

# Práctica 1//Redes de computadoras

Emmanuel Peto Gutiérrez

10 de octubre de 2020

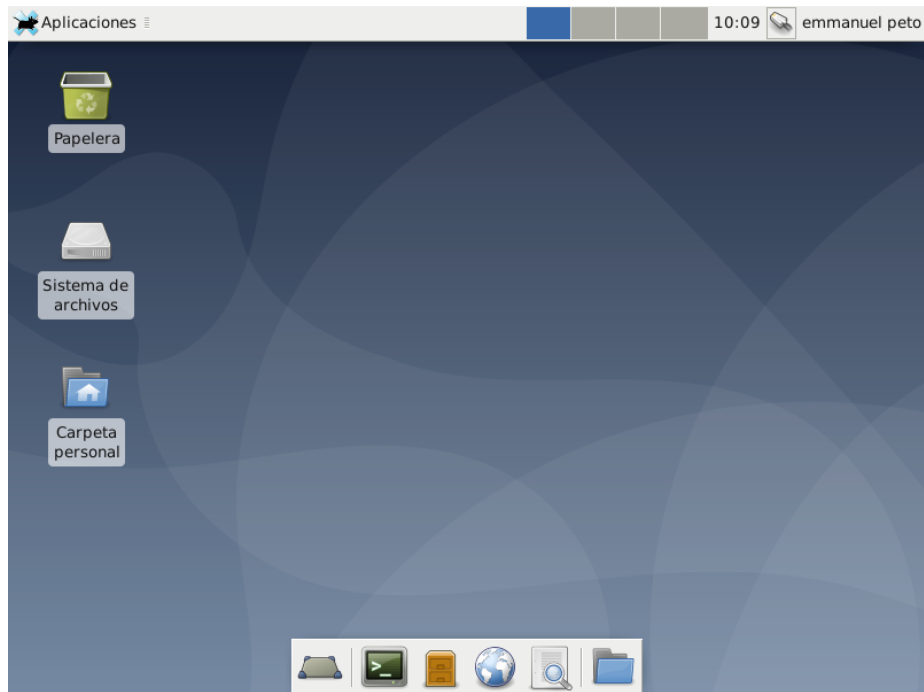
## 1. Pasos para realizar la práctica

Se instalaron los software: Virtual Box, Vagrant y Wireshark.

Se clonó el repositorio <https://gitlab.com/ismael.andrade/redes-2021-1.git> y en la sección lab1, en mi computadora, se ejecutó el comando `vagrant up`; sin embargo, se obtuvo el siguiente error que no se supo corregir: *A host only network interface you're attempting to configure via DHCP already has a conflicting host only adapter with DHCP enabled. The DHCP on this adapter is incompatible with the DHCP settings. Two host only network interfaces are not allowed to overlap, and each host only network interface can have only one DHCP server. Please reconfigure your host only network or remove the virtual machine using the other host only network.*

```
emmanuel@emmanuel-VPC5B45FL:~/Documentos/Redes/redes-2021-1/lab1$ sudo vagrant up
[sudo] contraseña para emmanuel:
Bringing machine 'default' up with 'virtualbox' provider...
==> default: Checking if box 'generic/debian10' version '3.0.34' is up to date..
.
==> default: Clearing any previously set network interfaces...
A host only network interface you're attempting to configure via DHCP
already has a conflicting host only adapter with DHCP enabled. The
DHCP on this adapter is incompatible with the DHCP settings. Two
host only network interfaces are not allowed to overlap, and each
host only network interface can have only one DHCP server. Please
reconfigure your host only network or remove the virtual machine
using the other host only network.
```

Dado el error, se procedió a instalar manualmente la máquina virtual de Debian 10 en Virtual Box, descargando el ISO de la página de Debian.



Para conocer las direcciones, MAC e IP, se ejecutó el comando `ip addr`.  
En la computadora:

```
emmanuel@emmanuel-VPCS845FL:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp5s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether f0:bf:97:e8:f9:a9 brd ff:ff:ff:ff:ff:ff
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 64:27:37:aa:35:ad brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.42/24 brd 192.168.1.255 scope global dynamic noprefixroute wlp2s0
        valid_lft 85613sec preferred_lft 85613sec
    inet6 fe80::7edb:3464:4a4b:98c1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

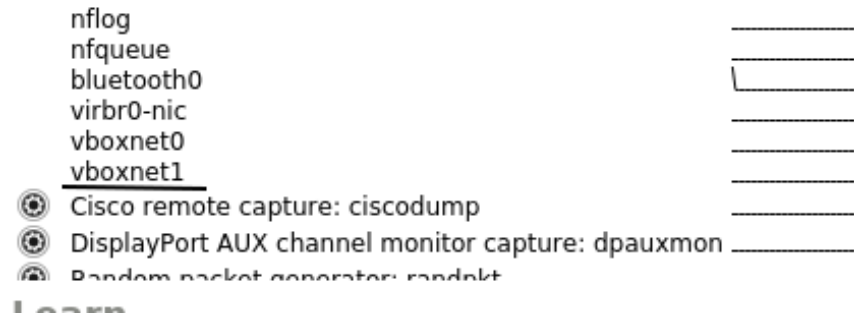
En la máquina virtual:

```
emmanuel@emmanuel:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:5b:ab:14 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.41/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
```

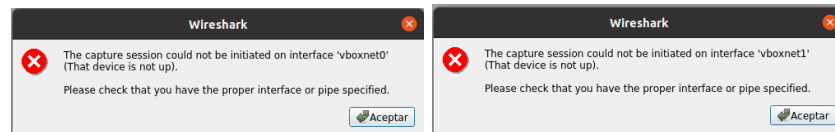
Se abrió Wireshark para capturar el tráfico. Se intentó entrar a vboxnet0 y vboxnet1.

## Capture

...using this filter:



Sin embargo, se obtuvieron los siguientes errores:



Así que se optó por wlp2s0. En esta opción, se aplicó el filtro ARP.

## Capture

...using this filter:



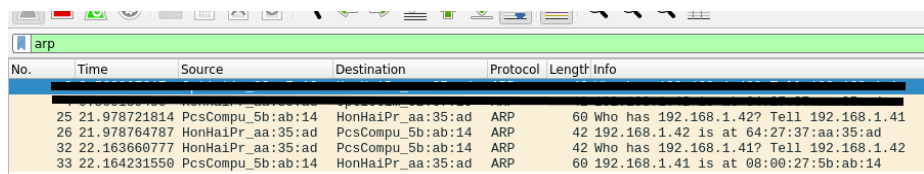
Posteriormente se procedió a hacer ping desde mi máquina (192.168.1.42) hacia la máquina virtual (192.168.1.41).

```

emmanuel@emmanuel-VPCSB45FL:~$ ping 192.168.1.41
PING 192.168.1.41 (192.168.1.41) 56(84) bytes of data.
64 bytes from 192.168.1.41: icmp_seq=1 ttl=64 time=0.604 ms
64 bytes from 192.168.1.41: icmp_seq=2 ttl=64 time=0.663 ms
64 bytes from 192.168.1.41: icmp_seq=3 ttl=64 time=0.699 ms
64 bytes from 192.168.1.41: icmp_seq=4 ttl=64 time=0.710 ms
^C
--- 192.168.1.41 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3069ms
rtt min/avg/max/mdev = 0.604/0.669/0.710/0.041 ms

```

Se puede observar el tráfico generado por el ping, en Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
25	21.978721814	PcsCompu_5b:ab:14	HonHaiPr_aa:35:ad	ARP	60	Who has 192.168.1.42? Tell 192.168.1.41
26	21.978764787	HonHaiPr_aa:35:ad	PcsCompu_5b:ab:14	ARP	42	192.168.1.42 is at 64:27:37:aa:35:ad
32	22.163666777	HonHaiPr_aa:35:ad	PcsCompu_5b:ab:14	ARP	42	Who has 192.168.1.41? Tell 192.168.1.42
33	22.164231550	PcsCompu_5b:ab:14	HonHaiPr_aa:35:ad	ARP	60	192.168.1.41 is at 08:00:27:5b:ab:14

## 2. Cuestionario

1. ¿Cuáles son las direcciones físicas de tu equipo y de la máquina virtual?

- La de mi equipo es 64:27:37:aa:35:ad.
- La de la máquina virtual es 08:00:27:5b:ab:14.

2. ¿Cuáles son las direcciones lógicas de tu equipo y la máquina virtual?

- La de mi equipo es 192.168.1.42.
- La de la máquina virtual es 192.168.1.41.

3. ¿Cuál es la diferencia a nivel de bits entre una dirección física y una lógica?

A nivel de bits se diferencian por la cantidad que una usa respecto a la otra. En la dirección MAC se usan 6 bloques de 8 bits, o sea 48 bits. La dirección IPv4 usa 4 bloques de 8 bits, o sea 32 bits.

4. ¿Por qué existen dos consultas ARP?

Porque primero, el dispositivo que realizó el ping (192.168.1.42) pregunta cuál es la dirección MAC del dispositivo al que envió el ping (192.168.1.41). Después, el dispositivo que recibe el ping envía un mensaje de regreso y debe preguntar por la dirección MAC de 192.168.1.42. Así, en este caso, se deben traducir las direcciones de la computadora y de la máquina virtual.

**5. Investigar y describir de manera breve en que consiste un ataque de ARP spoofing.**

Un atacante en una red se coloca como intermediario entre las comunicaciones de un dispositivo y un router.

**6. Investigar el fabricante del adaptador de red físico del equipo personal.**

El del wireless: Qualcomm Atheros.

El del Ethernet: Realtek Semiconductor Co., Ltd.