

---

*Informe Entrega 1*

---

Informe sobre la primera practica de la asignatura Garantía y Seguridad de la Información. En esta práctica hemos creado una red NAT (red formada por máquinas en el mismo segmento de red que se pueden relacionar con máquinas de otros segmentos a través de una máquina anfitriona/router) entre tres sistemas con distintas características. La práctica ha estado centrada en saber de que manera controlar las identidades de cada equipo, configurar esta red y comprobar que entidades forman la red a parte de los tres sistemas que estamos manejando.

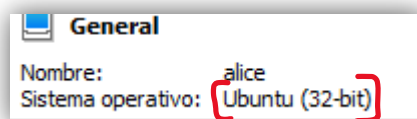
**Pregunta 1:**

**Indica las características de cada una de las máquinas virtuales utilizadas para montar el entorno de trabajo virtual: sistema operativo y arquitectura, número de procesadores, cantidad de memoria RAM asignada, velocidad de transmisión del adaptador de red:**

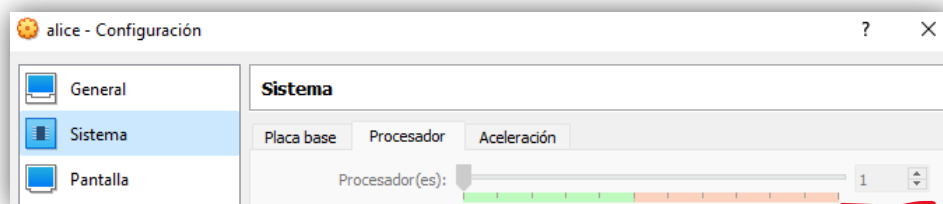
Tenemos tres máquinas virtuales:

- **Alice:** Sistema operativo Ubuntu con arquitectura de 32 bits, 1 procesador, 512 MB de memoria RAM y una velocidad de 1000 Megabits por segundo

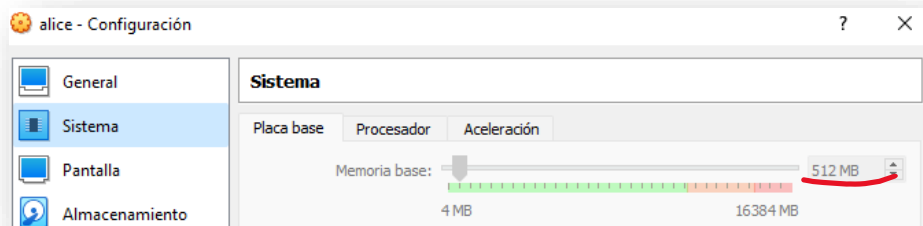
**SISTEMA Y ARQUITECTURA:**



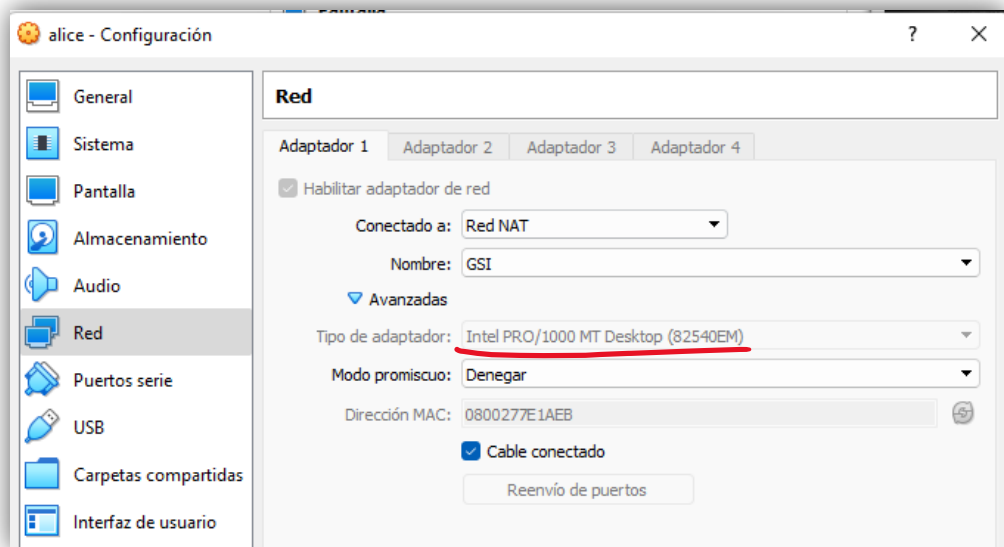
**PROCESADORES:**



RAM:



VELOCIDAD DE ADAPTADOR:



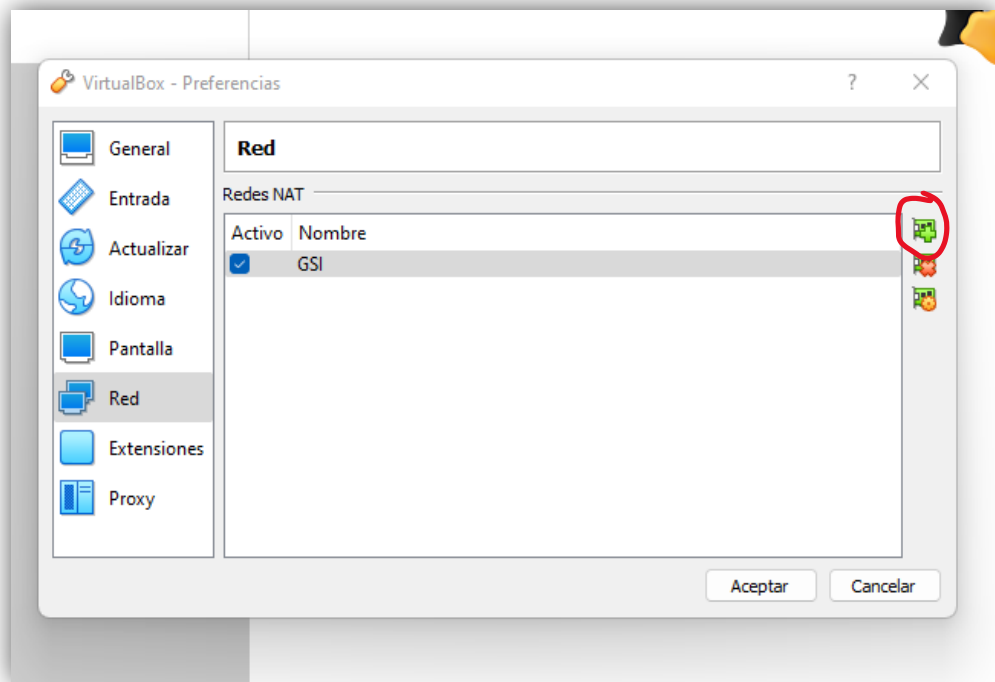
Intel PRO/1000 GT Desktop Adapter Interno  
Ethernet 1000Mbit/s Adaptador y Tarjeta de  
Red - Accesorio de Red (Alámbrico, PCI,  
Ethernet, RJ-45, 1000 Mbit/s, Full-Height

- **Bob:** Sistema operativo Debian (sistema en el que se basa Ubuntu) con arquitectura 32 bits, 1 procesador, 384 MB de memoria RAM y 1000 Megabits de velocidad de adaptador red. Los lugares en los que se encuentran estas configuraciones en virtual box son los mismos que en las capturas de Alice.
- **Mallet:** El mismo sistema y las mismas características que Alice.

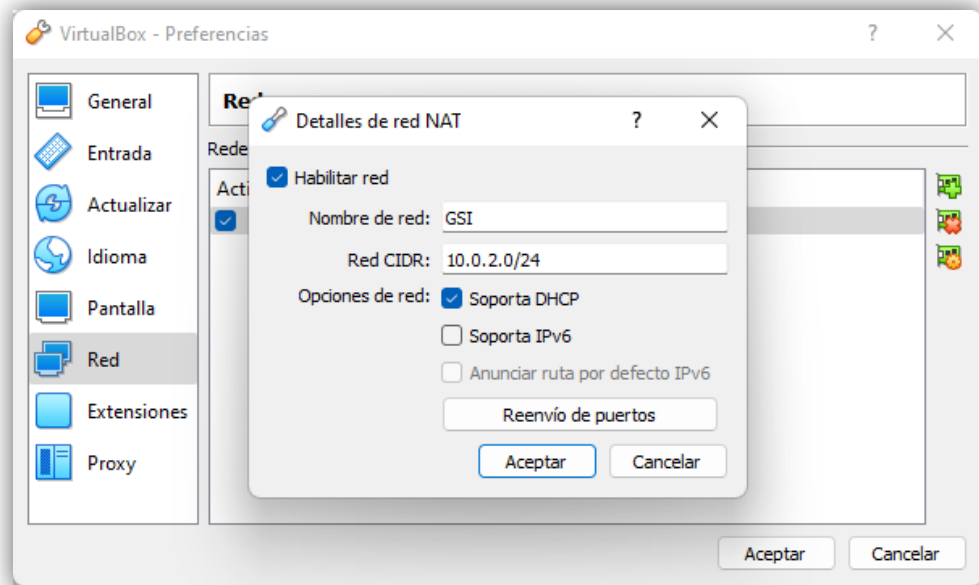
**Pregunta 2:**

**Configura el entorno de virtualización y las máquinas virtuales para que las tres máquinas se encuentren dentro de la Red NAT10.0.2.0/24 de nombre "GSI". Documenta todos los pasos realizados.**

Para realizar esta operación lo primero que tenemos que hacer es crear la red NAT a la que vamos a conectar los tres sistemas. Esto se hace en Archivo -> Preferencias -> Red:

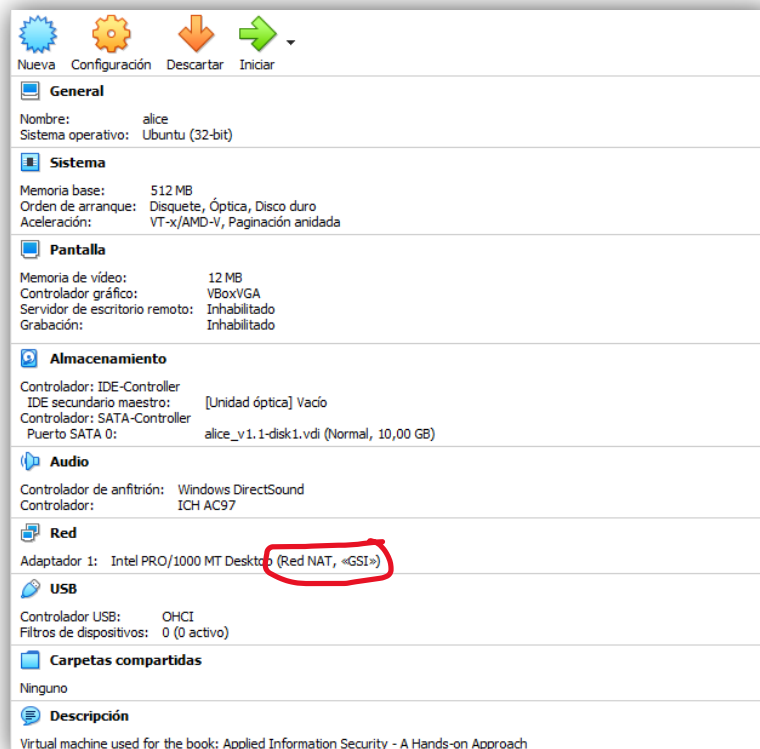


Tras entrar en Red y al pulsar el botón rodeado podemos añadir una nueva red NAT, introducimos los datos del enunciado y dejamos la casilla de DHCP (protocolo que proporciona una configuración de red dinámica a una máquina con su respectiva IP, mascara, puertas de enlace, etc.)



Ya tenemos la red NAT creada, solo queda asociarla a las máquinas.

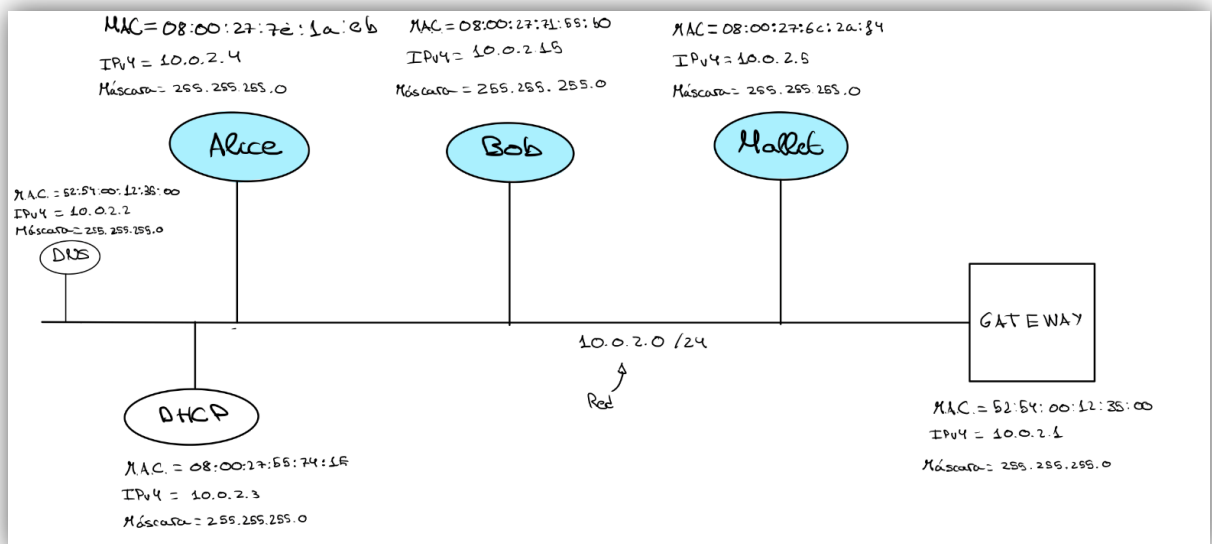
Para asociarla a las máquinas se puede hacer de dos maneras. Una es metiéndose en configuración de cada máquina en el apartado de Red. La otra manera es la más sencilla y es desde el propio menú principal de VB, en el resumen de configuraciones de la derecha se puede hacer clic en el paréntesis que hay en el apartado de Red y ahí lo cambiamos directamente.



Realizamos este proceso con las tres máquinas y las tenemos listas para arrancarlas.

### Pregunta 3:

Dibuja un diagrama de red lo más detallado posible de la red que forman las tres máquinas virtuales; alicé, bob, mallet. Para cada máquina proporciona su dirección MAC, dirección IPv4 y máscara de red. Indica la dirección de red en formato IPv4 de la red en la que se encuentran las máquinas y la puerta de enlace (gateway) de cada una de ellas. ¿Es la misma? Justifica tu respuesta.



En cuanto a las puertas de enlace es la misma en los tres sistemas ya que están conectados a la misma red NAT. Esto se puede observar con el comando "route -n" el cual nos muestra la tabla de enrutamiento en formato numérico. Las puertas de enlace son las que tienen el flag UG (Up Gateway). Ejecutando este comando en las tres

máquinas sale la misma puerta de enlace.

```
mallet@mallet: ~
File Edit View Terminal Help
mallet@mallet:~$ route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
0.0.0.0          0.0.0.0         255.255.255.0    U        1      0        0 eth4
169.254.0.0      0.0.0.0         255.255.0.0      U       1000    0        0 eth4
0.0.0.0          10.0.2.1        0.0.0.0          UG        0      0        0 eth4
0.0.0.0          10.0.2.1        0.0.0.0          UG       100     0        0 eth4
mallet@mallet:~$
```

La IPv4, máscara y MAC de mallet y de alice se pueden observar con el comando `ifconfig/ifconfig -a`:

```
mallet@mallet: ~
File Edit View Terminal Help
(Broadcast) tell mallet.local, length 28
13:59:00.358615 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.2.128
(Broadcast) tell mallet.local, length 28
^C13:59:00.358659 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 10.0.2.12
9 (Broadcast) tell mallet.local, length 28

137 packets captured
1480 packets received by filter
0 packets dropped by kernel
mallet@mallet:~$ ifconfig -a
eth4      Link encap:Ethernet  HWaddr 08:00:27:6c:2a:f4
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6c:2af4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5776 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7491 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:439174 (439.1 KB)  TX bytes:441612 (441.6 KB)
```

IPv4, máscara, MAC de Bob (antes de ejecutar el comando “`ip a`” y obtener la información necesaria, utilizamos “`ifdown eth0`” y “`ifup eth0`” para reiniciar la tarjeta de red):

```
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ql
en 1000
    link/ether 08:00:27:71:55:b0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
    inet6 fe80::a00:27ff:fe71:55b0/64 scope link
    valid_lft forever preferred_lft forever
```

El DNS y el DHCP de virtual box:

```
mallet@mallet: ~  
File Edit View Terminal Help  
mallet@mallet:~$ sudo nmap 10.0.2.0/24 -n -sA  
[sudo] password for mallet:  
  
Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-15 13:50 CEST  
All 1000 scanned ports on 10.0.2.1 are unfiltered  
MAC Address: 52:54:00:12:35:00 (QEMU Virtual NIC)  
All 1000 scanned ports on 10.0.2.2 are unfiltered  
MAC Address: 52:54:00:12:35:00 (QEMU Virtual NIC)  
All 1000 scanned ports on 10.0.2.3 are filtered  
MAC Address: 08:00:27:55:74:1E (Cadmus Computer Systems)  
All 1000 scanned ports on 10.0.2.4 are unfiltered  
MAC Address: 08:00:27:7E:1A:EB (Cadmus Computer Systems)  
All 1000 scanned ports on 10.0.2.5 are unfiltered  
All 1000 scanned ports on 10.0.2.15 are unfiltered  
MAC Address: 08:00:27:71:55:B0 (Cadmus Computer Systems)  
  
Nmap done: 256 IP addresses (6 hosts up) scanned in 3.48 seconds  
mallet@mallet:~$ sudo nmap 10.0.2.0/24 -n -sP
```

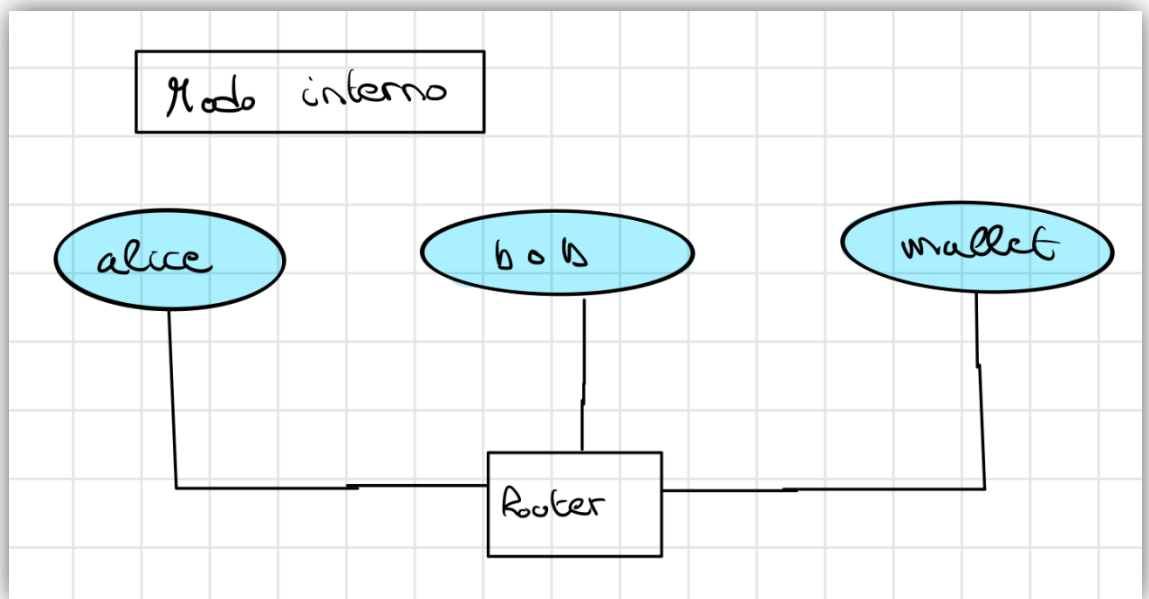
IPv4 de Router:

```
root@alice: ~  
File Edit View Terminal Help  
root@alice:~# route  
Kernel IP routing table  
Destination Gateway Genmask Flags Metric Ref Use Iface  
10.0.2.0 * 255.255.255.0 U 0 0 0 eth3  
link-local * 255.255.0.0 U 1000 0 0 eth3  
Sdefault 10.0.2.1 0.0.0.0 UG 100 0 0 eth3  
root@alice:~#
```

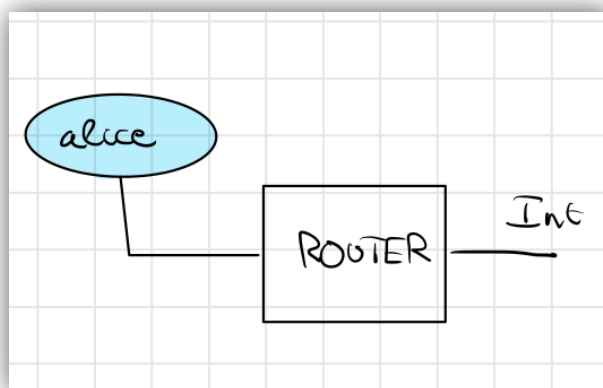
**Pregunta 4:**

Indica con tus palabras cuál es la diferencia, en el sistema de virtualización utilizado, entre el modo NAT, red NAT y red interna; para entenderlo mejor, proporciona un ejemplo gráfico de cada uno de los modos de funcionamiento.

Modo Interno: Las únicas conexiones que existen son entre las máquinas, estas máquinas no se conectan ni con el host ni con internet. El esquema sería algo así:



Modo NAT: Las máquinas se conectan con internet, pero no entre ellas. El siguiente boceto muestra de forma aproximada cómo funciona:



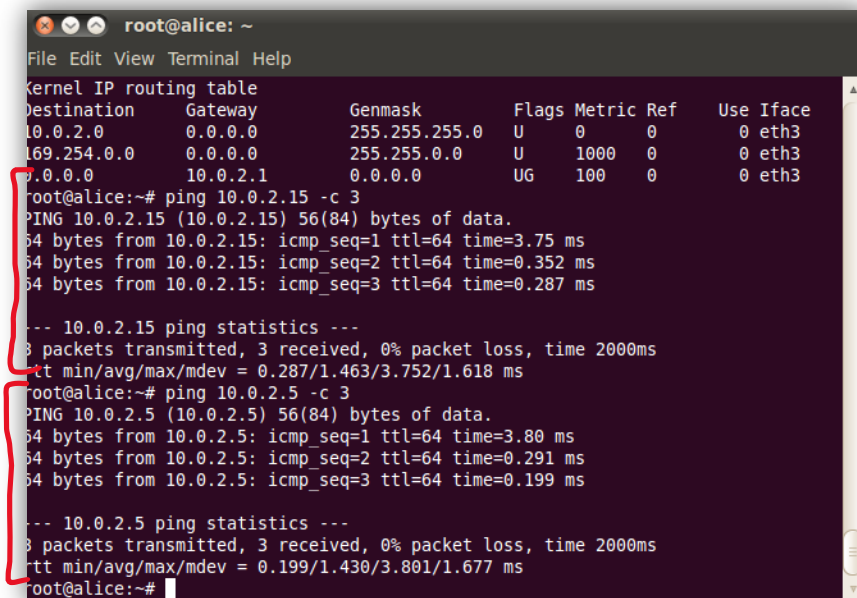


El modo red NAT es el mostrado en el esquema del ejercicio tres. En este se conectan las máquinas entre ellas, al router y a internet.

#### **Pregunta 5:**

**Realiza pruebas para comprobar que las máquinas virtuales se comunican entre sí a nivel de red (capa 3 del modelo de referencia OSI). Para ello, puedes utilizar el comando ping. Documenta la información necesaria que justifique que las máquinas tienen comunicación a nivel de red.**

Para comprobar las conexiones he hecho ping (con el flag -c 3 para que solo se hagan 3 envíos y no tener que interrumpir el ping) desde alice a bob y a mallet. Tras esto ya sabemos que alice se conecta a bob y a mallet, solo faltaría comprobar desde a mallet a bob.



The screenshot shows a terminal window titled 'root@alice: ~'. It displays the kernel IP routing table and the results of two ping tests performed from the 'root@alice' user.

```
root@alice: ~
File Edit View Terminal Help

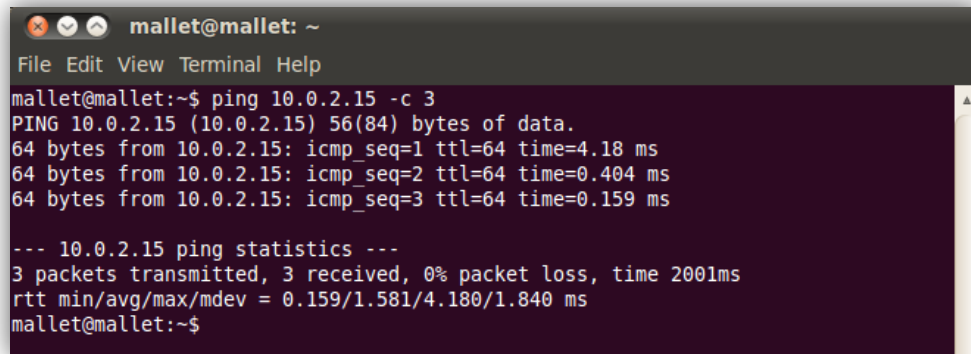
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          0.0.0.0         0.0.0.0         U        0      0      0 eth3
169.254.0.0      0.0.0.0         0.0.0.0         U        1000   0      0 eth3
10.0.0.0         10.0.2.1        0.0.0.0         UG       100    0      0 eth3

root@alice:~# ping 10.0.2.15 -c 3
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data:
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=3.75 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.352 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.287 ms

--- 10.0.2.15 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.287/1.463/3.752/1.618 ms
root@alice:~# ping 10.0.2.5 -c 3
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data:
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=3.80 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=0.291 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=0.199 ms

--- 10.0.2.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.199/1.430/3.801/1.677 ms
root@alice:~#
```

A continuación el ping entre mallet y bob para terminar de confirmar las conexiones:

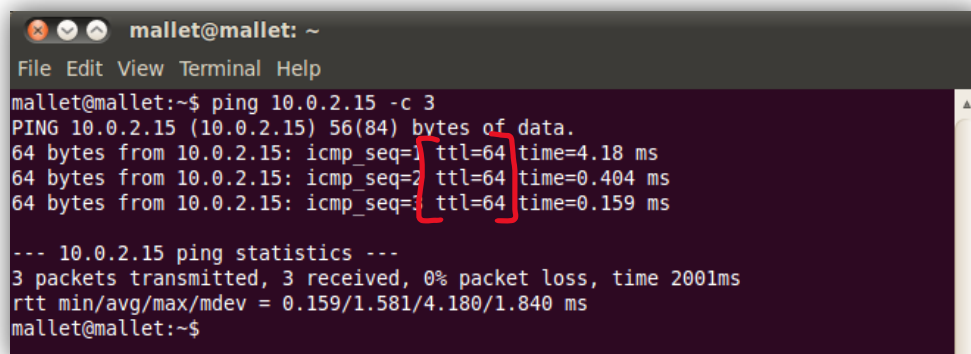


```
mallet@mallet: ~  
File Edit View Terminal Help  
mallet@mallet:~$ ping 10.0.2.15 -c 3  
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.  
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=4.18 ms  
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.404 ms  
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.159 ms  
  
--- 10.0.2.15 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2001ms  
rtt min/avg/max/mdev = 0.159/1.581/4.180/1.840 ms  
mallet@mallet:~$
```

### Pregunta 6:

¿Es posible inferir el sistema operativo de cada una de las máquinas a través del valor del TTL (Time To Live) del paquete que devuelven las máquinas después de recibir una petición de tipo ICMP(8)? Justifica tu respuesta. El siguiente enlace puede resultarte de utilidad: <https://subinsb.com/default-device-ttl-values/>

Según la información que proporciona el enlace, si que es posible diferenciar el sistema operativo. Esto es debido a que cada sistema operativo tiene un TTL asignado. En nuestro caso podemos observar como el TTL resultante de los ping es siempre 64, ya que 64 es el TTL predeterminado de los sistemas Linux. Si, por ejemplo, el TTL fuese 128 sabríamos que este TTL es el predeterminado asignado a los sistemas Windows.



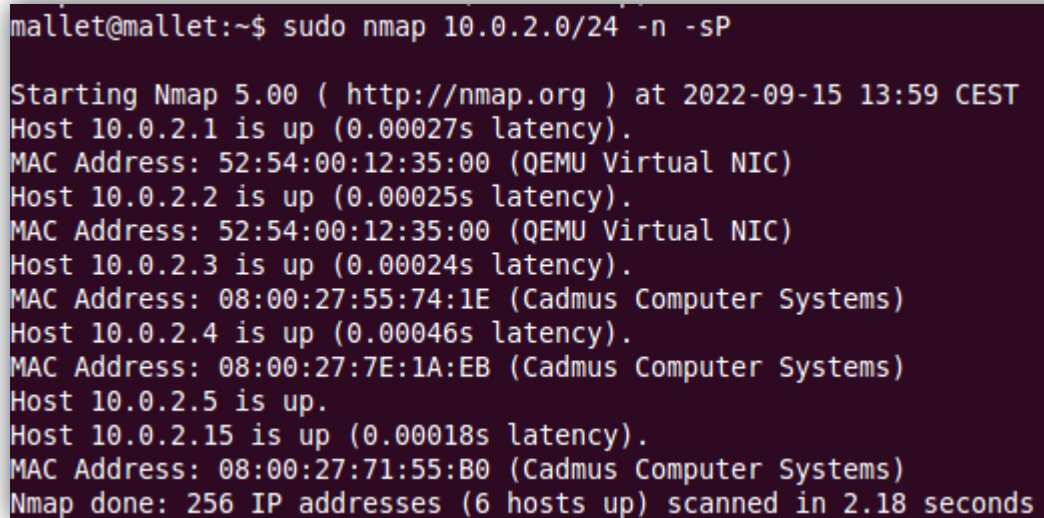
```
mallet@mallet: ~  
File Edit View Terminal Help  
mallet@mallet:~$ ping 10.0.2.15 -c 3  
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.  
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=4.18 ms  
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.404 ms  
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.159 ms  
  
--- 10.0.2.15 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2001ms  
rtt min/avg/max/mdev = 0.159/1.581/4.180/1.840 ms  
mallet@mallet:~$
```

### Pregunta 7:

Desde la máquina "mallet", utiliza la herramienta "map" para realizar un

**descubrimiento de los hosts que se encuentren en su mismo segmento de red pero sin escanear ningún servicio TCP/UDP. ¿Qué protocolo te parece más adecuado para ello, ARP o ICMP? Justifica tu respuesta.**

Antes de realizar el análisis, la tarjeta se pone en modo promiscuo para escuchar todo lo que va por la red. Utilizamos el siguiente comando “sudo nmap 10.0.2.0/24 -n -sP”, en el que las flags son “-n” para indicar que no realice nunca resolución por DNS y “-sP” para indicar que se envía ACK vacío y no se escanee TCP/UDP.

A terminal window with a dark purple background showing the output of a network scan. The command entered is 'sudo nmap 10.0.2.0/24 -n -sP'. The output lists several hosts that are 'up' with their latency, MAC addresses, and manufacturer information. The scan is completed in 2.18 seconds, finding 6 hosts up out of 256 IP addresses scanned.

```
mallet@mallet:~$ sudo nmap 10.0.2.0/24 -n -sP

Starting Nmap 5.00 ( http://nmap.org ) at 2022-09-15 13:59 CEST
Host 10.0.2.1 is up (0.00027s latency).
MAC Address: 52:54:00:12:35:00 (QEMU Virtual NIC)
Host 10.0.2.2 is up (0.00025s latency).
MAC Address: 52:54:00:12:35:00 (QEMU Virtual NIC)
Host 10.0.2.3 is up (0.00024s latency).
MAC Address: 08:00:27:55:74:1E (Cadmus Computer Systems)
Host 10.0.2.4 is up (0.00046s latency).
MAC Address: 08:00:27:7E:1A:EB (Cadmus Computer Systems)
Host 10.0.2.5 is up.
Host 10.0.2.15 is up (0.00018s latency).
MAC Address: 08:00:27:71:55:B0 (Cadmus Computer Systems)
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.18 seconds
```

Usaré esta captura también para mostrar la existencia de servidor DNS y DHCP en la red en el ejercicio 3.

ARP tiene muchas ventajas en estos casos. Tiene un mecanismo de cache propio y IPv4 no puede almacenar direcciones. ARP obtiene direcciones MAC por medio de peticiones a todos los hosts de la misma red, es como si gritásemos el nombre de alguien en una sala de espera, el nombre le oirán todos, pero solo contestará y entrará en la consulta la persona con ese nombre.

Por otro lado, ICMP está mas enfocado a envío de mensajes de error o información operativa para uno o varios segmentos de red. Por estos motivos y porque solo tenemos un segmento de red creo que es más adecuado la utilización de ARP.

**Pregunta 8:**

**Indica los problemas que te has encontrado y cómo los has resuelto .**

1. En los primeros ejercicios tuve dificultades para encontrar el DNS y el DHCP. Además de esto tuve que recordar bastantes cosas de redes, no me acordaba de comandos y algunas funciones.
2. Tampoco sabía como eran exactamente los esquemas de modo NAT, modo interno, y modo red NAT. Lo que he hecho es una aproximación según información que ido buscando.
3. Cuando entré por primera vez en bob me salía una IPv4 muy distinta a la que me daba en clase. Tardé un buen rato en darme cuenta de que tenía que reiniciar la tarjeta de internet de la máquina.