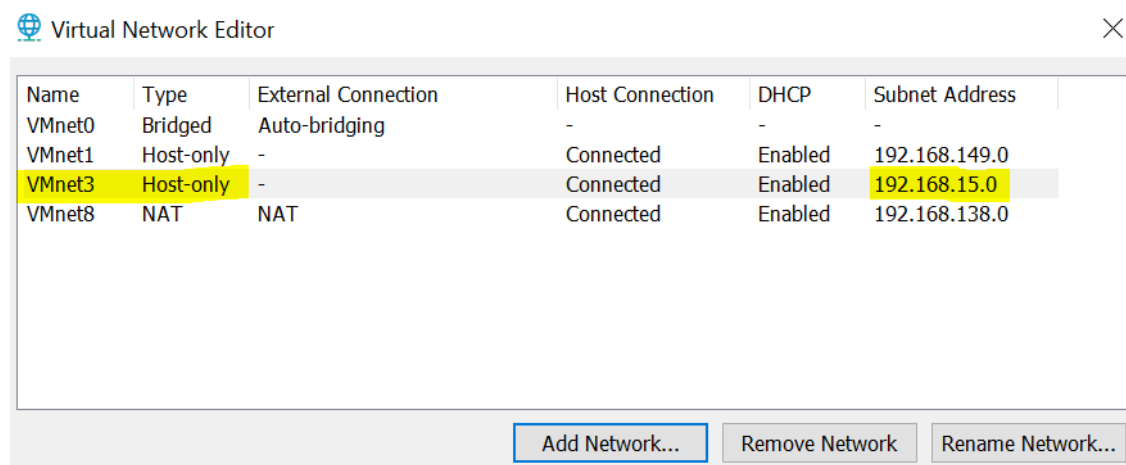
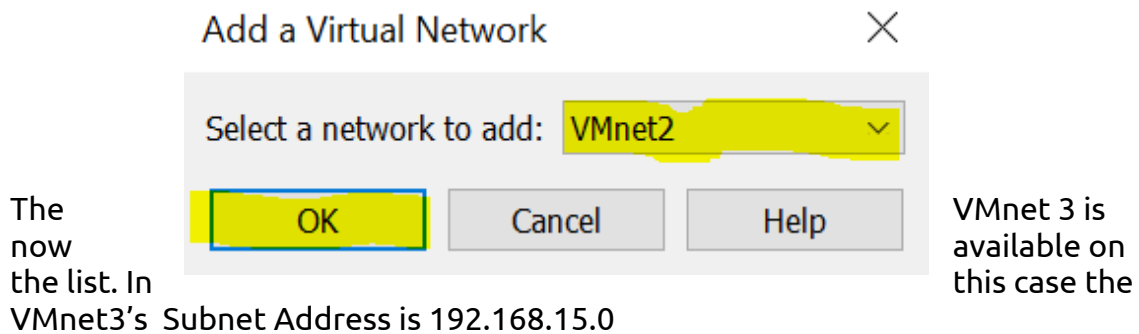
VMNet 3 on this machine is already on the list as shown in the picture. If not, you can simply click “Add network...” to add it.



Select Host-only in VMnet information field. Fill in the desired subnet IP , in this case it is 192.168.15.0 and a subnet mask of 255.255.255.0



Now the user has to choose “VMnet 3” in the following list and press “ok” (This picture show VMnet2 because the pc already has the VMnet3 up running)

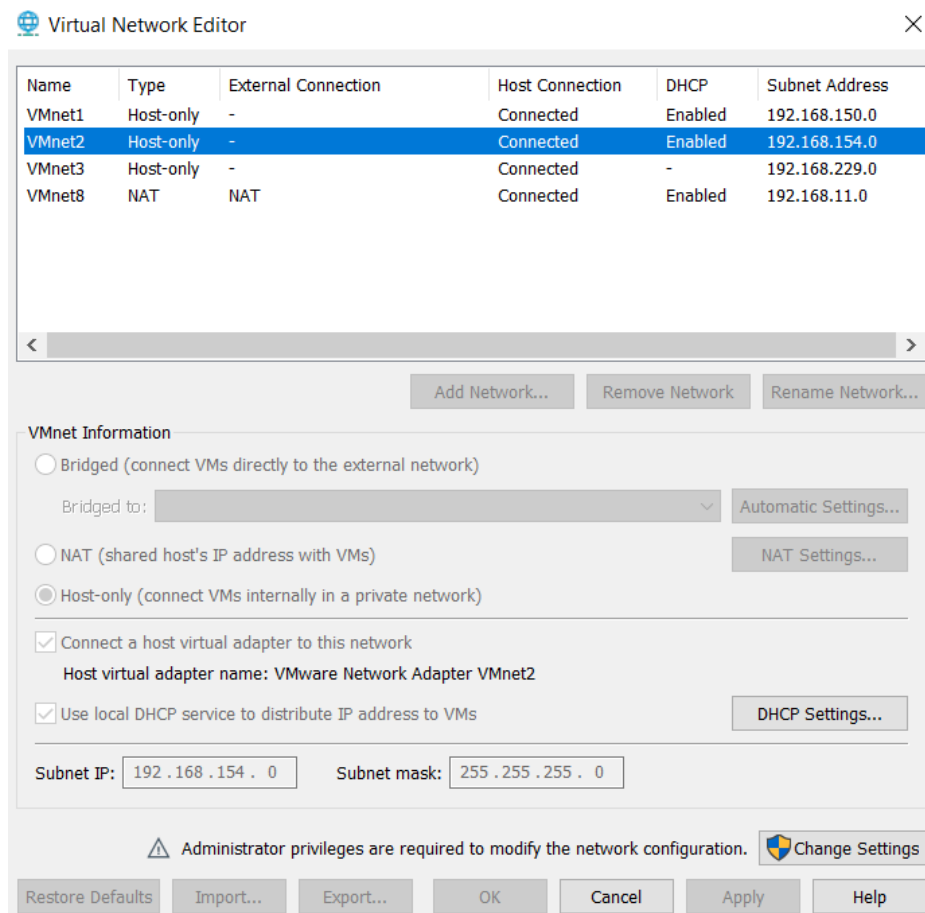


6 Explain what a host-only network is, and how to connect the host to it.

Host-Only network:

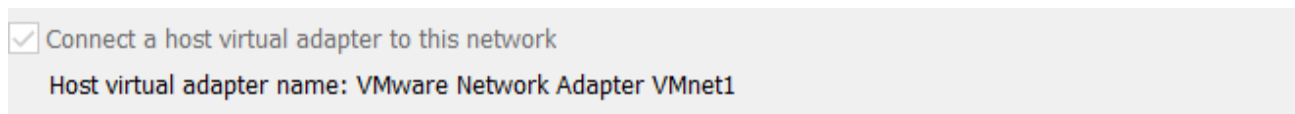
Host-only networks allow you to create your own private network on your host computer. To make a Host-only network, you need to follow these steps:

- 1) Select Edit and choose Virtual Network Editor
- 2) Click Add Network
- 3) Select a Virtual switch
- 4) Select the new virtual network from the list and select Host-Only (Connect VMs internally on a private network)



What it means to connect a Host Virtual Adaptor to this Network:

- By connecting a Host virtual Adaptor to this Network, you are able to connect the host system to the network.



- The host virtual adaptor allows you to communicate between your host computer and the virtual machines on that host computer.
- The host virtual adaptor is used in host-only and NAT configurations.

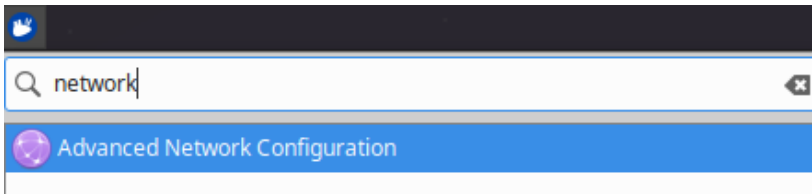
Remember: A host-only network has no access to the outside world and uses no default gateway

7 How to set static IP addresses on Linux hosts

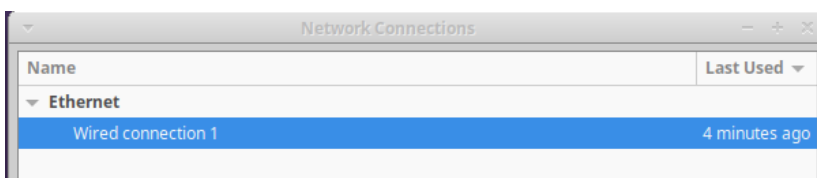
Many situations can call for a static IP address, for example, to establish stable reusable remote access to a certain device.

In this example I am using Linux Xubuntu.

1) Open Network settings as shown in the picture below. In different Ubuntu versions, it might be called Networking instead. In Xubuntu Linux, it is Advanced Network Configuration.



2) Click on your connection type, in this case, Wired connection 1, and navigate to the gear icon located in the left corner of the menu.



3) Navigate to the IPv4 Settings, change the Method from DHCP to Manual. Click the add button. In the address bar type in your desired address, in this case, 192.168.15.10, netmask stays as 24, and leave the gateway blank. Click save, reboot your device and the changes should take place



8 Show the connectivity between virtual and physical hosts via ping

To establish connectivity between virtual network adapter and virtual machine, First we need to see that they are on the same network; one way of doing it is through windows ipconfig command. Thereafter, we can send a Ping request from our host computer to the virtual machine.

The ping program sends ping requests to a device at the specified IP address and awaits ping replies. Ping does this by sending Internet Control Message Protocol (ICMP) echo request packets to the destination host and waits for a reply. Ping measures the time it takes for the packets to return.¹

```
C:\ Command Prompt
Default Gateway . . . . . : 192.168.1.1

Ethernet adapter VMware Network Adapter VMnet3:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::45c5:b8c8:888:a008%49
IPv4 Address. . . . . : 192.168.15.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : domain_not_set.invalid
IPv6 Address. . . . . : fd3f:8e26:93:0:d8b5:5679:43b:8565
Temporary IPv6 Address. . . . . : fd3f:8e26:93:0:7952:983e:9d2f:63ce
Link-local IPv6 Address . . . . . : fe80::d8b5:5679:43b:8565%24
IPv4 Address. . . . . : 192.168.1.149
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.254

C:\Users\olsen>ping 192.168.15.11

Pinging 192.168.15.11 with 32 bytes of data:
Reply from 192.168.15.11: bytes=32 time<1ms TTL=64
Reply from 192.168.15.11: bytes=32 time<1ms TTL=64
Reply from 192.168.15.11: bytes=32 time<1ms TTL=64
Reply from 192.168.15.11: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.15.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\olsen>
```

Here it shows that we have established a connection between the virtual and Physical host via ping.

¹[https://gitlab.com/PerPer/networking/-/blob/master/Troubleshooting/Network Troubleshooting Per Dahlstroem UCL.md](https://gitlab.com/PerPer/networking/-/blob/master/Troubleshooting/Network%20Troubleshooting%20Per%20Dahlstroem%20UCL.md)

9 Show how to use TCP dump/wireshark to monitor traffic

After you have gained access to a virtual machine, you need software which has the possibility to access network traffic, in order to monitor it.
In this case, we will be using the *Wireshark* program from within the virtual machine.

First of all, we need to make sure that the virtual machine has Wireshark installed. To do this, from within your virtual machine open your terminal and type:

```
sudo wireshark
```

If you can not open Wireshark, it is because you do not have it installed. If you however do open it, you have it installed, and can skip this next section regarding installation.

Wireshark installation²

To install Wireshark, you first open your terminal and run the following command:

```
sudo apt install wireshark
```

You should see an installation happening, and you are presented with an option to continue with giving non-superusers privilege to capture packets using Wireshark.

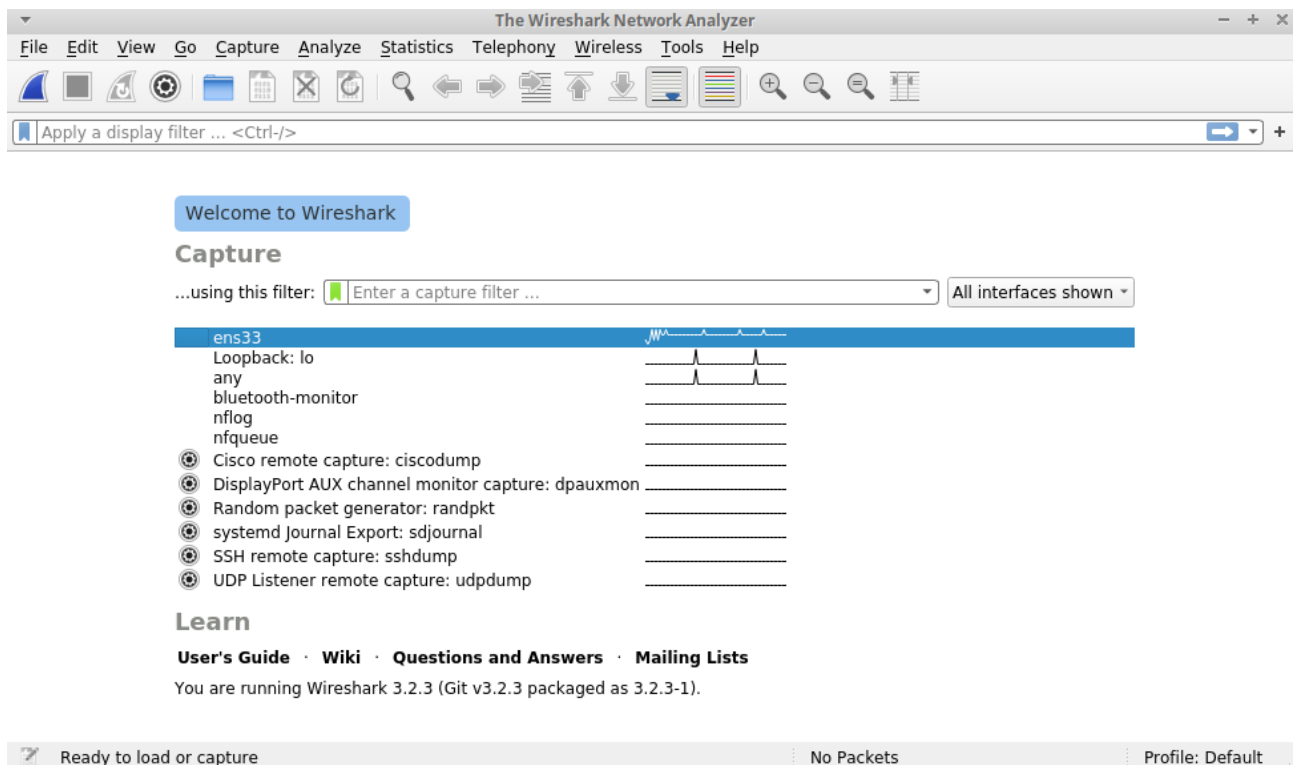
Select **<Yes>** to permit this, and hit **<Enter>**. Wireshark should now be installed.

Monitoring traffic

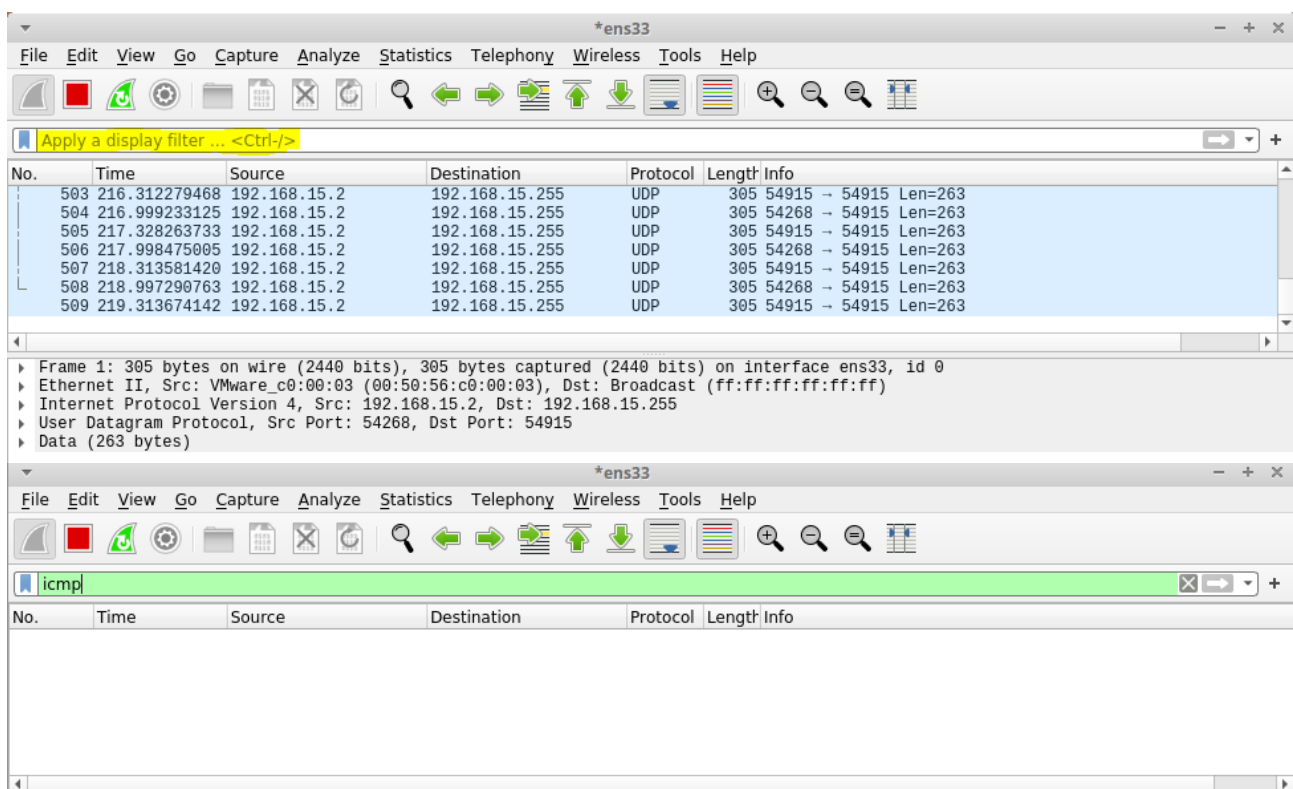
Once you have opened Wireshark, you should see something like this:
The next step is to actually 'sniff for packages' (or simply monitor them). You will want to double click on ens33, and quickly go to the "Apply a display filter ..." bar, type

² (Shovon)

ICMP, and hit **Enter**. That way we will only see relevant traffic, which we are looking



for.



Now that we have our filtered results, we can start sending the packages we are looking for. Open the terminal once again, and ping an address. We will be pinging our host machines. You could also use the address of your another VM, but for now, we will just ping our host machine. Type in the following:

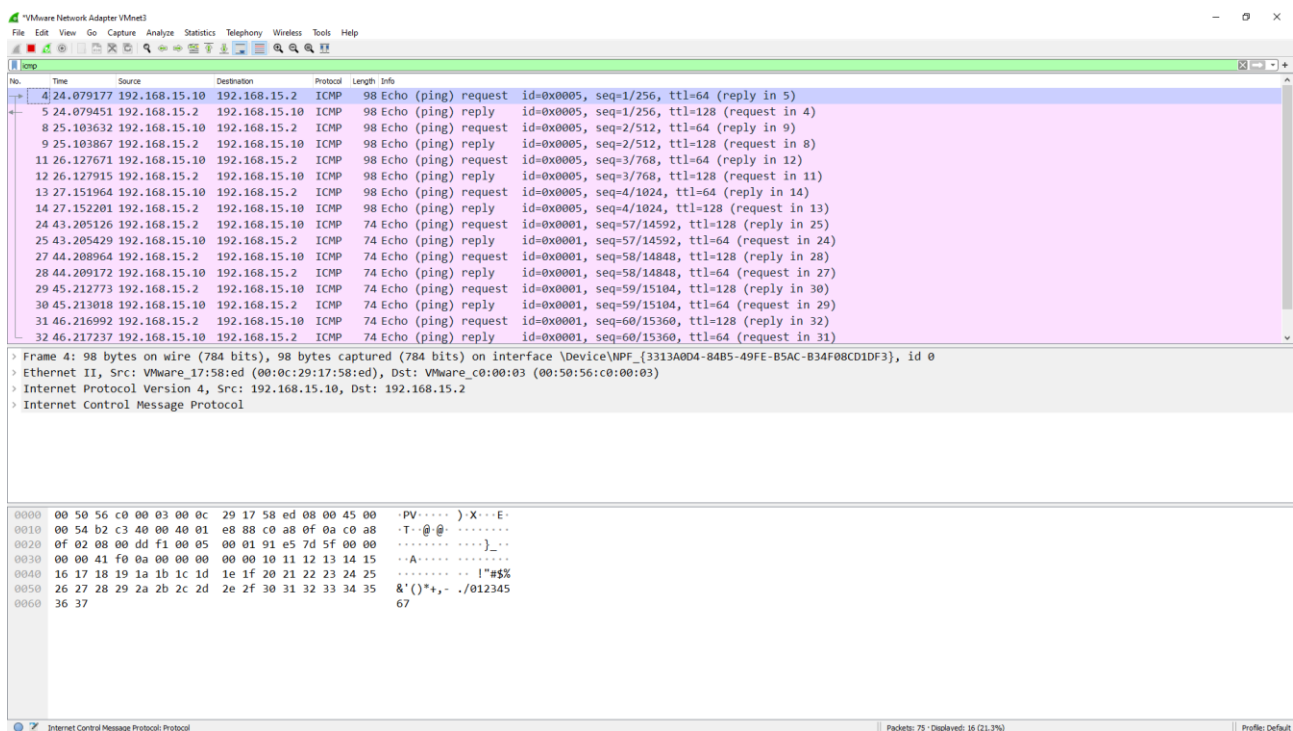
Ping 192.168.15.2

This should provide your terminal with some responses, and look like this:

```
Terminal - strindoi@ubuntu: ~
File Edit View Terminal Tabs Help

strindoi@ubuntu:~$ ping 192.168.15.2
PING 192.168.15.2 (192.168.15.2) 56(84) bytes of data.
64 bytes from 192.168.15.2: icmp_seq=1 ttl=128 time=0.511 ms
64 bytes from 192.168.15.2: icmp_seq=2 ttl=128 time=0.666 ms
64 bytes from 192.168.15.2: icmp_seq=3 ttl=128 time=0.486 ms
64 bytes from 192.168.15.2: icmp_seq=4 ttl=128 time=0.495 ms
^C
--- 192.168.15.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3073ms
rtt min/avg/max/mdev = 0.486/0.539/0.666/0.073 ms
strindoi@ubuntu:~$
```

When you have sent a ping request to 192.168.15.2 go back to Wireshark, and you can see the ingoing and outgoing traffic, which should look like this:



10 Extra: How to set up file sharing between two Linux hosts³

There exists many different softwares which will allow file sharing between two linux hosts. The best client/server for linux only setups will however be through the usage

³ (Boucheron)

of NFS (Network File System). In this setup, one ubuntu machine is called Server, and another is called Client.

10.1 NFS Server

To begin installation and setup, the following commands will have to be executed on the **server**:

```
sudo apt update
```

- update the package list the newest version.

```
sudo apt install nfs-kernel
```

- This is the main NFS package, which will install the server component needed for clients to mount the share we're creating.

```
sudo mkdir /nfs/open-filesharing -p
```

- Create a new directory based in /
The -p option is needed here to create any directories on the path to /nfs/open-filesharing that doesn't already exist.

```
sudo chown nobody:nogroup /nfs/open-filesharing
```

- Whenever NFS saves files originating from a `root` account, the ownership of all of them are changed to `nobody` and permissions in that directory must match that.

```
sudo nano /etc/exports
```

- Edit the exports file to tell NFS which directories it needs to serve to clients.

```
/nfs/open-filesharing    *(rw,sync,no_subtree_check)
```

- Add which directory should be served to clients in the bottom of the file, then specify options needed for working operation. In this case, it is:

`rw` = allows read/write operations by clients

`sync` = Force NFS to write changes to disk before replying back to the client computer. Actual state of the remote directory is much stable and consistent.

`no_subtree_check` = To prevent problems with checking the existence of files for every request. Used to avoid problems where a client has the file opened while trying to rename it.

After finishing writing down the options, save the file and exit back to the terminal.

```
sudo ufw allow nfs
```

- Allow NFS request through the firewall (opens port 2049)

```
sudo ufw enable
```

Enable the firewall on the next startup. Not actually needed in this case, but certainly best practice.

10.2 NFS Client

The next part here concerns the **client**:

```
sudo apt update
```

- As always, update the package list the newest version

```
sudo apt install nfs-common
```

- This will install the NFS components needed for the client to connect to the NFS server

```
sudo mkdir /mnt/nfs/open-filesharing -p
```

- Create the directory where the share should be mounted. Best practice is to put any mounted drives or shares in /mnt
Usage of the -p option is explained in the server section

Optional:

If the goal is to mount the share only once, or just test whether the mount will be successful, the following command can be used:

```
sudo mount 192.168.15.10:/nfs/open-filesharing /mnt/nfs/open-filesharing
```

Otherwise see below:

```
sudo nano /etc/fstab
```

- The fstab config file must be modified to mount the share everytime the machine starts.

```
192.168.15.10:/nfs/open-filesharing    /nfs/open-filesharing    nfs defaults
```

- The lines above must be added to the bottom of the file. The `defaults` option specified at the end might not be optimal, but will be okay in this case. More options can be found using `man nfs`
Save the file and exit back to the terminal. Reboot the machine.

Access to the NFS share on the local machine should now work. The way this is setup will only allow root users to write to the share, which, while certainly not optimal, will work for now.

11 Conclusion

With this paper we, the students, have written guides on how to set up various basic network configurations in VMware, in order to demonstrate a variety of use-cases. These cases range from basic ping commands to capturing ICMP packages in Wireshark. The optional exercise of file sharing was also completed using NFS.

Bibliography

Boucheron, Brian. "How to set up NFS." *How To Set Up an NFS Mount on Ubuntu 20.04*, 2020, <https://www.digitalocean.com/community/tutorials/how-to-set-up-an-nfs-mount-on-ubuntu-20-04>.

Accessed 07 10 2020.

Dahlstrøm, Per. "*Troubleshooting tools and example use on Linux*"

Network_Troubleshooting_Per_Dahlstroem_UCL.md

Accessed 12 10 2020.

Shovon, Shahriar. "How to Install and Use Wireshark on Ubuntu." *Install Wireshark Ubuntu*, Linuxhint, 2018,

https://linuxhint.com/install_wireshark_ubuntu/. Accessed 07 10 2020.