universidade de aveiro
theoria poiesis praxis

DEPARTAMENTO DE ELECTRÓNICA, TELECOMUNICAÇÕES E INFORMÁTICA
LICENCIATURA EM ENG. DE COMPUTADORES E INFORMÁTICA

REDES DE COMUNICAÇÕES I

LAB GUIDE

TRANSPORT PROTOCOLS, SERVICES AND APPLICATIONS

Objectives

- Study of UDP and TCP transport protocols.
- Service deployment and study of DNS, HTTP, TFTP and FTP

Duration

- 2 weeks

1. VirtualBox Virtual Machines

If you do not have yet VirtulBox installed:

- Download and install VirtulBox
- Import the Appliance (*.OVA) provided on the e-learning.

If you already have the "Labcom" virtual machine installed and you are already using it inside GNS3, in order to proceed with this guide, please configure the networking as explained on the following section.

If you prefer to use multiple VM instances, one for GNS3 and one for this Guide, clone the original machine in VirtualBox interface.

2. Virtual Machine Network preparation

Go to Oracle VM VirtualBox Manager

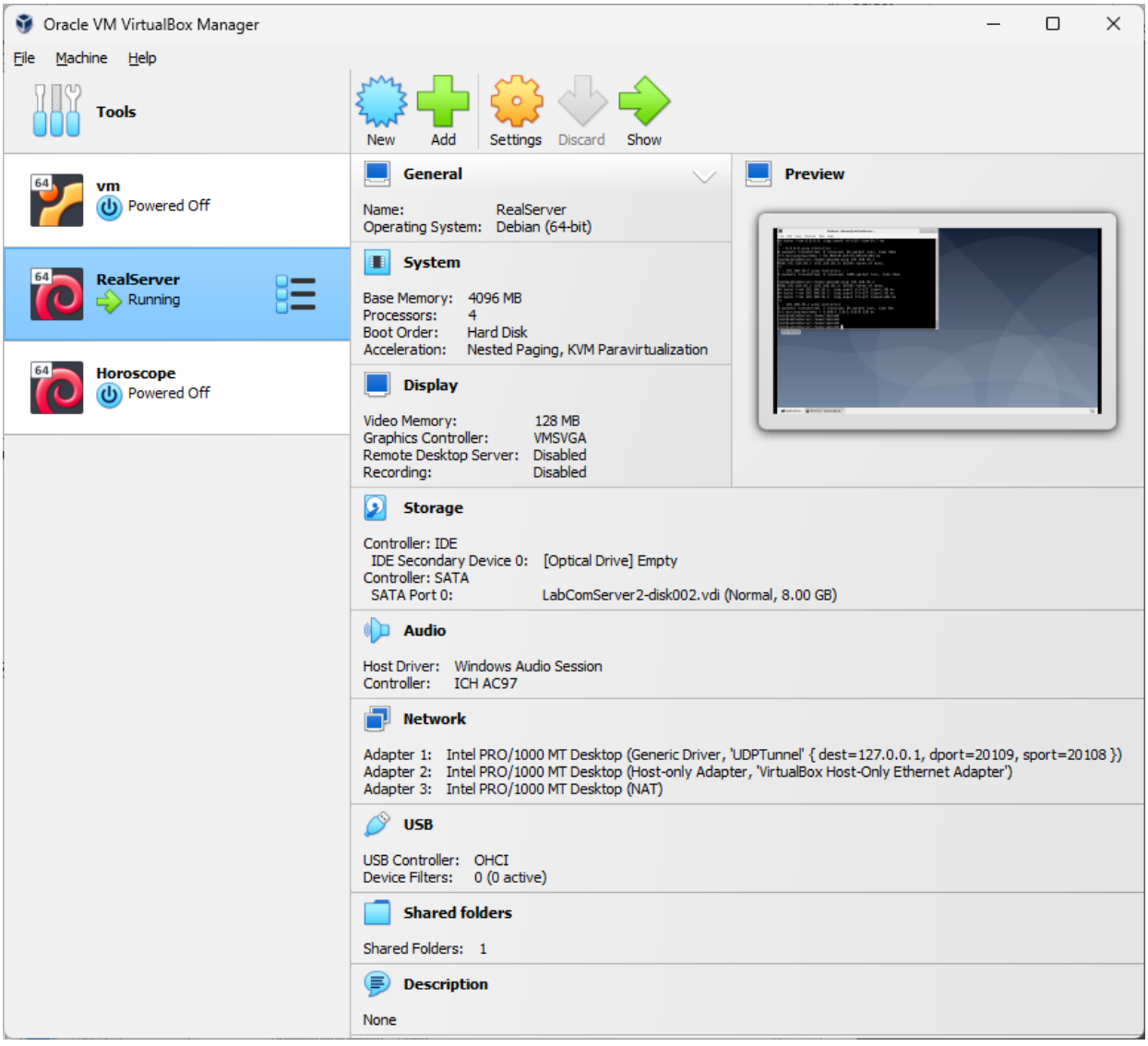


Figure 1: Oracle VirtualBox Manager

Select the correct VM and go to settings.

Edit the network settings to have 3 network adapters, configured as presented on the following pictures.

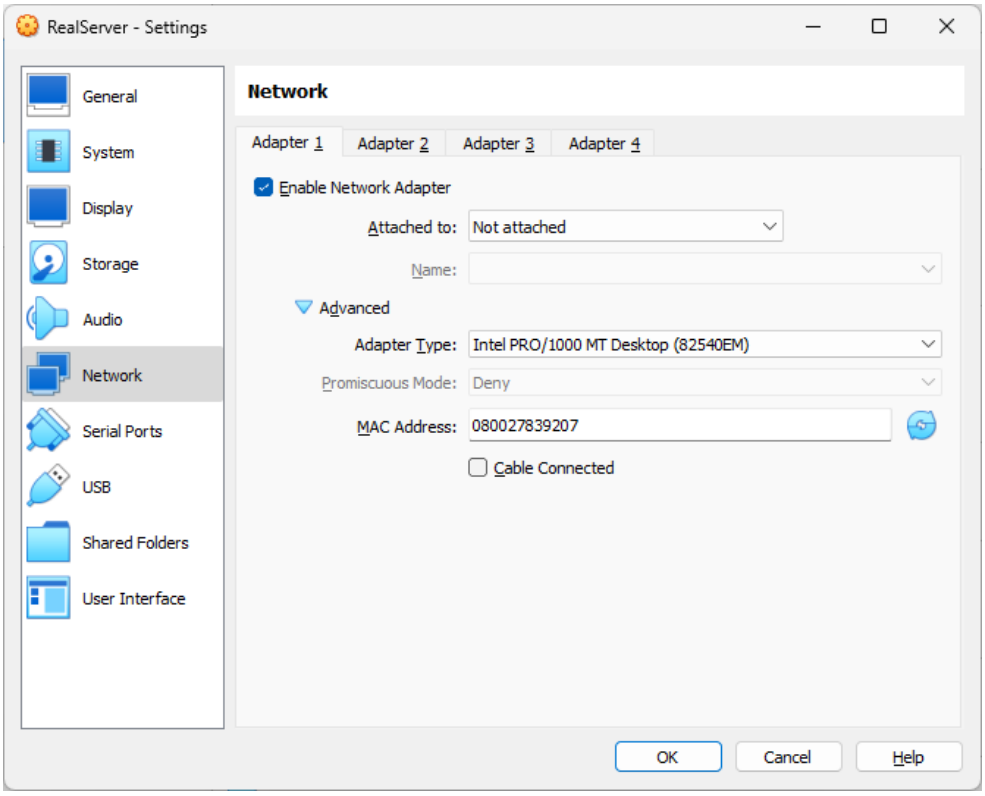


Figure 2: VM Network Adapter 1

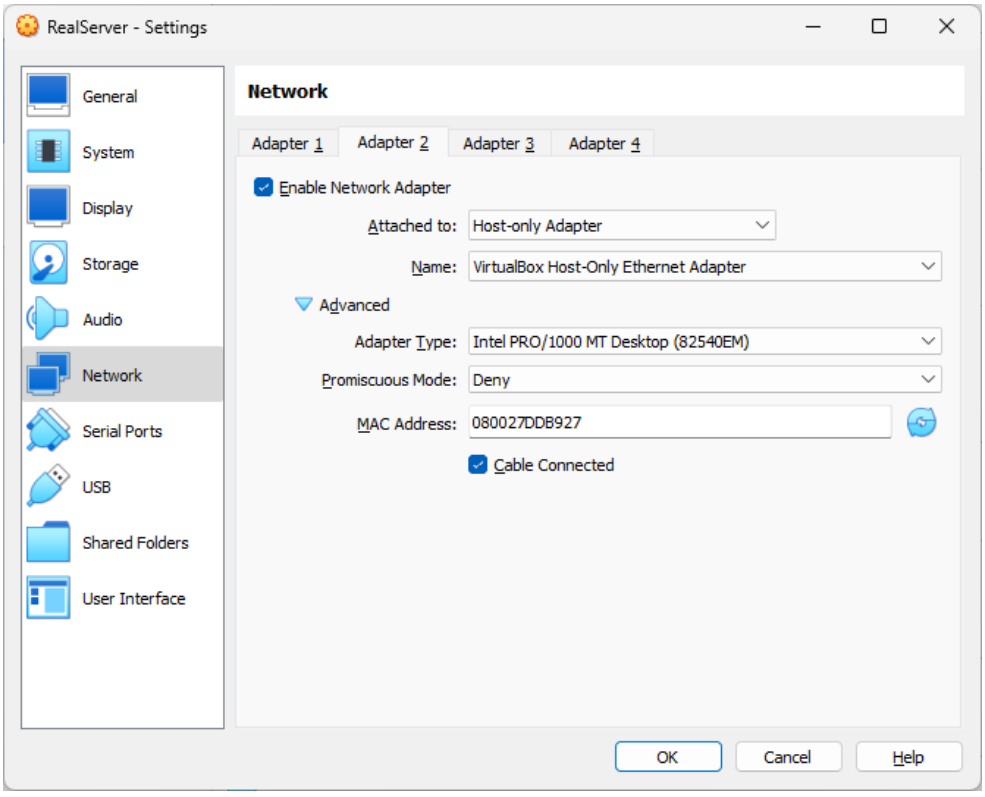


Figure 3: VM Network Adapter 2

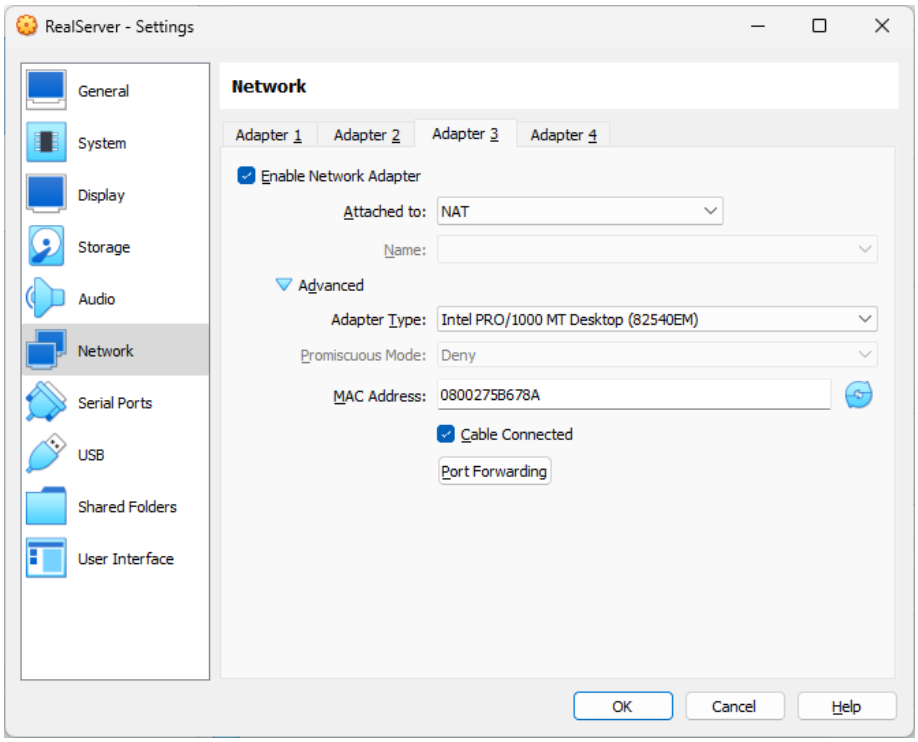


Figure 4: VM Network Adapter 3

At this stage, you may also go to GNS3, without opening any project, and select Edit->Preferences->VirtualBox VMs and edit the configuration of the VM to guarantee that you choose 3 Adapters.

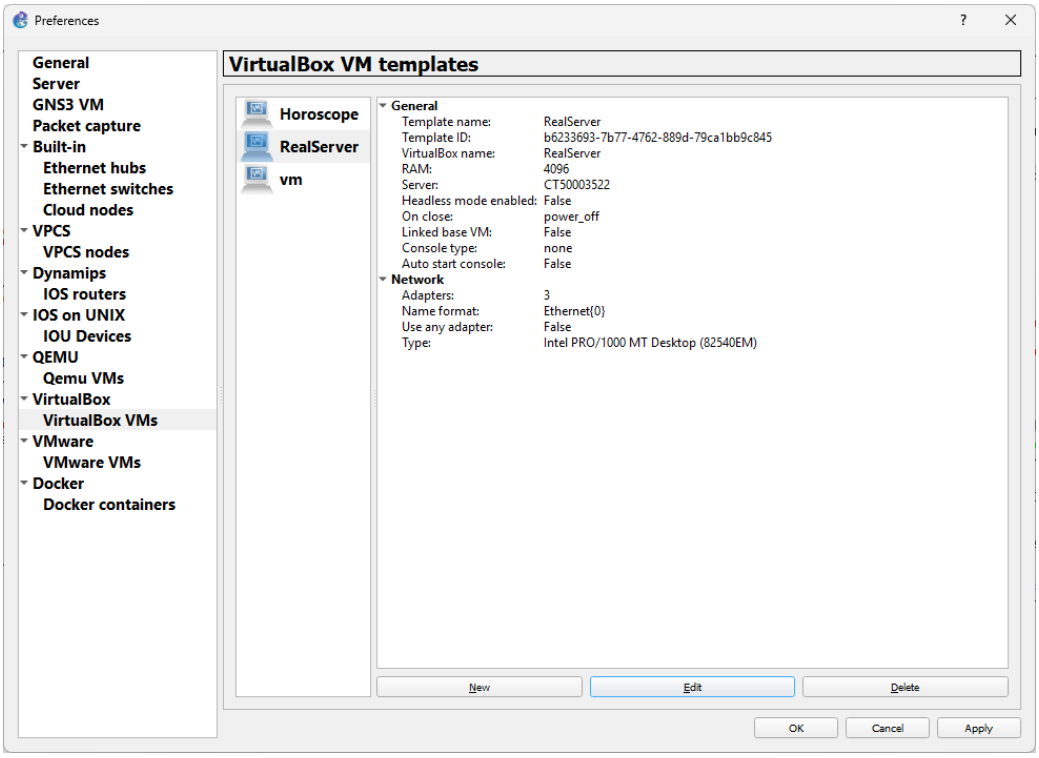


Figure 5: VirtualBox VM templates

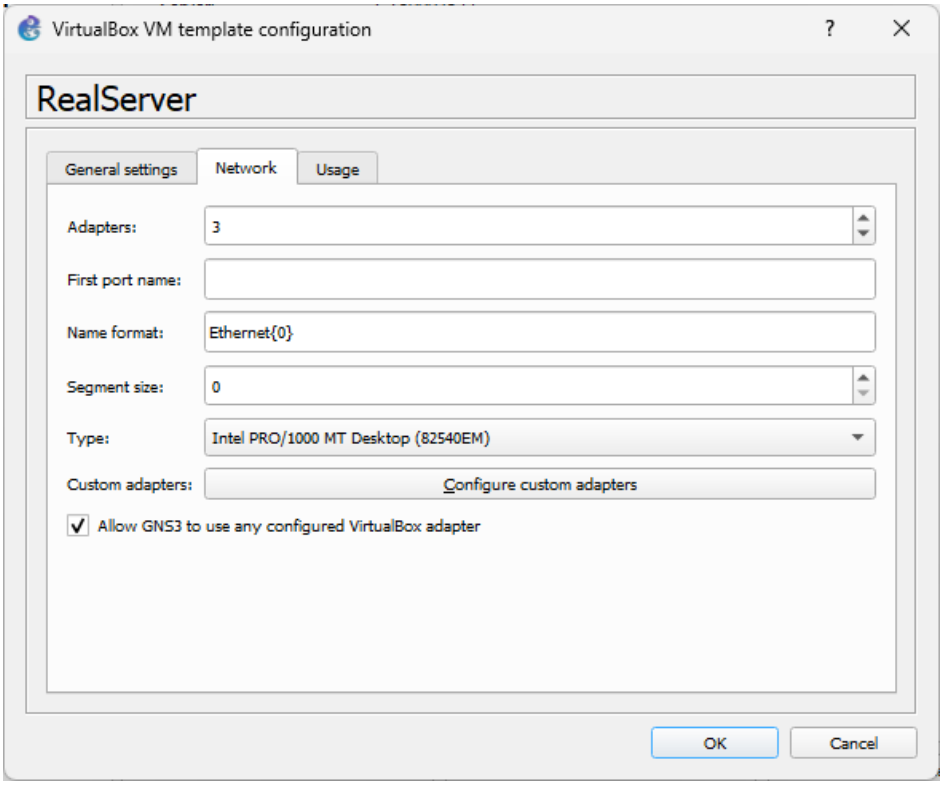


Figure 6: VirtualBox VM Network

This guide may be done with the VM running in stand-alone mode, started from Oracle VirtualBox. In order to do that, you should not open any project that uses the VM.

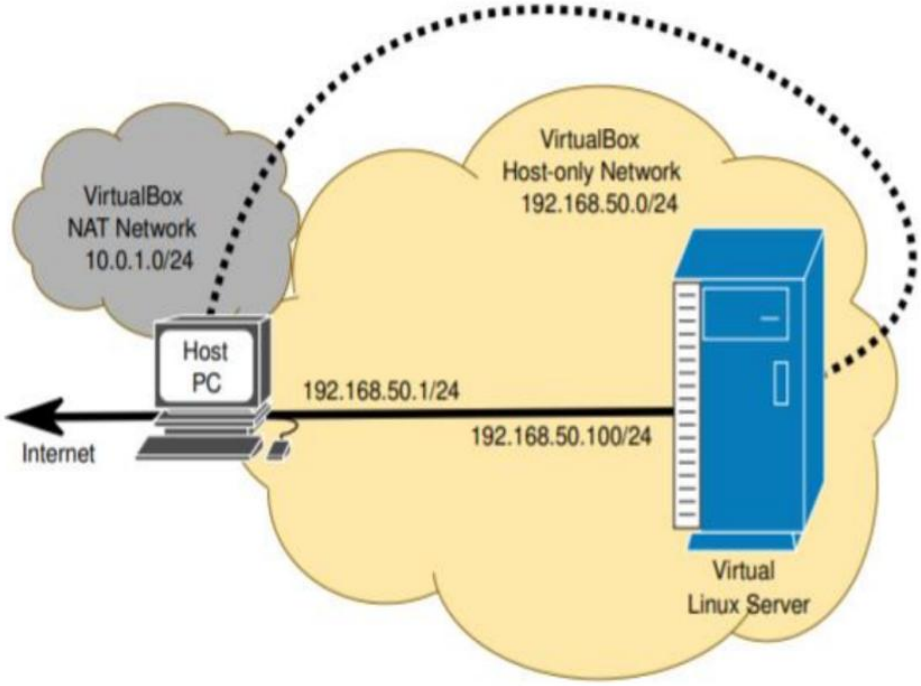
The network adapters that are going to be used are the second and third on your network list, when you do a "sudo ifconfig". If you cannot see 3 network adapters, please ask for assistance.

3. IPv4 Network Services

NOTE:

The IP networks presented on this guide may differ from the ones you may find on your VM:

- **Instead of 192.168.50.0/24, you may have 192.168.56.0/24**
- **Instead of 10.0.1.0/24, you may find 10.0.4.0/24 (or even a different "10.0.x.0/24)**
- **The Host PC IP address may not be 192.168.50.1. It may, for instance, be 192.168.56.2 (please check the correct IP on the host machine VirtualBox Host-Only Ethernet Adapter properties).**



Start the Virtual Linux Server, start a terminal, and verify the network connections:

```
sudo ifconfig                          #shows active interfaces
sudo ifconfig -a                       #shows all interfaces
```

Note: interface eth0 should be the NAT network connection, and eth1 the Host-only connection.

Two Ethernet (eth) interfaces must be active. One for the NAT network, and another for the Host-only network. The NAT network should acquire the IPv4 address (and gateway) automatically. However, the IPv4 address (gateway is not required) for the Host-only network must be configured:

```
sudo ifconfig eth1 up                  #activates eth1 interface
sudo ifconfig eth1 192.168.50.100/24       #configures eth1 IPv4 address
```

Test the server connectivity with the Internet and Host PC (192.168.50.1).

Note: Windows Host PCs' Firewall may be blocking ICMP Echo (ping) request packets.

3.1. DNS

7. At the server, verify if the DNS (bind9) service is installed and active with the command:

```
service bind9 status
```

To install, run the following commands (with sudo):

```
apt-get update
apt-get install bind9
```

To start the FTP service and recheck the status of the service:

```
service bind9 start
service bind9 status
```

8. Assuming that you have the domain ArqRedes.pt, configure your DNS server as master with authority over this domain. Start by creating the zone for the domain by adding to the configuration file /etc/bind/named.conf.local the following defintitions:

```
zone "arqredes.pt" in{
   type master;                    //define the zone as master
   file "/etc/bind/db.arqredes.pt";           //file with the domain records
};
```

Create the file /etc/bind/db.arqredes.pt and add to it the following definitions and DNS records:

```
$TTL  604800
$ORIGIN arqredes.pt.
@     IN    SOA   ns1.arqredes.pt. adm.arqredes.pt. (
                  2           ; Serial
                  604800      ; Refresh
                  86400       ; Retry
                  2419200     ; Expire
                  604800)     ; Negative Cache TTL
      IN    NS    ns1.arqredes.pt.
ns1   IN    A     192.168.50.100
@     IN    A     192.168.50.100
www   IN    A     192.168.50.100
siteA IN    A     192.168.50.100
hostPC      IN    A     192.168.50.1
```

Verify if the file with the zone definitions is correctly constructed:

```
named-checkzone arqredes.pt db.arqredes.pt
```

Restart the DNS server:

```
service bind9 restart
```

At the Host PC, define your Virtual Server as main DNS server, start a Wireshark capture in the interface that connects to the server (Host-only adapter), perform the following DNS queries:

```
nslookup arqredes.pt
nslookup www.arqredes.pt
nslookup siteA.arqredes.pt
nslookup hostPC.arqredes.pt
```

Note: To configure the DNS server in Linux edit the file /etc/resolv.conf with the Virtual Server address.
>> Analyze the captured DNS packets.

3.2. HTTP

9. At the server, verify if the DNS (apache2) service is installed and active with the command:

```
service apache2 status
```

To install, run the following commands (with sudo):

```
apt-get update
apt-get install  apache2
```

To start the FTP service and recheck the status of the service:

```
service apache2 start
service apache2 status
```

Analyze the content of the apache2 main configtration file (/etc/apache2/apache2.conf). At the Host PC, start a Wireshark capture in the interface that connects to the server (Host-only adapter), and test the HTTP server accessing the following URL (with a browser):

```
http://192.168.50.100
http://arqredes.pt
http://www.arqredes.pt
http://siteA.arqredes.pt
```

>> Based on the captured packets, identify and analyze the TCP sessions (including sequence and acknowledge numbers and flags), and the content of the HTTP packets. Explain how the HTTP server identifies the webpage/data to sent to the client.

10. In the apache2 default content folder /var/www/html/, create a new folder named “arqredes.pt-80” (name format is not mandatory, but it is import to maintain consistence, e.g., *domain-port*) to store the webpage associated with the domain arqredes.pt. Inside the new folder create a new HTML file named index.html (default webpage name) with the following content (you may change it):

```
<html>
<body>
<h1>arqredes.pt</h1>
<h2>Porto 80</h2>
</body>
</html>
```

In order to create a new website at the server it is requeired to define a new apache2 Virtual Host. in the folder /etc/apache2/sites-available/ create a new file (named arqredes.pt-80.conf) with the following content:

```
<VirtualHost *:80>
      DocumentRoot /var/www/html/arqredes.pt-80
      ServerName arqredes.pt
</VirtualHost>
```

Enable the new domain/site and restart the HTTP server:

```
a2ensite arqredes.pt-80
service apache2 restart
```

Test the HTTP server accessing the following URL (with a browser):

```
http://192.168.50.100
http://arqredes.pt
http://www.arqredes.pt
http://siteA.arqredes.pt
```

>> What do you conclude?

11. At the Virtual Host definition (arqredes.pt-80) add the following directive (below *ServerName*):

```
ServerAlias www.arqredes.pt
```

Restart the HTTP server:

```
service apache2 restart
```

Test the HTTP server accessing the following URL:

```
http://192.168.50.100
http://arqredes.pt
http://www.arqredes.pt
http://siteA.arqredes.pt
```

>> What do you conclude?

12. Create a different site/webpage for the subdomain siteA.arqredes.pt.

3.3. TFTP

1. At the server, verify if the TFTP service is installed and active with the command:

```
service atftpd status
```

To install, run the following commands (with sudo):

```
apt-get update
apt-get install atftpd
```

To start service, first, edit the file /etc/default/atftpd by adding the following line (at top):

```
USE_INETD=false
```

After, start the TFTP service and recheck the status of the service:

```
service atftpd start
service atftpd status
```

Note: The TFTP service root folder is /srv/tftp.

2. Verify which IPv4 services are active at the server listing all the UDP open ports and TCP ports in LISTEN state, with the command:

```
netstat -lnutp4
```

Note: UDP port 69 is (by default) the TFTP service assign UDP port

3. At the server, in the folder (/srv/tftp/), create two files with random content, one with 1500 bytes and another with 1024 bytes,

```
sudo su
cd /srv/tftp/
dd if=/dev/urandom of=file1500 bs=1 count=1500
dd if=/dev/urandom of=file1024 bs=1 count=1024
chown nobody:nogroup *
```

At the Host PC, start a Wireshark capture in the interface that connects to the server (Host-only adapter).

At the Host PC install and run a TFTP client:

(Linux)

Install: `apt install tftp`

Connect the TFTP client to the service and activate binary transference:

```
tftp 192.168.50.100
bin
```

Download the two files form the server:

```
get file1500
get file1024
```

Upload both files to the server:

```
put file1500
put file1024
```

(Windows)

Install: Control Panel→ Programs→ Turn Windows features on and off→ Activate TFTP client.

Download the two files form the server:

```
tftp -i 192.168.50.100 GET file1500
tftp -i 192.168.50.100 GET file1024
```

Upload both files to the server:

```
tftp -i 192.168.50.100 PUT file1500
tftp -i 192.168.50.100 PUT file1024
```

Note: you may need to disable the Windows Firewall.

>>Analyze the sequence of exchanged TFTP packets. Explain the UDP ports chosen to transfer files. Explain why a packet with zero data bytes is transmitted at the end of the 1024 bytes file transference. Explain why some TFTP packets are padded with zeros.

3.4. FTP

4. At the server, verify if the FTP service is installed and active with the command:

```
service vsftpd status
```

To install, run the following commands (with sudo):

```
apt-get update
apt-get install vsftpd
```

To start the FTP service and recheck the status of the service:

```
service vsftpd start
service vsftpd status
```

Edit the file */etc/vsftpd.conf and uncomment the line "write_enable=YES" to enable write commands.*
Restart the service:

```
service vsftpd restart
```

Note: The FTP service maps each user folder as respective root (i.e., for labcom user is /home/labcom/).

5. At the server, in the home folder (/home/labcom/), create one file with 15K bytes:

```
dd if=/dev/urandom of=file15K bs=1k count=15
```

At the Host PC, start a Wireshark capture in the interface that connects to the server (Host-only adapter), start the FTP client and activate the binary mode of transference:

```
ftp 192.168.50.100
bin
```

Dowload file file15 from the server:

```
get file15k
```

Upload the same file to the server:

```
put file15K
```

>> Based on the captured packets, identify and analyze the TCP sessions (including sequence and acknowledge numbers and flags).
>> Analyze the exchanged FTP commands.
Note: Wireshark packet decoding (by default) uses relative TCP sequence numbers, i.e., the first packet TCP sequence number is always shown as zero and all following sequence numbers are adjusted accordingly. In reality, the first sequence number is not zero.

6. Activate the passive FTP transference mode (PASV), and upload the file file15K to the server:
(Linux – at the FTP client prompt)

```
passive
put file15k
```

(Windows)
The FTP command line in Windows does not support the passive mode. Download and install another FTP client. For example: FileZilla: https://filezilla-project.org/ , File→ Network Configuration Wizard….
Note: FTP passive mode is FileZilla's default.
>> Analyze the differences between passive and non-passive TFP transfer modes. In which scenarios is the passive mode essential?