



Apelidos, Nome: Iglesias Nieto, Rodrigo

Proxecto de configuración de redes

Introdución: Neste prototipo de configuración dunha rede empresarial empregaremos catro máquinas virtuais, como se detalla a continuación:

Cliente1: <ul style="list-style-type: none">○ Máquina virtual○ Sistema operativo: Windows 10○ Hostname: cliente1○ Rede VirtualBox:<ul style="list-style-type: none">▪ Adapter 1:<ul style="list-style-type: none">• Attached to: Internal Network• Name: intnet• IP: 192.168.250.101	Cliente2: <ul style="list-style-type: none">○ Máquina virtual○ Sistema operativo: Windows 10○ Hostname: cliente2○ Rede VirtualBox:<ul style="list-style-type: none">▪ Adapter 1:<ul style="list-style-type: none">• Attached to: Internal Network• Name: intnet• IP: 192.168.250.102
Cliente3: <ul style="list-style-type: none">○ Máquina virtual○ Sistema operativo: Ubuntu 22 (GUI)○ Hostname: cliente3○ Rede VirtualBox:<ul style="list-style-type: none">▪ Adapter 1:<ul style="list-style-type: none">• Attached to: Internal Network• Name: intnet• IP: 192.168.250.103	Server: <ul style="list-style-type: none">○ Máquina virtual○ Sistema operativo: Debian 11 (CLI)○ Hostname: server○ Rede VirtualBox:<ul style="list-style-type: none">▪ Adapter 1:<ul style="list-style-type: none">• Attached to: NAT• IP: 10.0.2.15/24• Broadcast: 10.0.2.255• Gateway: 10.0.2.2• DNS: 10.0.2.3▪ Adapter 2:<ul style="list-style-type: none">• Attached to: Internal Network• Name: intnet• IP: 192.168.250.1

A máquina Server, aparte de proporcionar un servidor Web, actuará como porta de enlace para as máquinas clientes.

CA5.7 Utilizáronse dispositivos de interconexión de redes (10%)



1. Dada as seguintes especificacións (cliente1, cliente2 e cliente 3):

Cliente1:

- *Máquina virtual*
- *Sistema operativo: Windows 10*
- *Hostname: cliente1*
- *Rede VirtualBox:*
 - *Adapter 1:*
 - *Attached to: Internal Network*
 - *Name: intnet*
 - *IP: 192.168.250.101/24*

Cliente2:

- *Máquina virtual*
- *Sistema operativo: Windows 10*
- *Hostname: cliente1*
- *Rede VirtualBox:*
 - *Adapter 1:*
 - *Attached to: Internal Network*
 - *Name: intnet*
 - *IP: 192.168.250.102/24*

Cliente3:

- *Máquina virtual*
- *Sistema operativo: Ubuntu 22 (GUI)*
- *Hostname: cliente3*
- *Rede VirtualBox:*
 - *Adapter 1:*
 - *Attached to: Internal Network*
 - *Name: intnet*
 - *IP: 192.168.250.103/24*

a) Configura a rede de cliente1 segundo as especificacións subministradas. Comproba que cliente1 non ten acceso a Internet [Captura de pantalla da configuración de rede][Captura de pantalla de ping 8.8.8.8]

b) Configura a rede de cliente2 segundo as especificacións subministradas. Comproba que cliente2 non ten acceso a Internet [Captura de pantalla da configuración de rede][Captura de pantalla de ping 8.8.8.8]

c) Configura a rede de cliente3 segundo as especificacións subministradas. Comproba que cliente3 non ten acceso a Internet. [Captura de pantalla da configuración de rede][Captura de pantalla de ping 8.8.8.8]

d) Crea o cartafol “Sistemas informáticos” no escritorio de cliente1 [Captura de pantalla da máquina virtual co cartafol]

e) Comparte este cartafol para o grupo de traballo “Workgroup” e proporciona “Control total” para o grupo Todos. [Captura de pantalla de compartir]

f) Comproba dende cliente2 que podes acceder ao cartafol “Sistemas

informáticos" da máquina cliente1 [Captura de pantalla]

g) Configura as máquinas para que respondan a ping [Captura de pantalla]

h) Dende cliente1 fai ping á dirección IP de cliente2 [Captura de pantalla]

i) Dende cliente2 fai ping á dirección IP de cliente1 [Captura de pantalla]

j) Dende cliente1 fai ping á dirección IP de cliente3 [Captura de pantalla]

k) Dende cliente3 fai ping á dirección IP de cliente1 [Captura de pantalla]

Resposta

a) Configura a rede de cliente1 segundo as especificacións subministradas. Comproba que cliente1 non ten acceso a Internet [Captura de pantalla da configuración de rede]
[Captura de pantalla de ping 8.8.8.8]

```
cliente1_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

C:\Simbolo del sistema
Microsoft Windows [Versión 10.0.19044.1288]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\User>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

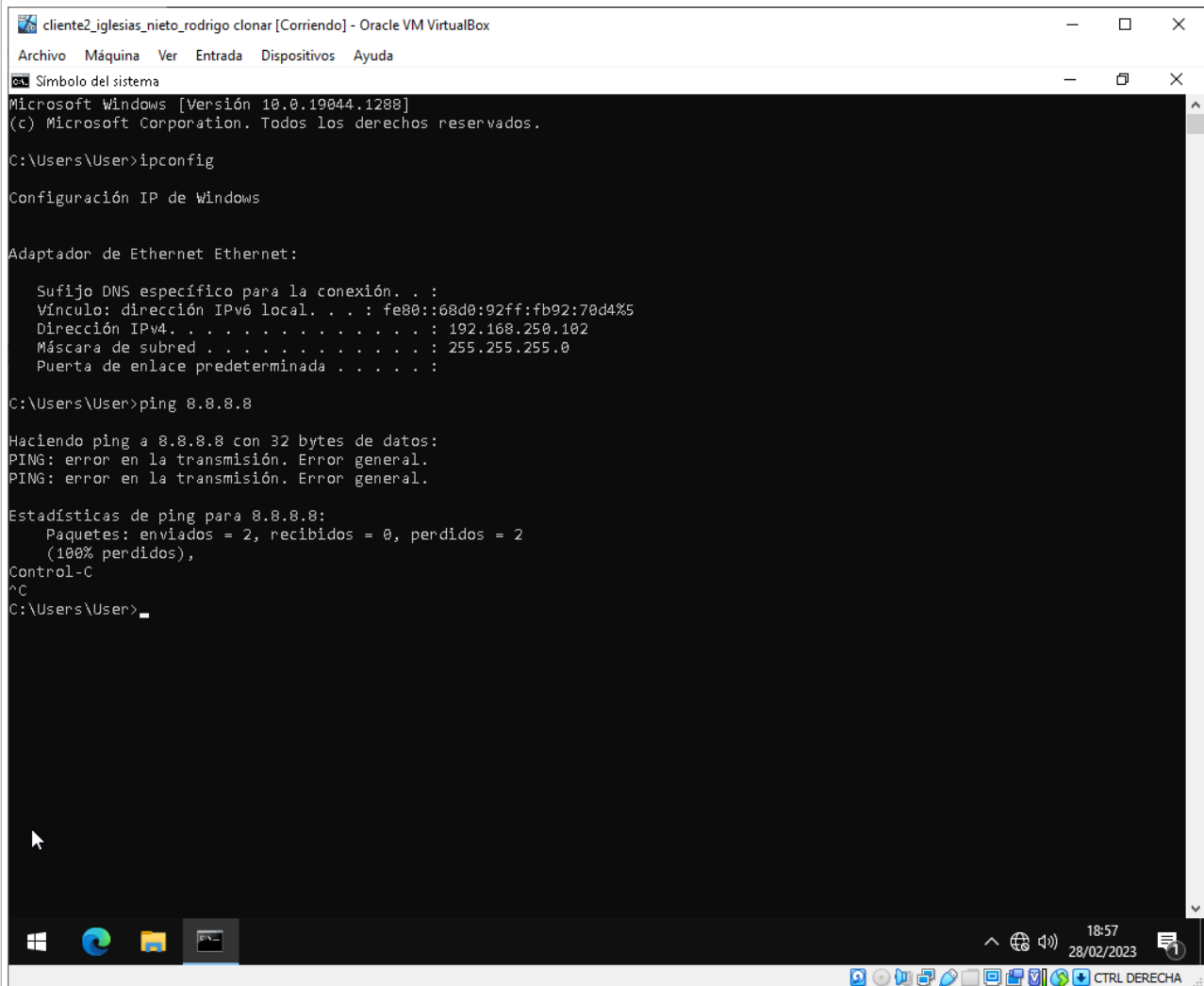
    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::ddd9:8fff:4d81:d552%5
    Dirección IPv4. . . . . : 192.168.250.101
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . :

C:\Users\User>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 2, recibidos = 0, perdidos = 2
    (100% perdidos),
Control-C
^C
C:\Users\User>
```

b) Configura a rede de cliente2 segundo as especificacións subministradas. Comproba que cliente2 non ten acceso a Internet [Captura de pantalla da configuración de rede] [Captura de pantalla de ping 8.8.8.8]



The screenshot shows a Windows command prompt window titled "cliente2_iglesias_nieto_rodrigo clonar [Corriendo] - Oracle VM VirtualBox". The window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". The command prompt shows the following text:

```
Microsoft Windows [Versión 10.0.19044.1288]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\User>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufixo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::68d0:92ff:fb92:70d4%5
    Dirección IPv4. . . . . : 192.168.250.102
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . :

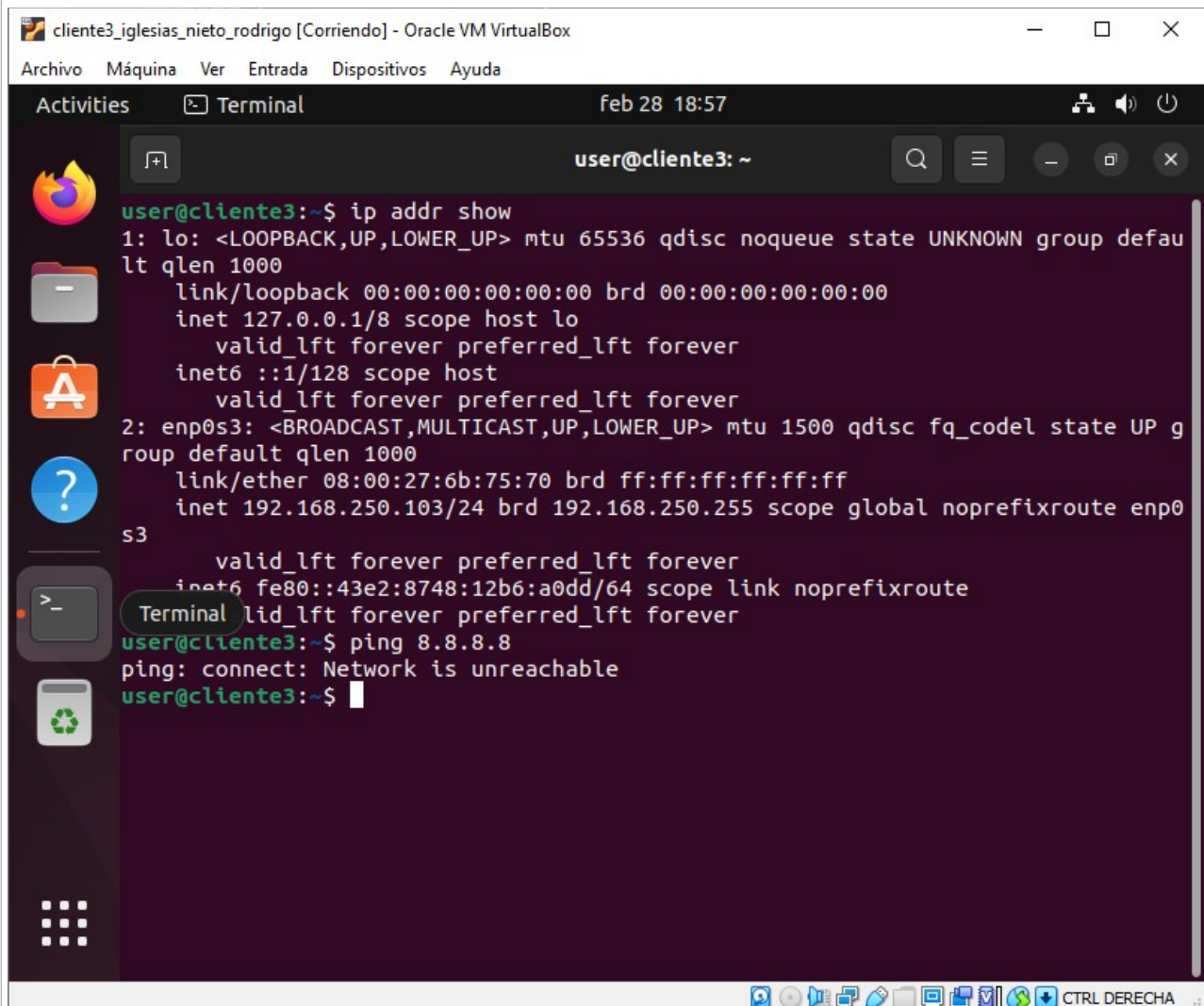
C:\Users\User>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 2, recibidos = 0, perdidos = 2
    (100% perdidos),
Control-C
^C
C:\Users\User>
```

The taskbar at the bottom shows the Windows logo, several application icons, and the system clock displaying 18:57 on 28/02/2023. A "CTRL DERECHA" button is visible in the bottom right corner of the taskbar.

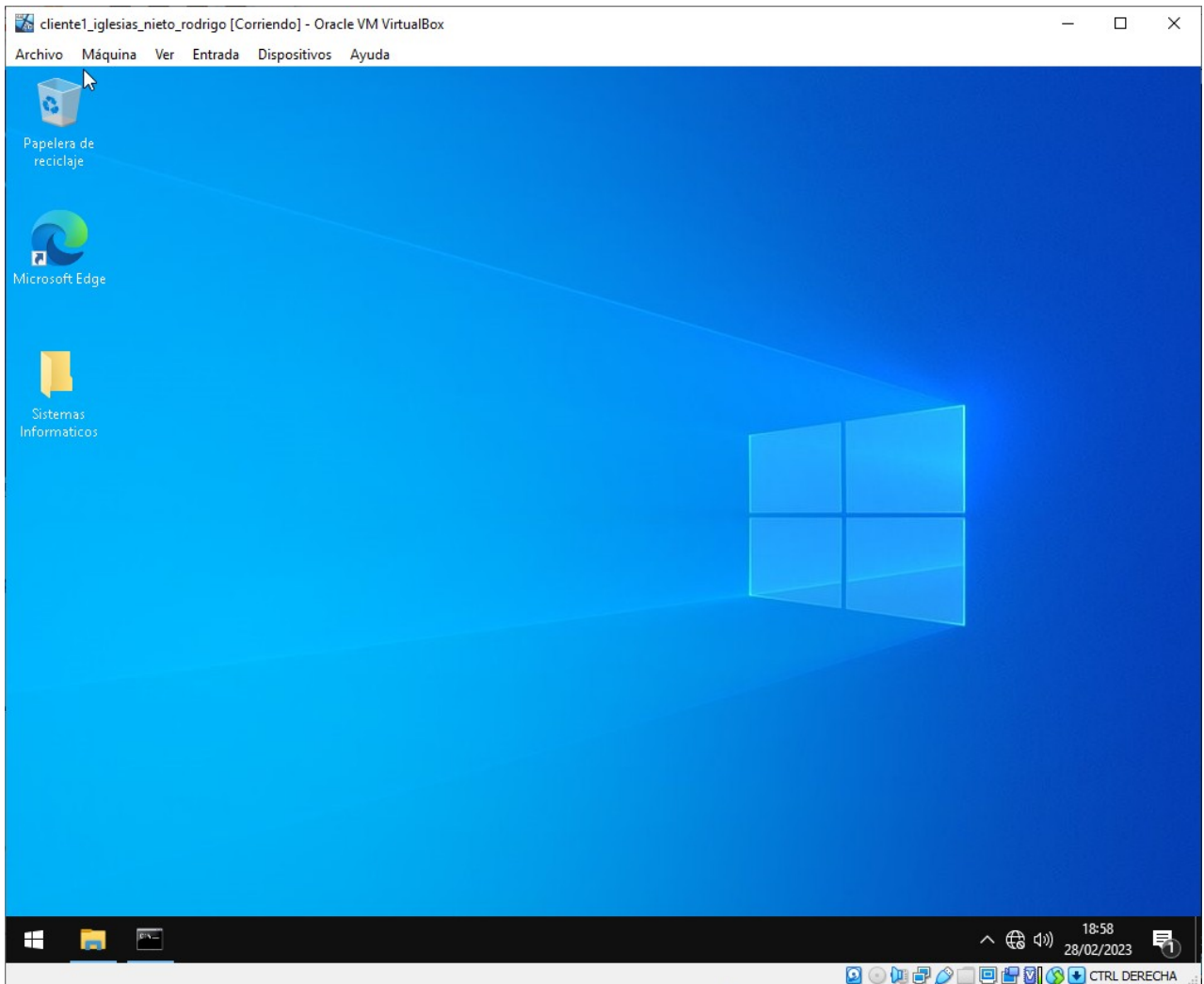
c) Configura a rede de cliente3 segundo as especificacións subministradas. Comproba que cliente3 non ten acceso a Internet. [Captura de pantalla da configuración de rede] [Captura de pantalla de ping 8.8.8.8]



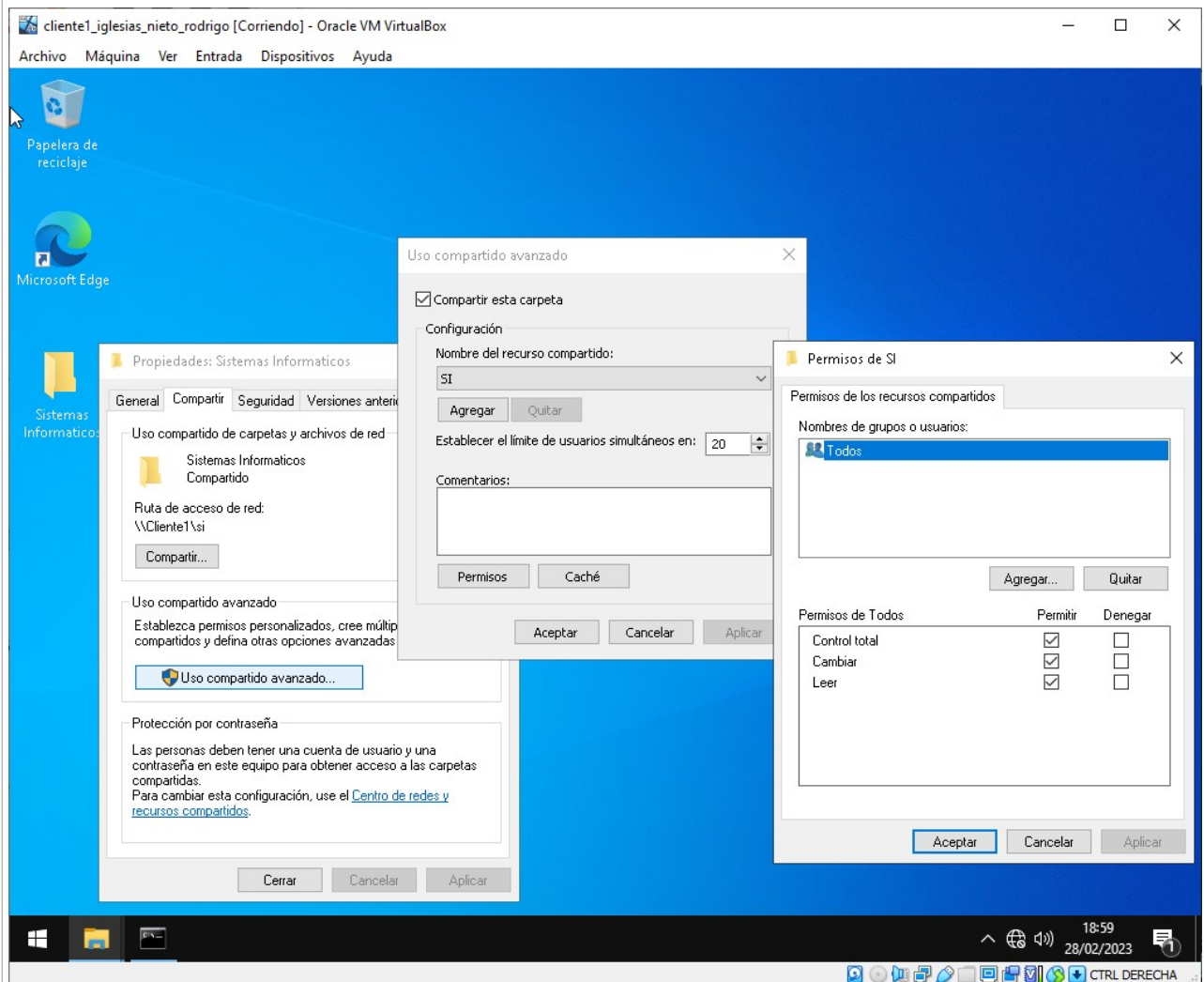
The screenshot shows a terminal window titled "cliente3_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox". The terminal displays the output of the command "ip addr show". It shows two network interfaces: "lo" (loopback) with IP 127.0.0.1 and "enp0s3" (ethernet) with IP 192.168.250.103. The "enp0s3" interface is configured with a static IP and a default gateway. Below the configuration, the command "ping 8.8.8.8" is executed, resulting in the message "ping: connect: Network is unreachable".

```
user@cliente3:~$ 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:6b:75:70 brd ff:ff:ff:ff:ff:ff
    inet 192.168.250.103/24 brd 192.168.250.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::43e2:8748:12b6:a0dd/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
user@cliente3:~$ ping 8.8.8.8
ping: connect: Network is unreachable
user@cliente3:~$
```

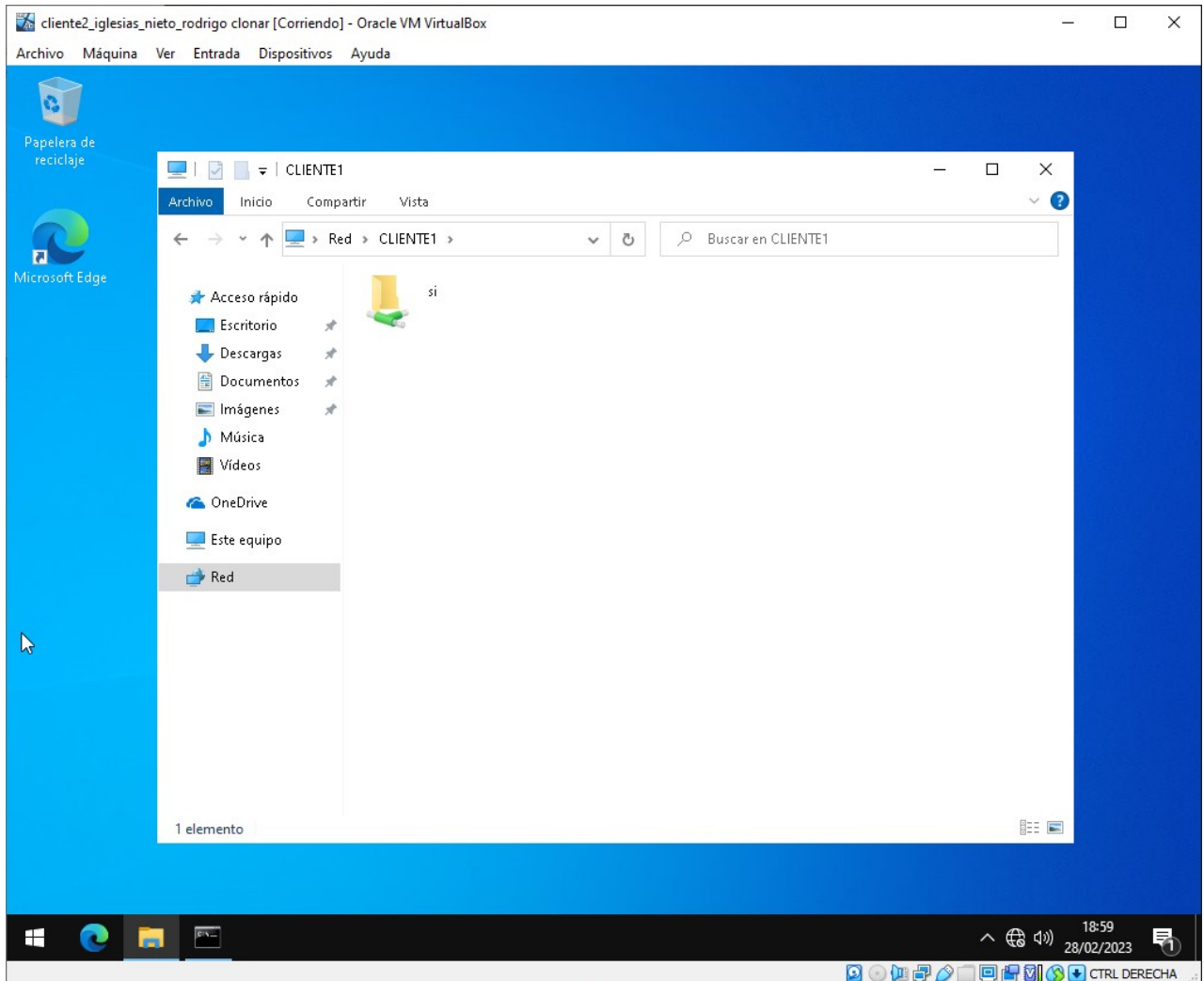
d) Crea o cartafol “Sistemas informáticos” no escritorio de cliente1 [Captura de pantalla da máquina virtual co cartafol]



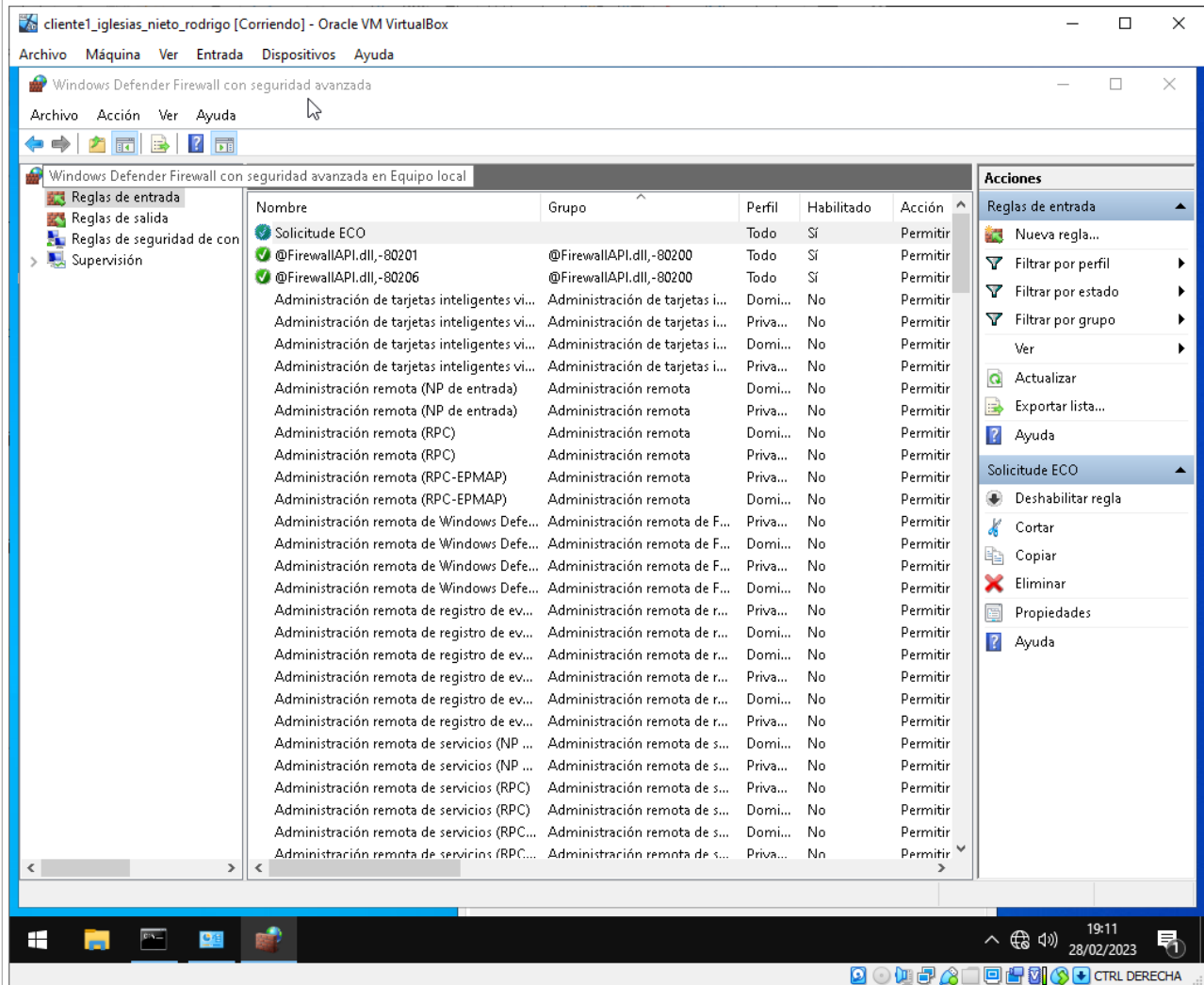
e) Comparte este cartafol para o grupo de traballo “Workgroup” e proporciona “Control total” para o grupo Todos. [Captura de pantalla de compartir]



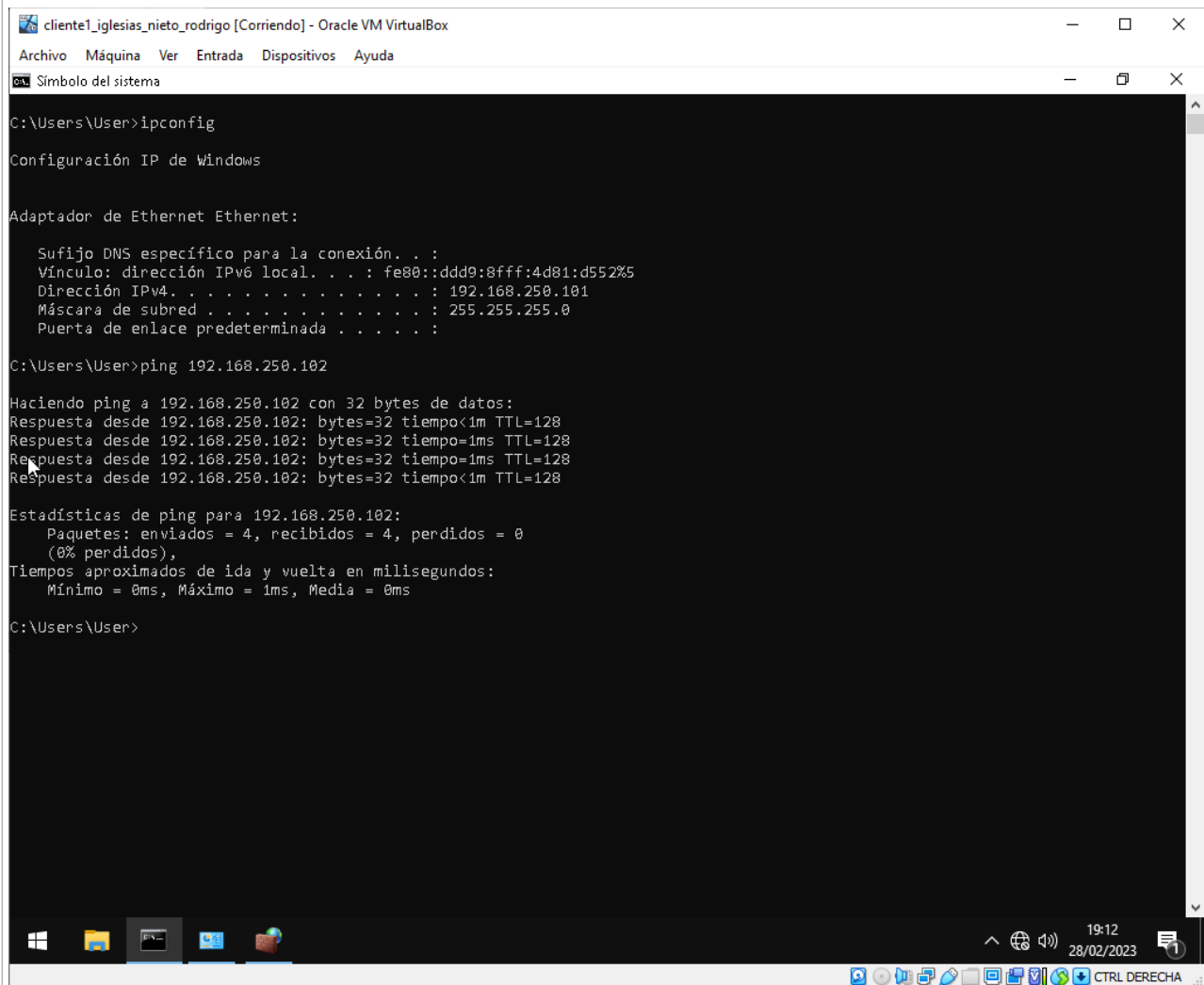
f) Comproba dende cliente2 que podes acceder ao cartafol “Sistemas informáticos” da máquina cliente1 [Captura de pantalla]



g) Configura as máquinas para que respondan a ping [Captura de pantalla]



h) Dende cliente1 fai ping á dirección IP de cliente2 [Captura de pantalla]



The screenshot shows a Windows command prompt window titled "cliente1_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox". The window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". The command prompt shows the following text:

```
C:\Users\User>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufixo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::ddd9:8fff:4d81:d552%5
    Dirección IPv4. . . . . : 192.168.250.101
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . :

C:\Users\User>ping 192.168.250.102

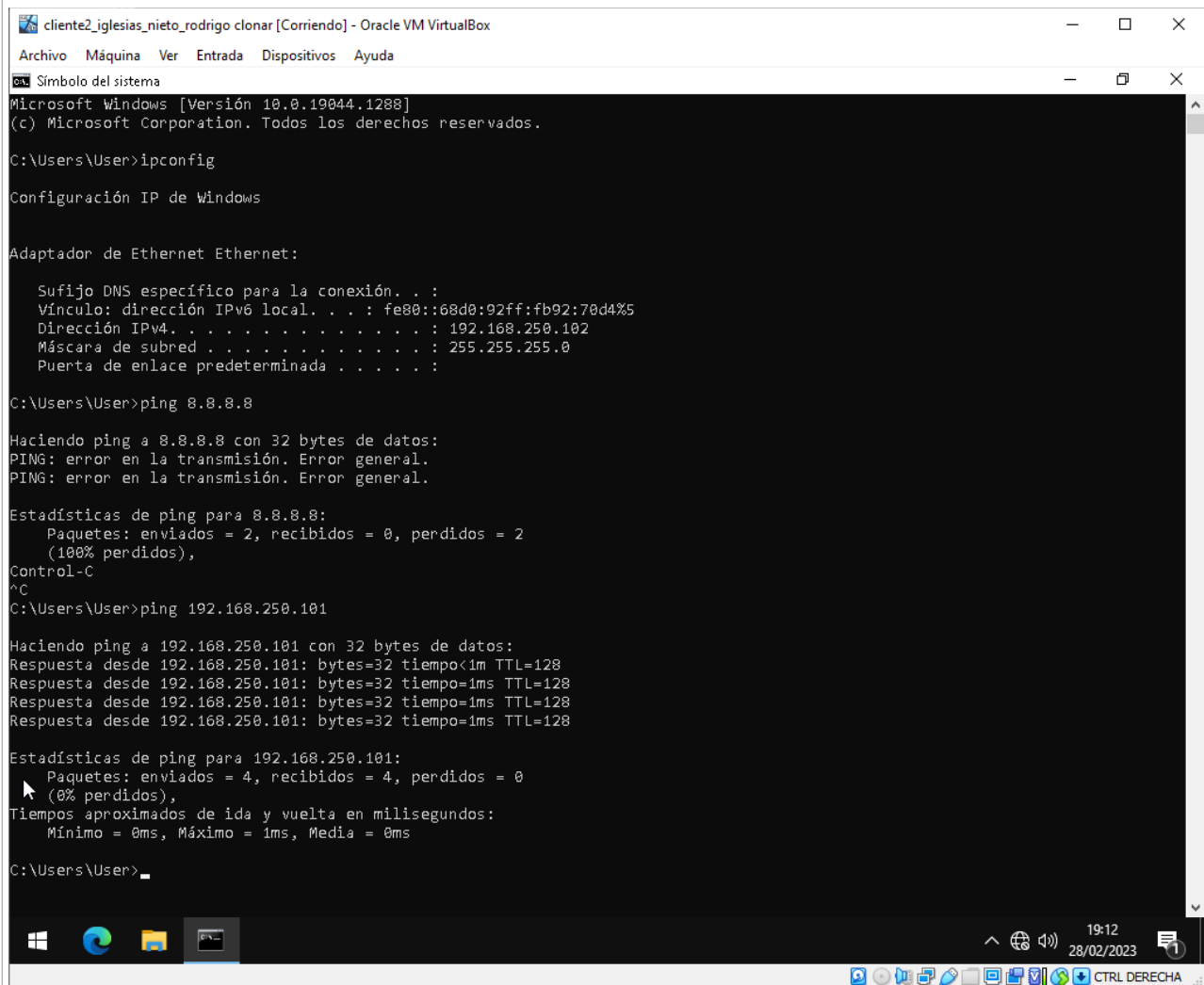
Haciendo ping a 192.168.250.102 con 32 bytes de datos:
Respuesta desde 192.168.250.102: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.250.102: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.250.102: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.250.102: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.250.102:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\User>
```

The taskbar at the bottom shows the Windows Start button, task view, and several application icons. The system tray on the right shows the time as 19:12, the date as 28/02/2023, and a notification icon. The text "CTRL DERECHA" is visible in the bottom right corner of the taskbar.

i) Dende cliente2 fai ping á dirección IP de cliente1 [Captura de pantalla]



```
cliente2_iglesias_nieto_rodrigo clonar [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

C:\Simbolo del sistema
Microsoft Windows [Versión 10.0.19044.1288]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\User>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufixo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::68d0:92ff:fb92:70d4%5
    Dirección IPv4. . . . . : 192.168.250.102
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

C:\Users\User>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.

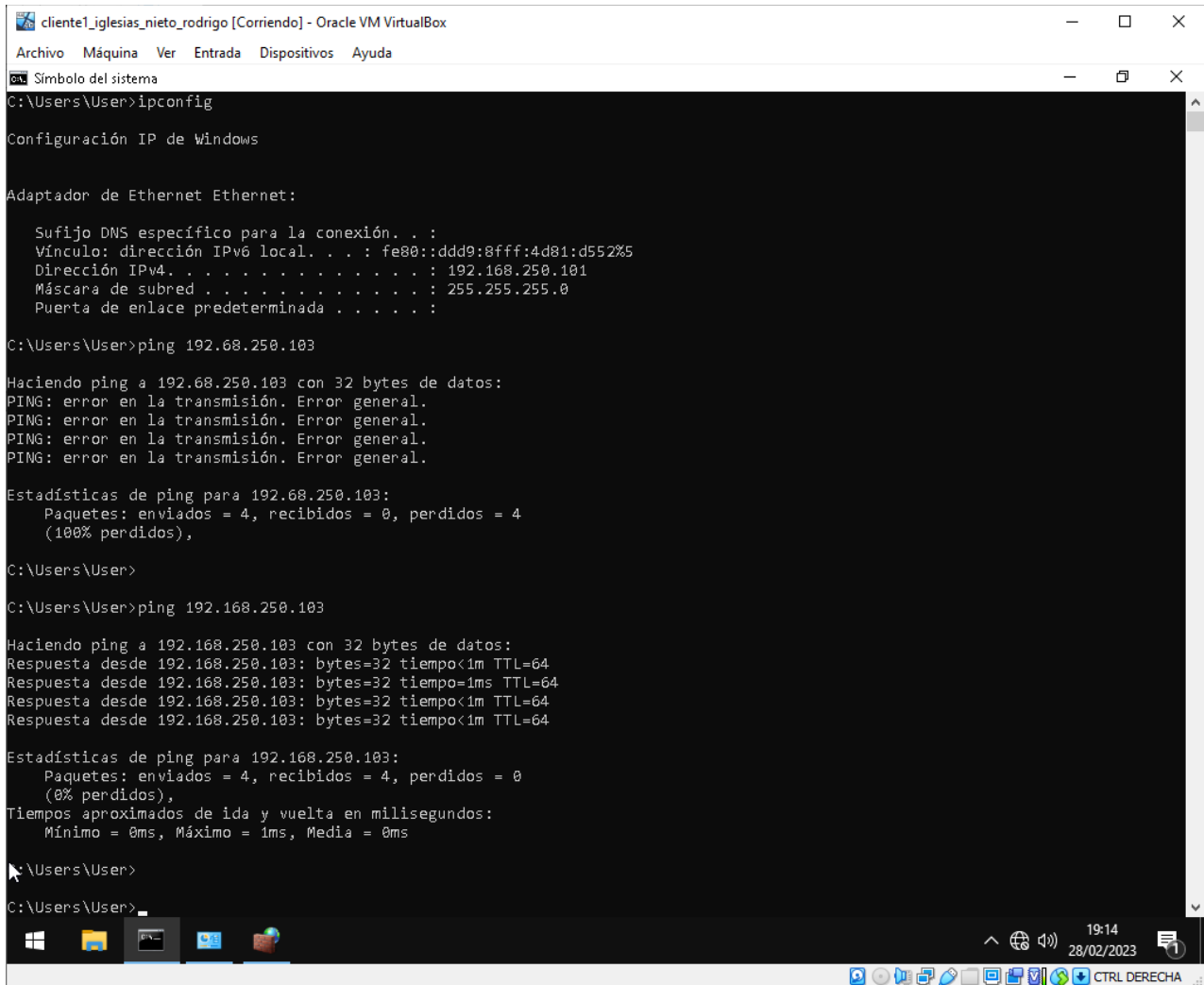
Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 2, recibidos = 0, perdidos = 2
    (100% perdidos),
Control-C
^C
C:\Users\User>ping 192.168.250.101

Haciendo ping a 192.168.250.101 con 32 bytes de datos:
Respuesta desde 192.168.250.101: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.250.101: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.250.101: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.250.101: bytes=32 tiempo=1ms TTL=128

Estadísticas de ping para 192.168.250.101:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\User>
```

j) Dende cliente1 fai ping á dirección IP de cliente3 [Captura de pantalla]



```
cliente1_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
C:\Users\User>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufixo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::ddd9:8fff:4d81:d52%5
    Dirección IPv4. . . . . : 192.168.250.101
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

C:\Users\User>ping 192.68.250.103

Haciendo ping a 192.68.250.103 con 32 bytes de datos:
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.

Estadísticas de ping para 192.68.250.103:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\Users\User>

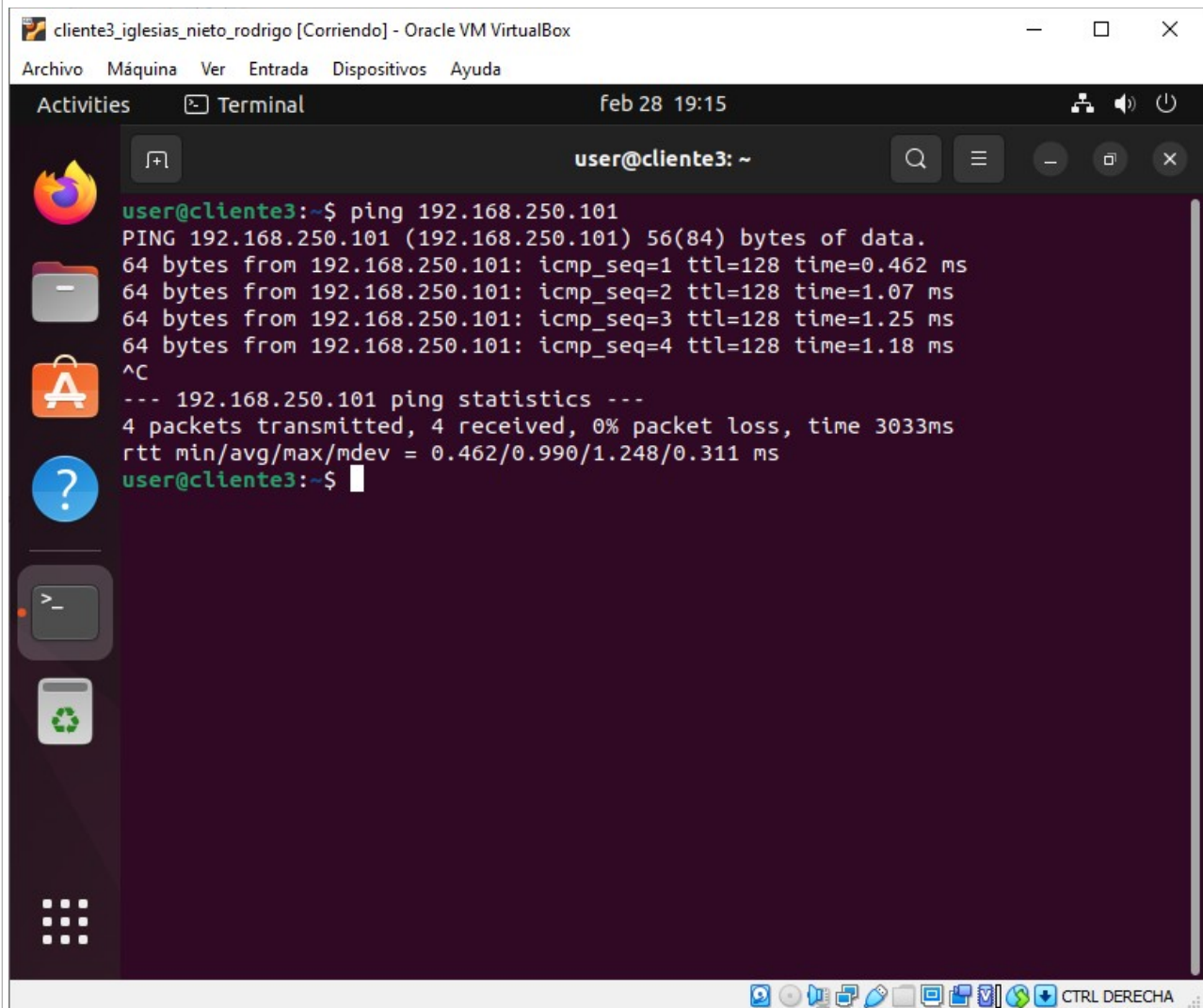
C:\Users\User>ping 192.168.250.103

Haciendo ping a 192.168.250.103 con 32 bytes de datos:
Respuesta desde 192.168.250.103: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.250.103: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.250.103: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.250.103: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.250.103:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\User>
```

k) Dende cliente3 fai ping á dirección IP de cliente1 [Captura de pantalla]



The screenshot shows a terminal window titled "cliente3_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox". The terminal displays the output of a ping command from "user@cliente3: ~" to the IP address 192.168.250.101. The output shows four successful ping attempts with varying response times. After pressing Ctrl+C, the terminal displays the ping statistics, indicating 4 packets transmitted, 4 received, and 0% packet loss. The terminal window is part of a desktop environment with a sidebar on the left containing icons for Firefox, Files, Applications, Help, and a terminal icon. The top bar shows the date and time as "feb 28 19:15". The bottom bar contains various system icons and the text "CTRL DERECHA".

```
user@cliente3:~$ ping 192.168.250.101
PING 192.168.250.101 (192.168.250.101) 56(84) bytes of data.
64 bytes from 192.168.250.101: icmp_seq=1 ttl=128 time=0.462 ms
64 bytes from 192.168.250.101: icmp_seq=2 ttl=128 time=1.07 ms
64 bytes from 192.168.250.101: icmp_seq=3 ttl=128 time=1.25 ms
64 bytes from 192.168.250.101: icmp_seq=4 ttl=128 time=1.18 ms
^C
--- 192.168.250.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3033ms
rtt min/avg/max/mdev = 0.462/0.990/1.248/0.311 ms
user@cliente3:~$
```

CA5.8 Configúrese o acceso a redes de área extensa (10%)



2. Configura a máquina server como se sinala a continuación:

Server:

- *Máquina virtual*
- *Sistema operativo: Debian 11 (CLI)*
- *Hostname: server*
- *Rede VirtualBox:*
 - *Adapter 1:*
 - *Attached to: NAT*
 - *IP: 10.0.2.15/24*
 - *Broadcast: 10.0.2.255*
 - *Gateway: 10.0.2.2*
 - *DNS: 10.0.2.3*
 - *Adapter 2:*
 - *Attached to: Internal Network*
 - *Name: intnet*
 - *IP: 192.168.250.1/24*

Para proceder con esta parte é necesario ter as máquinas cliente1 e cliente2 acendidas.

a) Configura os interfaces de rede segundo as especificacións subministradas [Captura de pantalla]

```
Server [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
user@server:~$ cat /etc/resolv.conf
nameserver 8.8.8.8
user@server:~$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

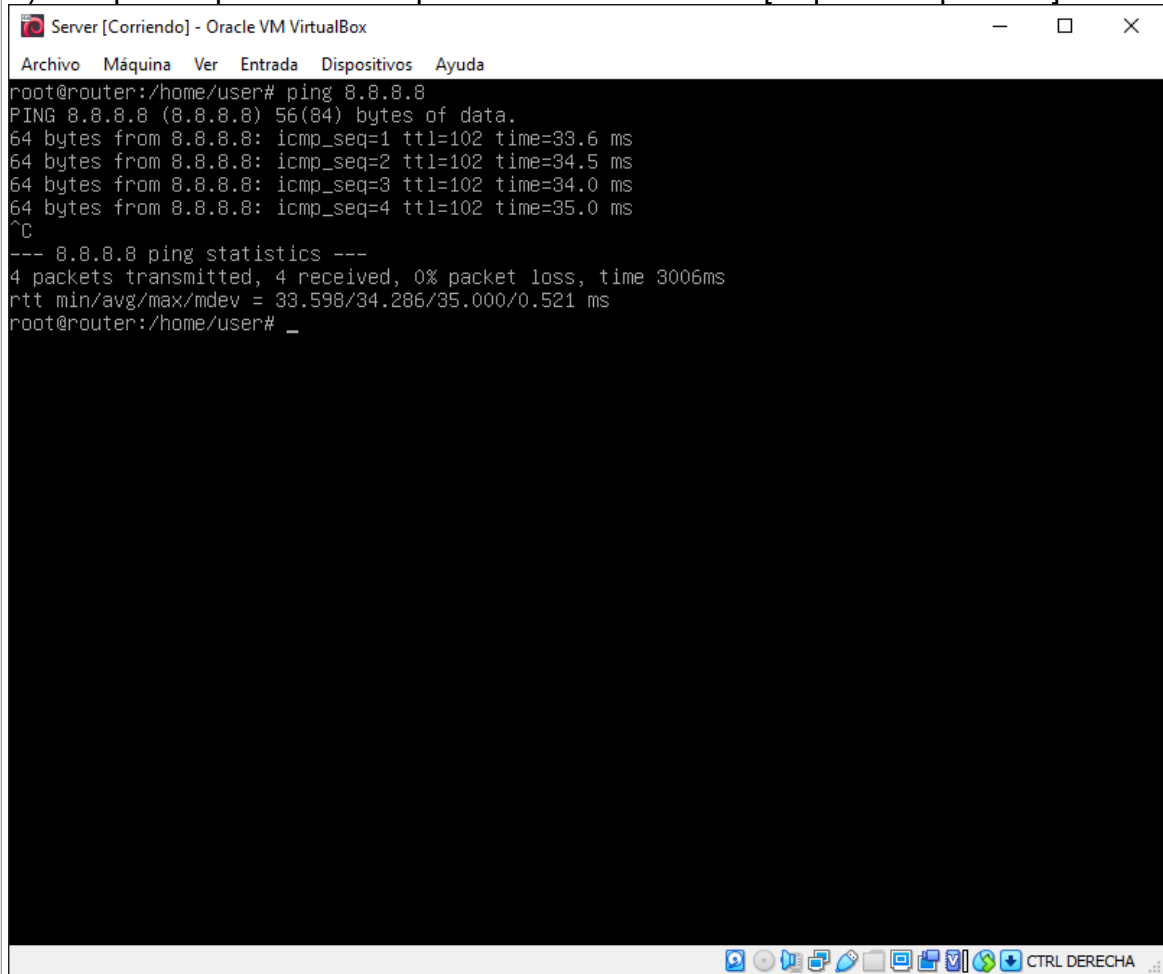
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface (Virtual Box Adapter 1 attached to NAT)
allow-hotplug enp0s3
iface enp0s3 inet static
address 10.0.2.15
netmask 255.255.255.0
broadcast 10.0.2.255
gateway 10.0.2.2

# Secondary network interface (Virtual Box Adapter 2 attached to internal network)
allow-hotplug enp0s8
iface enp0s8 inet static
address 192.168.250.1
netmask 255.255.255.0
user@server:~$
```

b) Comproba que o servidor pode acceder a Internet [Captura de pantalla]

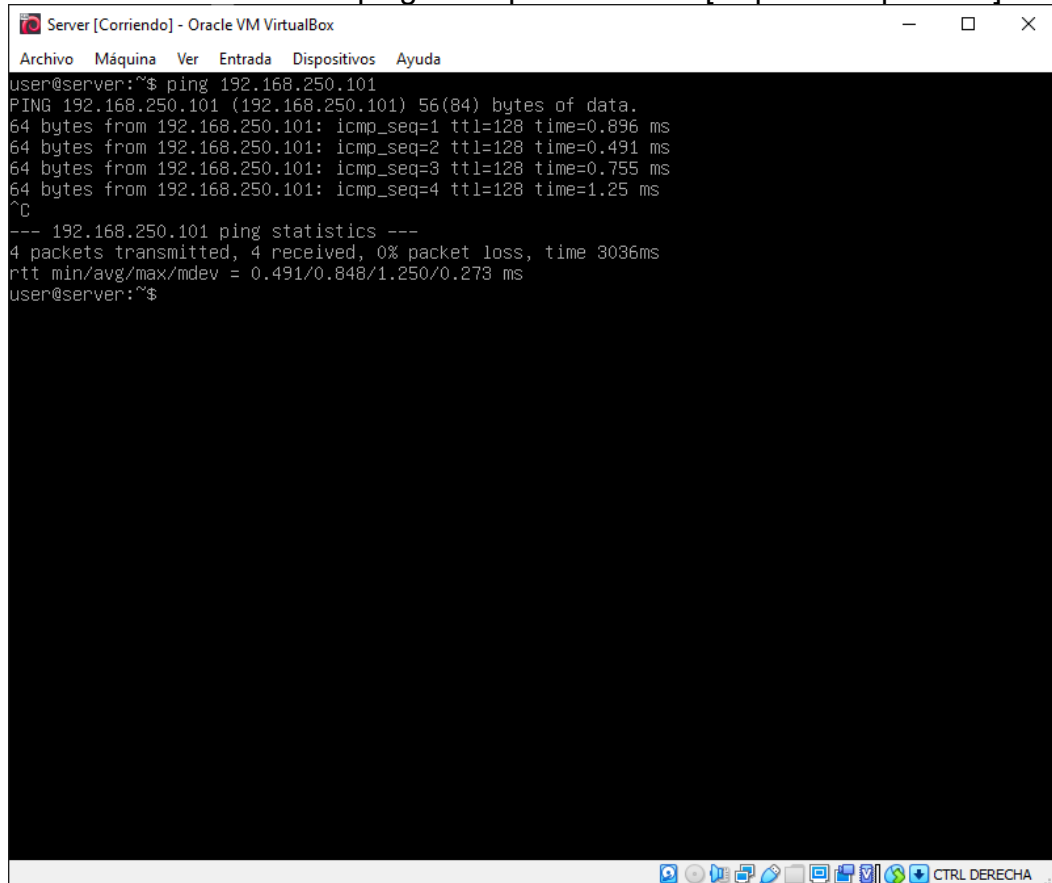


The screenshot shows a terminal window titled "Server [Corriendo] - Oracle VM VirtualBox". The terminal output is as follows:

```
root@router:/home/user# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=102 time=33.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=102 time=34.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=102 time=34.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=102 time=35.0 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 33.598/34.286/35.000/0.521 ms
root@router:/home/user# _
```

The terminal window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". The bottom status bar shows various icons and the text "CTRL DERECHA".

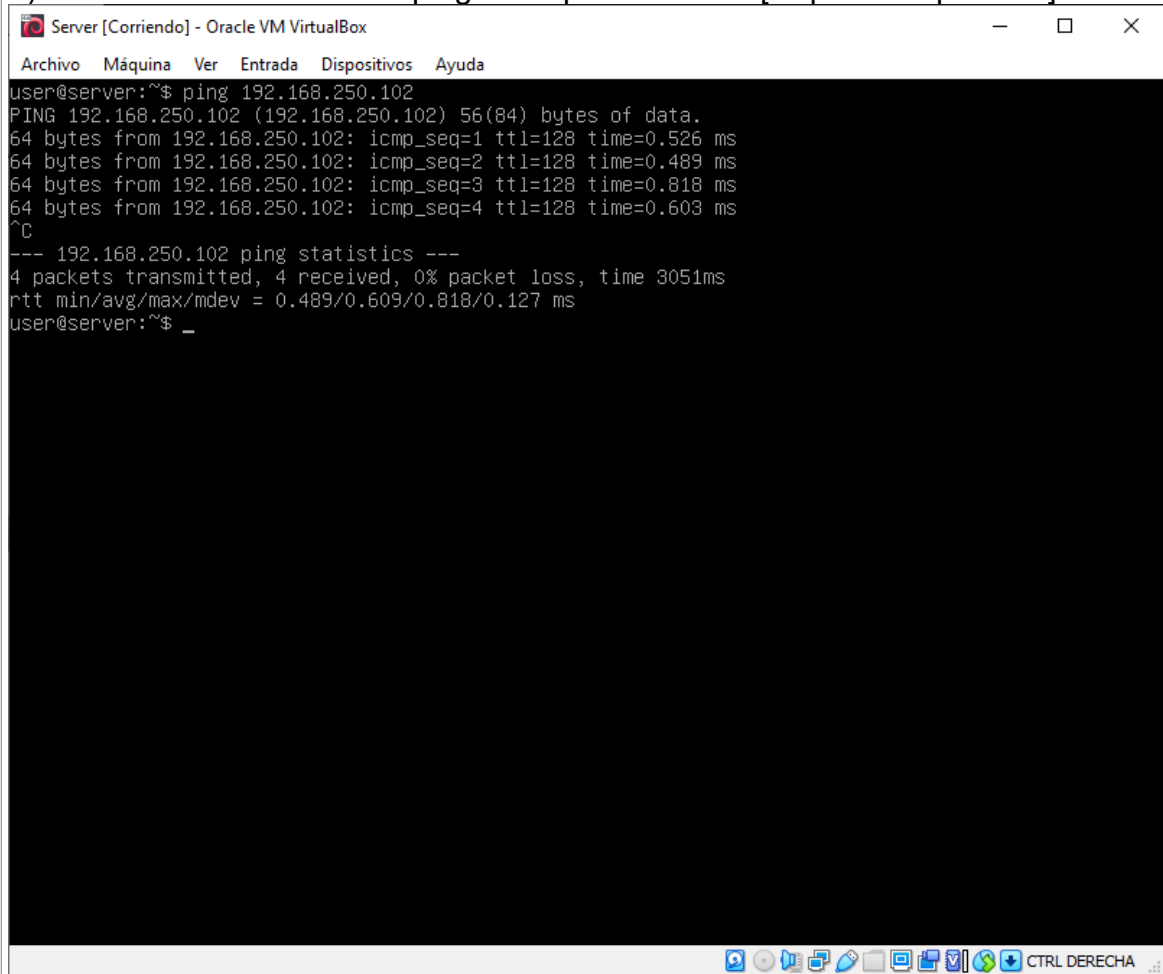
c) Dende o servidor efectúa ping á máquina cliente1 [Captura de pantalla]



The screenshot shows a terminal window titled "Server [Corriendo] - Oracle VM VirtualBox". The terminal displays the output of a ping command executed from a user@server prompt. The command is "ping 192.168.250.101". The output shows four successful ping requests, each with a 64-byte payload, a TTL of 128, and response times ranging from 0.491 ms to 1.25 ms. Below the individual pings, a summary line indicates "192.168.250.101 ping statistics ---", followed by "4 packets transmitted, 4 received, 0% packet loss, time 3036ms" and "rtt min/avg/max/mdev = 0.491/0.848/1.250/0.273 ms". The prompt "user@server:~\$" is visible at the bottom of the terminal output.

```
Server [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
user@server:~$ ping 192.168.250.101
PING 192.168.250.101 (192.168.250.101) 56(84) bytes of data:
64 bytes from 192.168.250.101: icmp_seq=1 ttl=128 time=0.896 ms
64 bytes from 192.168.250.101: icmp_seq=2 ttl=128 time=0.491 ms
64 bytes from 192.168.250.101: icmp_seq=3 ttl=128 time=0.755 ms
64 bytes from 192.168.250.101: icmp_seq=4 ttl=128 time=1.25 ms
^C
--- 192.168.250.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3036ms
rtt min/avg/max/mdev = 0.491/0.848/1.250/0.273 ms
user@server:~$
```


d) Dende o servidor efectúa ping á máquina cliente2 [Captura de pantalla]



The screenshot shows a terminal window titled "Server [Corriendo] - Oracle VM VirtualBox". The terminal output is as follows:

```
user@server:~$ ping 192.168.250.102
PING 192.168.250.102 (192.168.250.102) 56(84) bytes of data.
64 bytes from 192.168.250.102: icmp_seq=1 ttl=128 time=0.526 ms
64 bytes from 192.168.250.102: icmp_seq=2 ttl=128 time=0.489 ms
64 bytes from 192.168.250.102: icmp_seq=3 ttl=128 time=0.818 ms
64 bytes from 192.168.250.102: icmp_seq=4 ttl=128 time=0.603 ms
^C
--- 192.168.250.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3051ms
rtt min/avg/max/mdev = 0.489/0.609/0.818/0.127 ms
user@server:~$ _
```

The terminal window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". The bottom status bar shows various icons and the text "CTRL DERECHA".

Resposta

CA5.9 Xestionáronse portos de comunicacións (10%)

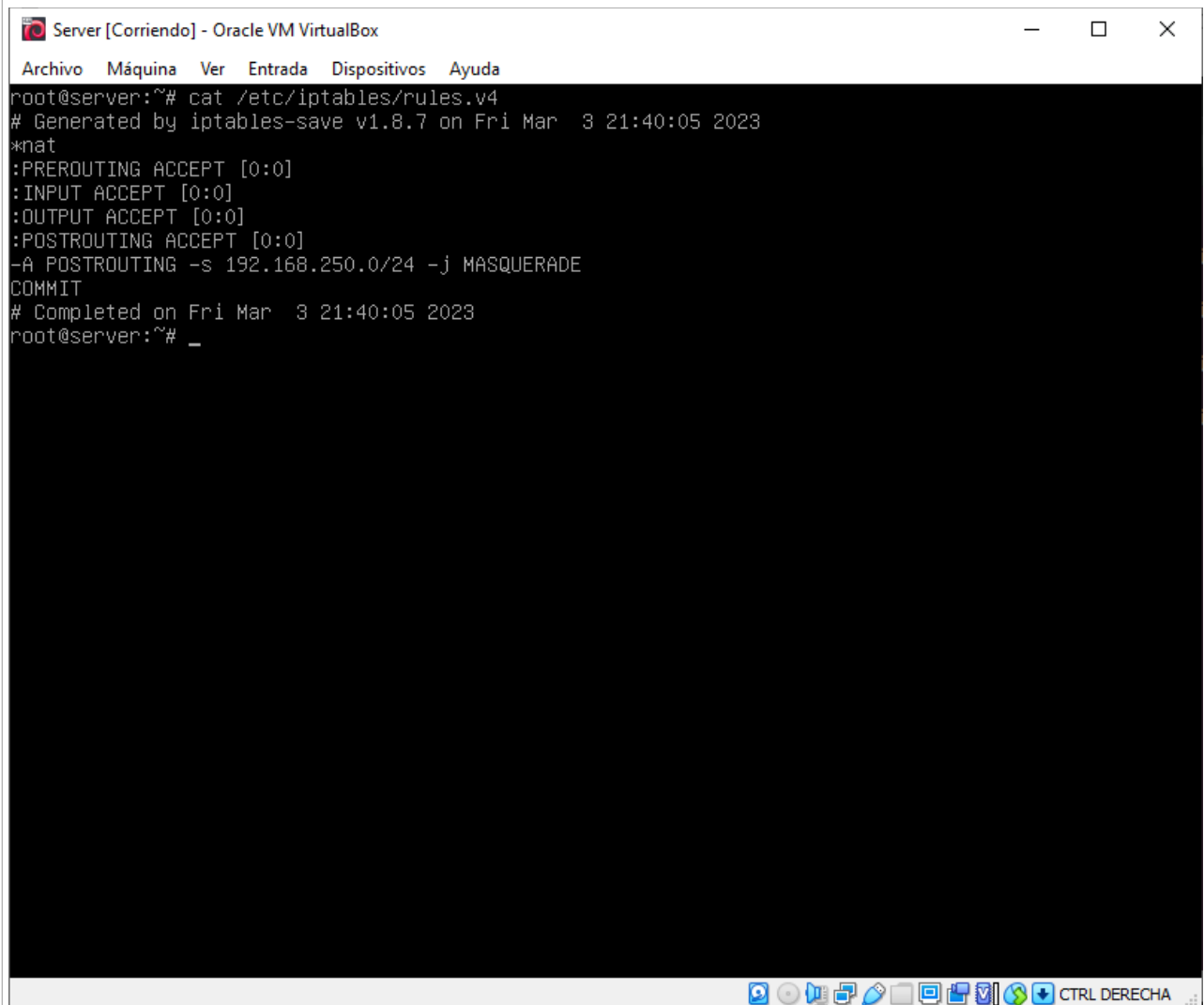


3. Configura a máquina server como router para que as máquinas cliente1 e cliente2 podan navegar por Internet.

- a) Configura o server como router [Captura de pantalla]
- b) Configura a rede de cliente1 para que a porta de enlace sexa a IP 192.168.250.1 correspondente ao servidor [Captura de pantalla]
- c) Comproba que o cliente1 é capaz de navegar por Internet [Captura de pantalla]
- d) Configura a rede de cliente2 para que a porta de enlace sexa a IP 192.168.250.1 correspondente ao servidor [Captura de pantalla]
- e) Comproba que o cliente2 é capaz de navegar por Internet [Captura de pantalla]
- f) Configura a rede de cliente3 para que a porta de enlace sexa a IP 192.168.250.1 correspondente ao servidor [Captura de pantalla]
- g) Comproba que o cliente3 é capaz de navegar por Internet [Captura de pantalla]

Resposta

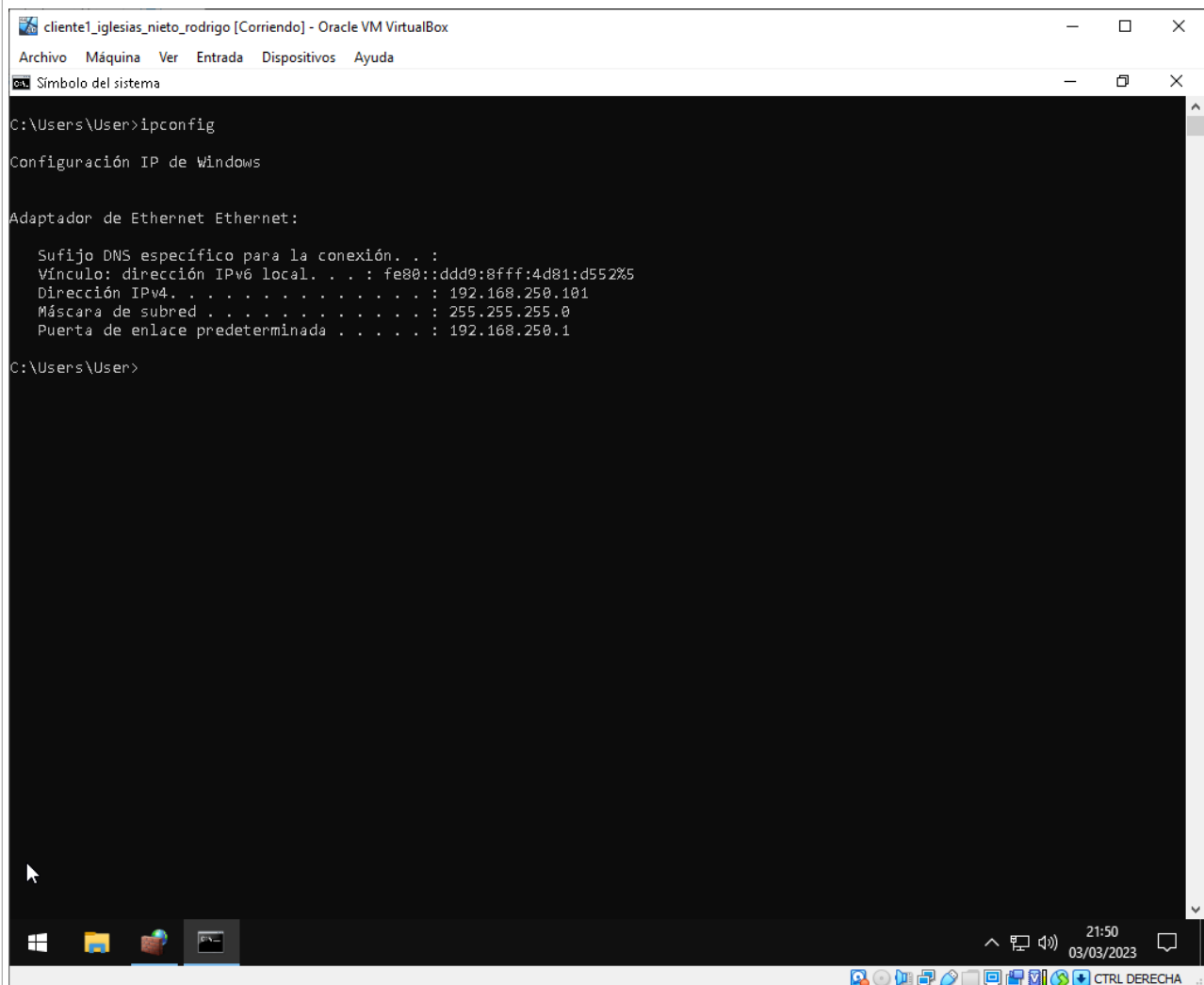
a) Configura o server como router [Captura de pantalla]



The screenshot shows a terminal window titled "Server [Corriendo] - Oracle VM VirtualBox". The terminal output displays the contents of the file /etc/iptables/rules.v4, which has been generated by iptables-save v1.8.7 on Fri Mar 3 21:40:05 2023. The configuration sets up NAT rules for the *nat table, accepting all PREROUTING, INPUT, OUTPUT, and POSTROUTING traffic. A specific rule is added to the POSTROUTING chain to masquerade traffic from the 192.168.250.0/24 network. The configuration is committed and the process is completed on the same date and time.

```
root@server:~# cat /etc/iptables/rules.v4
# Generated by iptables-save v1.8.7 on Fri Mar  3 21:40:05 2023
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -s 192.168.250.0/24 -j MASQUERADE
COMMIT
# Completed on Fri Mar  3 21:40:05 2023
root@server:~# _
```

b) Configura a rede de cliente1 para que a porta de enlace sexa a IP 192.168.250.1 correspondente ao servidor [Captura de pantalla]



The screenshot shows a Windows command prompt window titled "cliente1_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox". The window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". The command prompt shows the following text:

```
C:\Users\User>ipconfig

Configuración IP de Windows

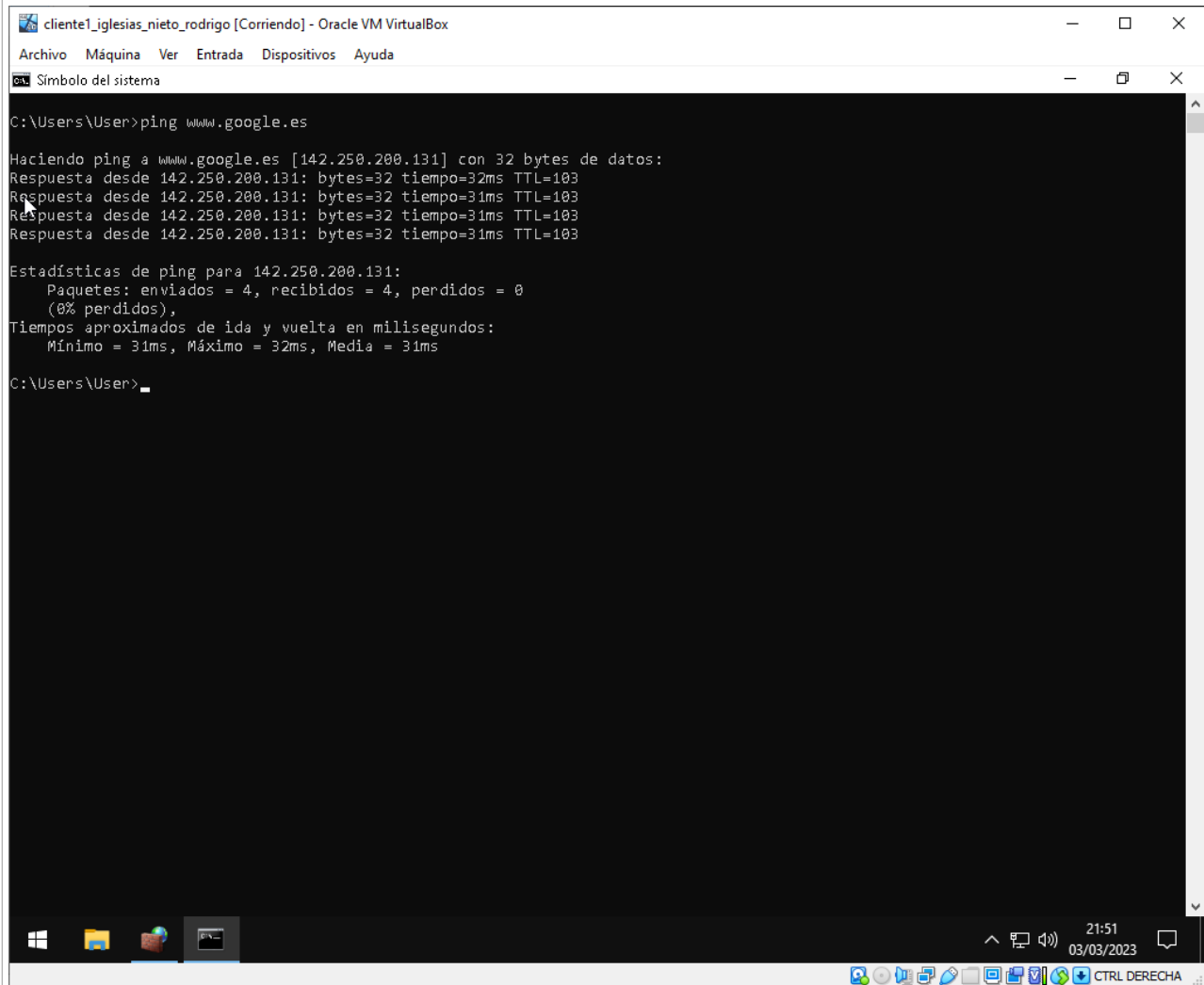
Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::ddd9:8fff:4d81:d552%5
    Dirección IPv4. . . . . : 192.168.250.101
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 192.168.250.1

C:\Users\User>
```

The taskbar at the bottom shows the Windows Start button, taskbar icons for File Explorer, Edge, and a terminal window. The system tray on the right shows the time as 21:50, the date as 03/03/2023, and a "CTRL DERECHA" button.

c) Comproba que o cliente1 é capaz de navegar por Internet [Captura de pantalla]



The screenshot shows a Windows 10 desktop environment. At the top, a window titled 'cliente1_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox' is open. Below it, a 'Símbolo del sistema' (Command Prompt) window is active. The command prompt shows the user typing 'ping www.google.es'. The output displays four successful ping responses from the IP address 142.250.200.131, each with 32 bytes, a time of 31ms, and a TTL of 103. Below the individual responses, it shows the ping statistics: 4 packets sent, 4 received, 0 lost (0% loss), and round-trip times of 31ms (minimum), 32ms (maximum), and 31ms (average). The command prompt is running in the 'C:\Users\User>' directory. The Windows taskbar at the bottom shows the Start button, several application icons, and the system tray with the date and time (21:51, 03/03/2023).

```
C:\Users\User>ping www.google.es

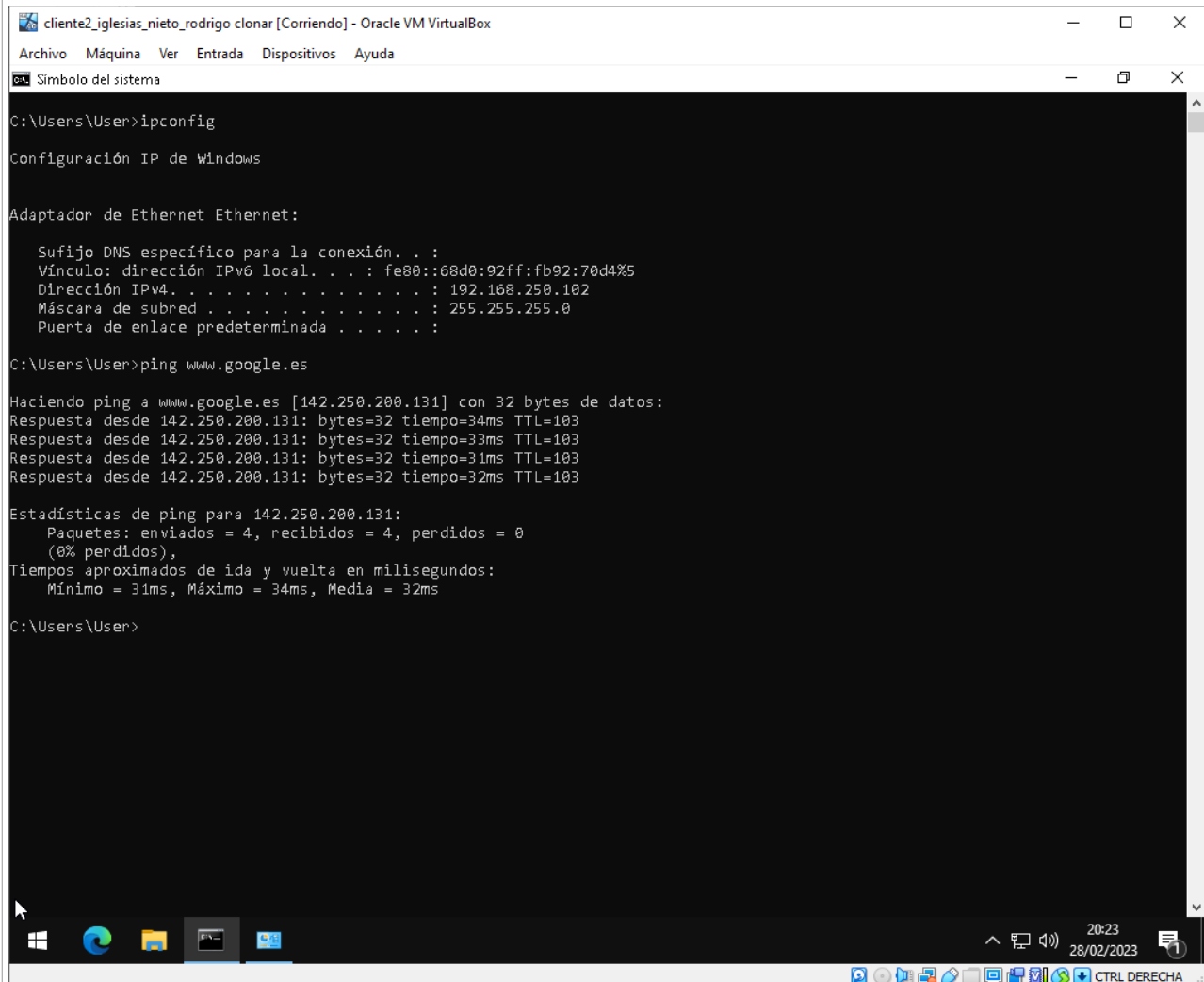
Haciendo ping a www.google.es [142.250.200.131] con 32 bytes de datos:
Respuesta desde 142.250.200.131: bytes=32 tiempo=31ms TTL=103
Respuesta desde 142.250.200.131: bytes=32 tiempo=31ms TTL=103
Respuesta desde 142.250.200.131: bytes=32 tiempo=31ms TTL=103
Respuesta desde 142.250.200.131: bytes=32 tiempo=31ms TTL=103

Estadísticas de ping para 142.250.200.131:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 31ms, Máximo = 32ms, Media = 31ms

C:\Users\User>
```

d) Configura a rede de cliente2 para que a porta de enlace sexa a IP 192.168.250.1 correspondente ao servidor [Captura de pantalla]

e) Comproba que o cliente2 é capaz de navegar por Internet [Captura de pantalla]



```
cliente2_iglesias_nieto_rodrigo clonar [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Simbolo del sistema

C:\Users\User>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::68d0:92ff:fb92:70d4%5
    Dirección IPv4. . . . . : 192.168.250.102
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . :

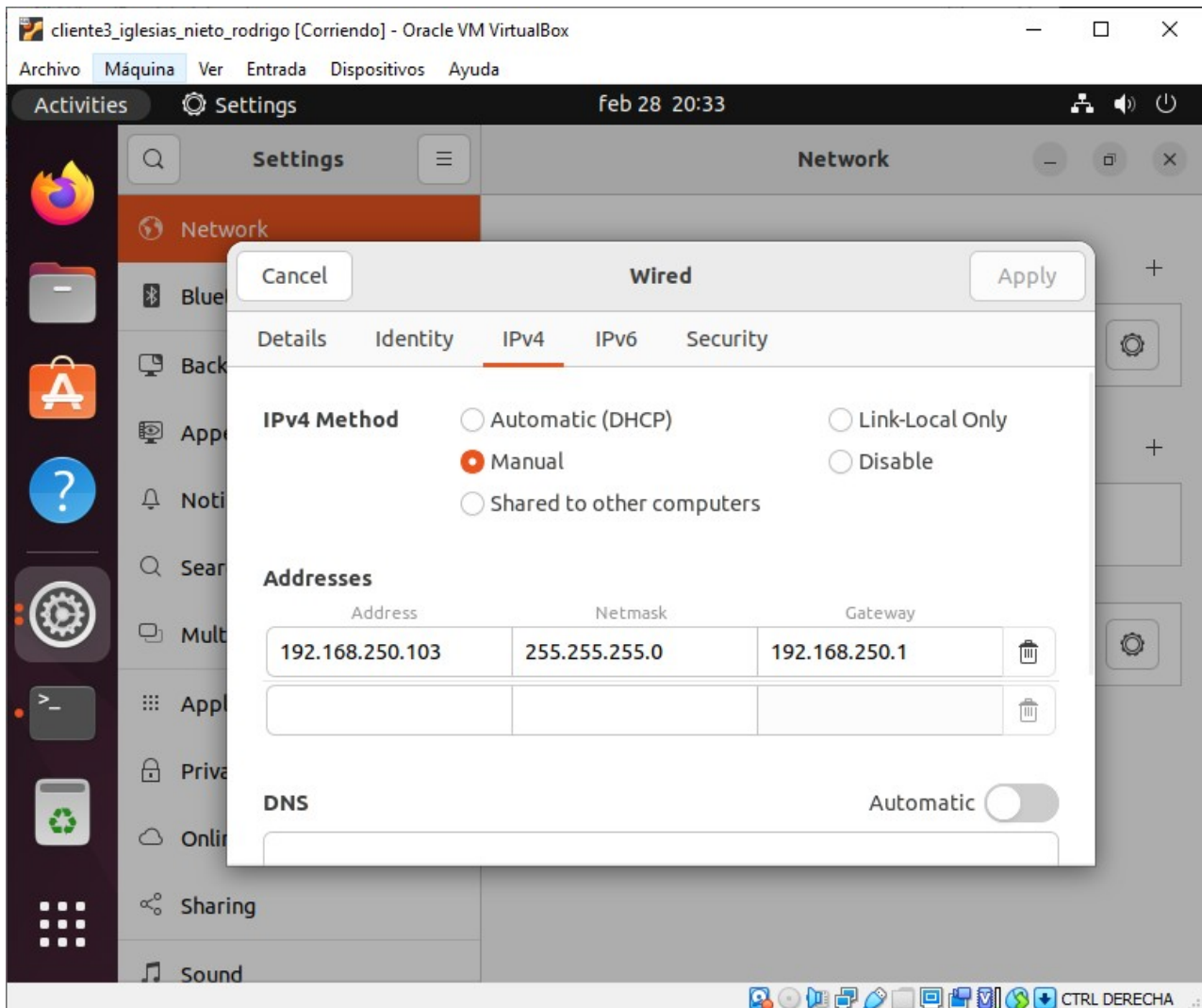
C:\Users\User>ping www.google.es

Haciendo ping a www.google.es [142.250.200.131] con 32 bytes de datos:
Respuesta desde 142.250.200.131: bytes=32 tiempo=34ms TTL=103
Respuesta desde 142.250.200.131: bytes=32 tiempo=33ms TTL=103
Respuesta desde 142.250.200.131: bytes=32 tiempo=31ms TTL=103
Respuesta desde 142.250.200.131: bytes=32 tiempo=32ms TTL=103

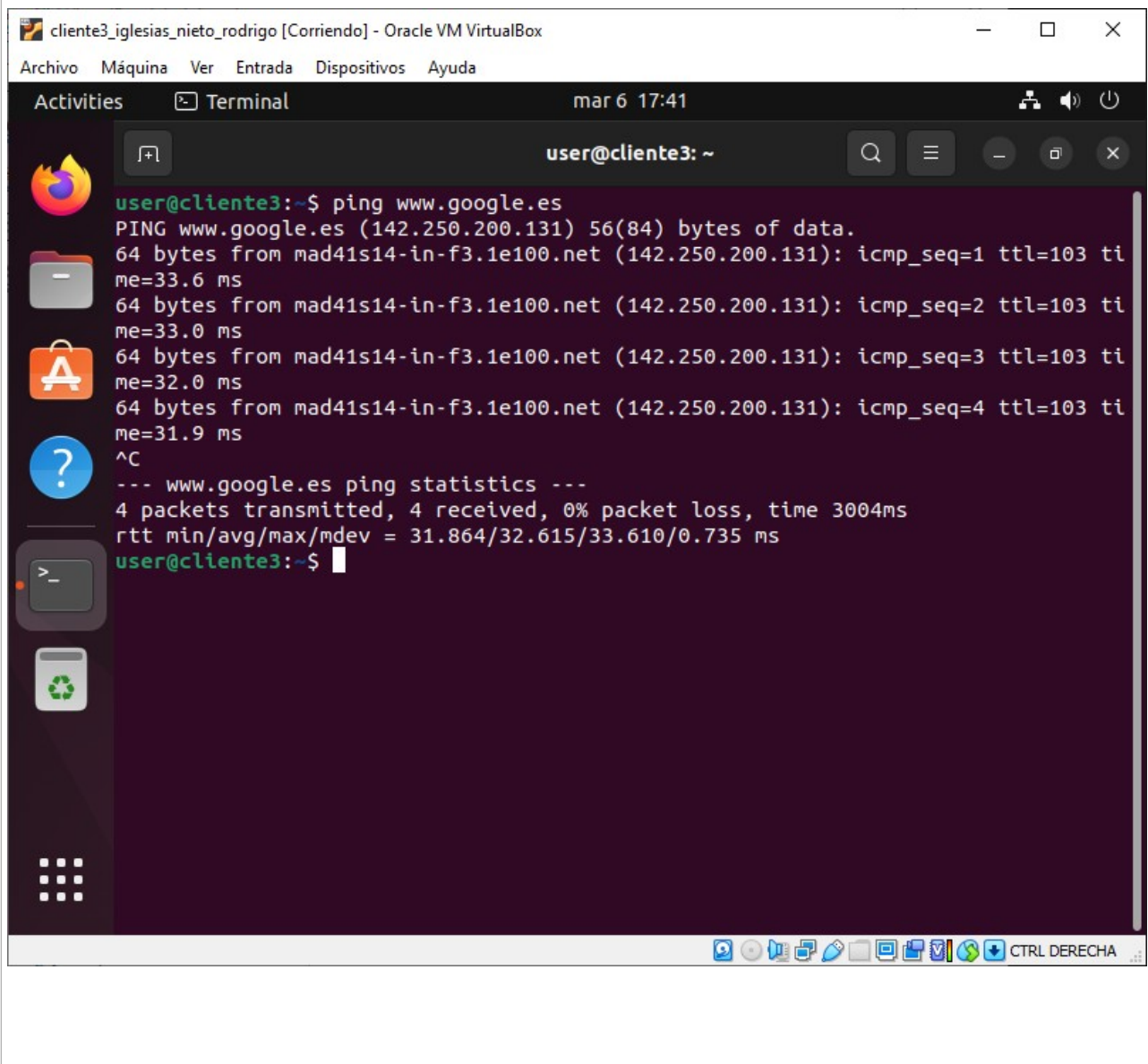
Estadísticas de ping para 142.250.200.131:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 31ms, Máximo = 34ms, Media = 32ms

C:\Users\User>
```

f) Configura a rede de cliente3 para que a porta de enlace sexa a IP 192.168.250.1 correspondente ao servidor [Captura de pantalla]



g) Comproba que o cliente3 é capaz de navegar por Internet [Captura de pantalla]



The screenshot shows a terminal window titled 'cliente3_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox'. The terminal output shows a successful ping to www.google.es (142.250.200.131) with 4 packets transmitted, 4 received, 0% packet loss, and a time of 3004ms. The ping statistics show an rtt min/avg/max/mdev of 31.864/32.615/33.610/0.735 ms.

```
user@cliente3:~$ ping www.google.es
PING www.google.es (142.250.200.131) 56(84) bytes of data.
64 bytes from mad41s14-in-f3.1e100.net (142.250.200.131): icmp_seq=1 ttl=103 ti
me=33.6 ms
64 bytes from mad41s14-in-f3.1e100.net (142.250.200.131): icmp_seq=2 ttl=103 ti
me=33.0 ms
64 bytes from mad41s14-in-f3.1e100.net (142.250.200.131): icmp_seq=3 ttl=103 ti
me=32.0 ms
64 bytes from mad41s14-in-f3.1e100.net (142.250.200.131): icmp_seq=4 ttl=103 ti
me=31.9 ms
^C
--- www.google.es ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 31.864/32.615/33.610/0.735 ms
user@cliente3:~$
```

CA5.10 Verifícase o funcionamento da rede mediante o uso de comandos e ferramentas básicas. (10%)



4. Realiza as seguintes tarefas de comprobación de funcionamento da rede.

- Dende cliente3 descobre os portos abertos na máquina cliente3 [Captura de pantalla]
- Dende cliente3 comproba se o servidor web proporcionado por server é accesible [Captura de pantalla]

- d) Detecta desde cliente3 todas as máquinas activas na rede interna local (192.168.250.0/24) mediante nmap [Captura de pantalla]
- e) Desde cliente3 trata de descubrir mediante nmap os portos abertos en Server [Captura de pantalla]
- f) Desde cliente3 e mediante nmap trata descubrir o sistema operativo que está instalado en server [Captura de pantalla]

Resposta

- a) Desde cliente3 descubre os portos abertos na máquina cliente3 [Captura de pantalla]

cliente3_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Activities Terminal mar 6 18:32

user@cliente3: ~

```
user@cliente3:~$ ss -tlnp
```

State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
LISTEN	0	4096	127.0.0.53%lo:53	0.0.0.0:*	
LISTEN	0	128	127.0.0.1:631	0.0.0.0:*	
LISTEN	0	128	:::1:631	:::1:*	

user@cliente3:~\$ S

cliente3_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Activities Terminal mar 6 18:34

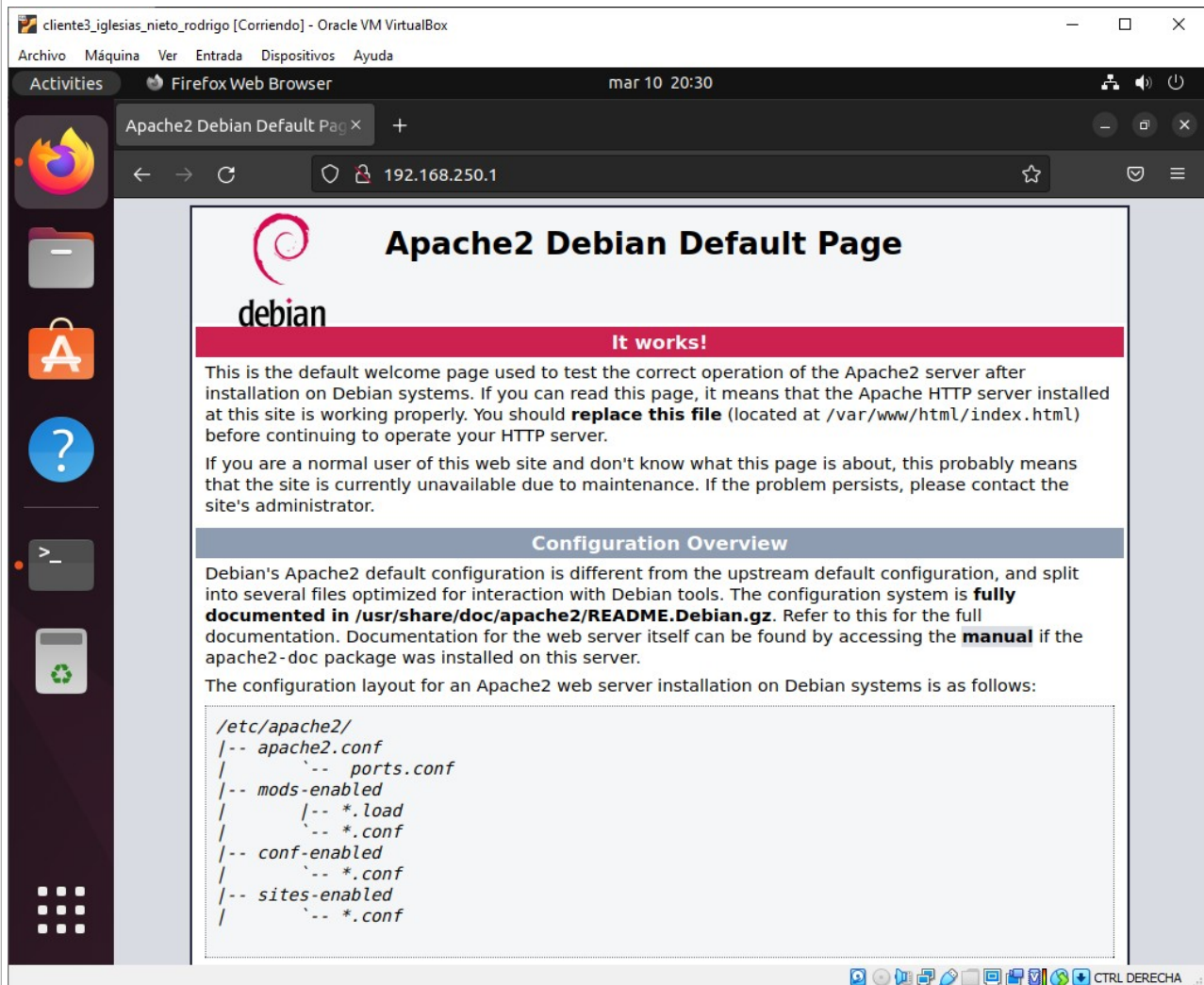
user@cliente3: ~

```
user@cliente3:~$ ss -ulnp
```

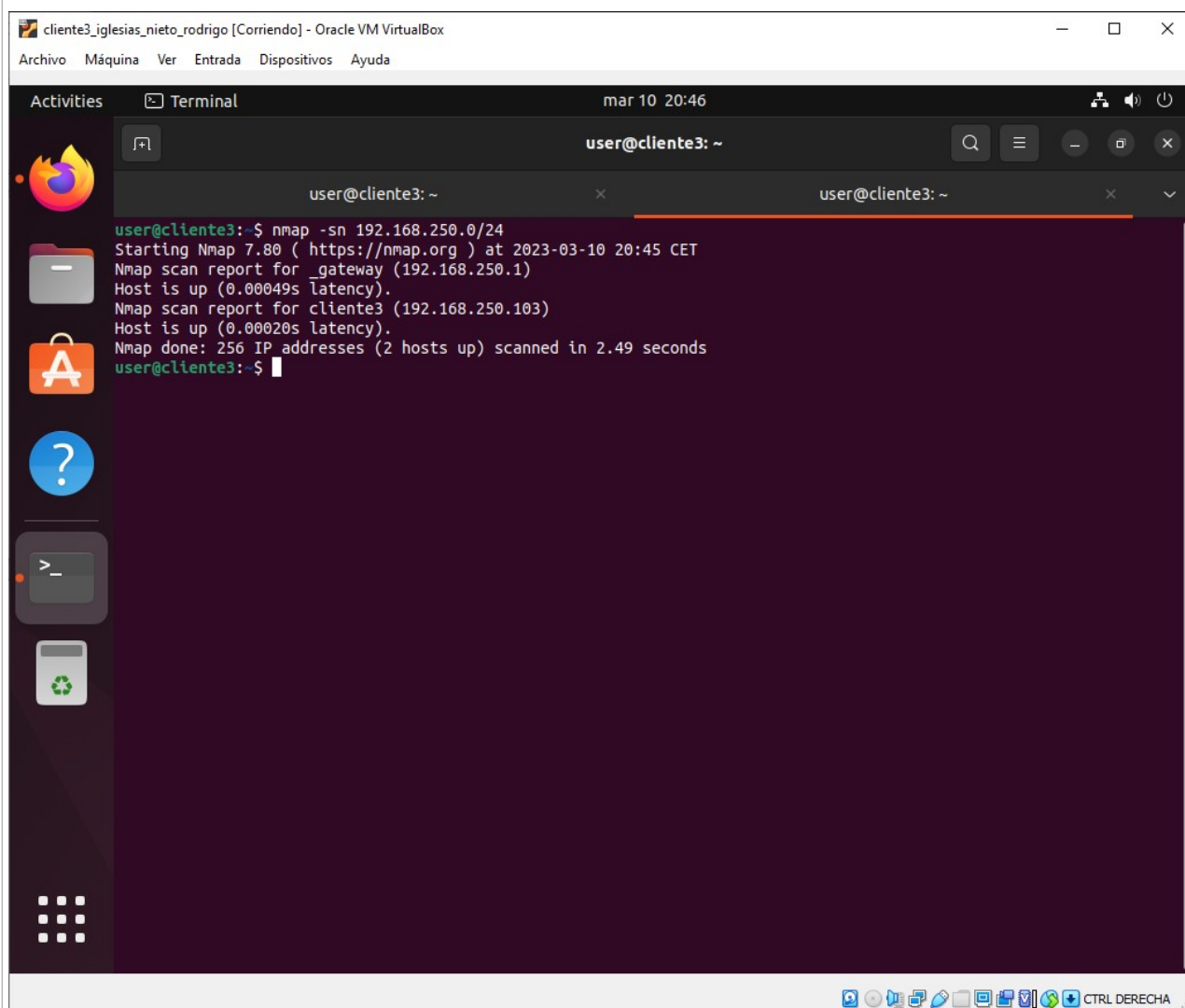
State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
UNCONN	0	0	0.0.0.0:5353	0.0.0.0:*	
UNCONN	0	0	0.0.0.0:631	0.0.0.0:*	
UNCONN	0	0	0.0.0.0:44677	0.0.0.0:*	
UNCONN	0	0	127.0.0.53%lo:53	0.0.0.0:*	
UNCONN	0	0	:::5353	:::1:*	
UNCONN	0	0	:::34931	:::1:*	

user@cliente3:~\$

b) Dende cliente3 comproba se o servidor web proporcionado por server é accesible
[Captura de pantalla]



d) Detecta desde cliente3 todas as máquinas activas na rede interna local (192.168.250.0/24) mediante nmap [Captura de pantalla]



```
cliente3_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

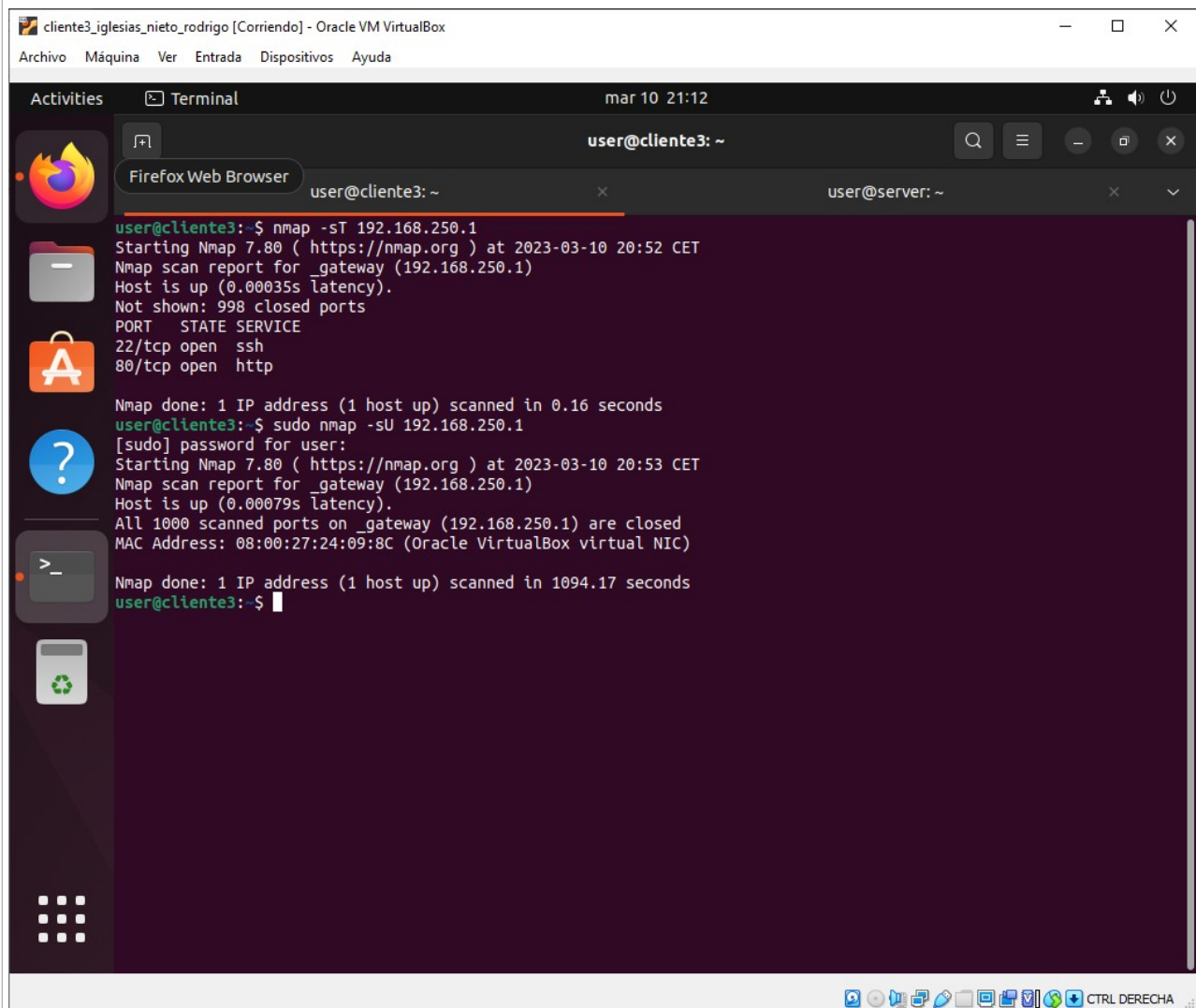
Activities  Terminal  mar 10 20:46

user@cliente3: ~

user@cliente3: ~
user@cliente3: ~

user@cliente3:~$ nmap -sn 192.168.250.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 20:45 CET
Nmap scan report for _gateway (192.168.250.1)
Host is up (0.00049s latency).
Nmap scan report for cliente3 (192.168.250.103)
Host is up (0.00020s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.49 seconds
user@cliente3:~$
```

e) Dende cliente3 trata de descubrir mediante nmap os portos abertos en Server
[Captura de pantalla]

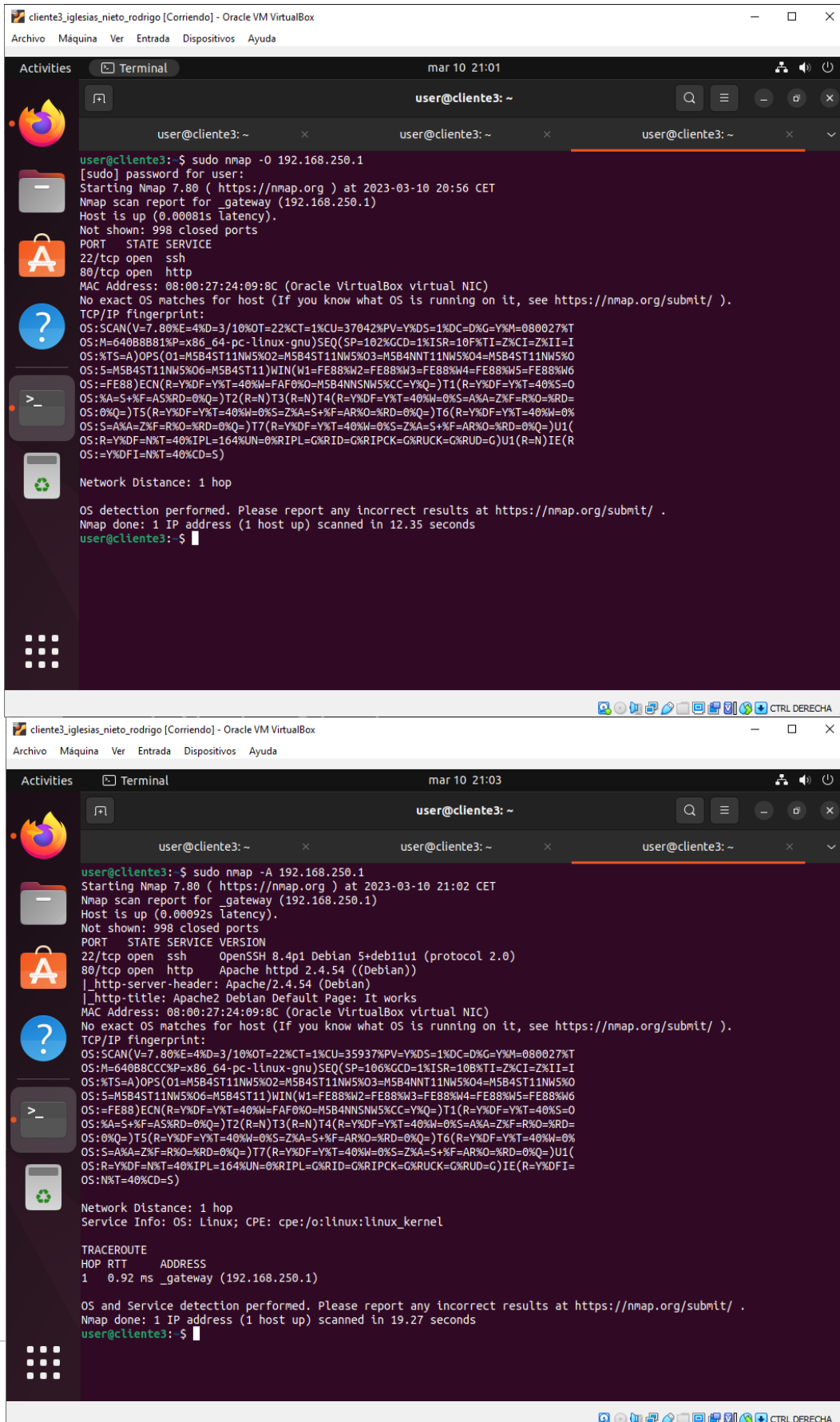


The screenshot shows a terminal window titled "cliente3_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox". The terminal is running a series of nmap scans from a host named "cliente3" to a target IP "192.168.250.1".

```
user@cliente3: ~  
user@cliente3: $ nmap -sT 192.168.250.1  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 20:52 CET  
Nmap scan report for _gateway (192.168.250.1)  
Host is up (0.00035s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds  
user@cliente3: $ sudo nmap -sU 192.168.250.1  
[sudo] password for user:  
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 20:53 CET  
Nmap scan report for _gateway (192.168.250.1)  
Host is up (0.00079s latency).  
All 1000 scanned ports on _gateway (192.168.250.1) are closed  
MAC Address: 08:00:27:24:09:8C (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 1094.17 seconds  
user@cliente3: $
```

The terminal window is part of a desktop environment with a sidebar on the left containing icons for Firefox, a file manager, an application store, a help icon, and a terminal. The top of the window shows the date and time as "mar 10 21:12". The bottom of the window has a taskbar with various system icons and a "CTRL DERECHA" button.

f) Desde cliente3 e mediante nmap trata descubrir o sistema operativo que está instalado en server [Captura de pantalla]



```
cliente3_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

Activities Terminal mar 10 21:01

user@cliente3: ~

user@cliente3:~
user@cliente3:~
user@cliente3:~

user@cliente3:~$ sudo nmap -O 192.168.250.1
[sudo] password for user:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 20:56 CET
Nmap scan report for _gateway (192.168.250.1)
Host is up (0.00081s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:24:09:8C (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=3/10%OT=22%CT=1%CU=37042%PV=Y%D5=1%DC=D%G=Y%M=080027%T
OS:M=640B8B81P=x86_64-pc-linux-gnu)SEQ(SP=102%CCD=1%ISR=10F%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW5%O2=M5B4ST11NW5%O3=M5B4NNT11NW5%O4=M5B4ST11NW5%O
OS:5=M5B4ST11NW5%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW5%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)U1(R=N)IE(R
OS:Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.35 seconds
user@cliente3:~$
```

```
cliente3_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

Activities Terminal mar 10 21:03

user@cliente3: ~

user@cliente3:~
user@cliente3:~
user@cliente3:~

user@cliente3:~$ sudo nmap -A 192.168.250.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-10 21:02 CET
Nmap scan report for _gateway (192.168.250.1)
Host is up (0.00092s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.54 ((Debian))
|_http-server-header: Apache/2.4.54 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 08:00:27:24:09:8C (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=3/10%OT=22%CT=1%CU=35937%PV=Y%D5=1%DC=D%G=Y%M=080027%T
OS:M=640B8CCC%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10B%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW5%O2=M5B4ST11NW5%O3=M5B4NNT11NW5%O4=M5B4ST11NW5%O
OS:5=M5B4ST11NW5%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW5%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.92 ms _gateway (192.168.250.1)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.27 seconds
user@cliente3:~$
```

CA5.11 Aplicáronse protocolos seguros de comunicacións. (5%)



5. Instalación remota.

- Realiza unha conexión ssh á maquina server [Captura de pantalla]
- Instala suricata na máquina server por medio de ssh [Captura de pantalla]
- Configura suricata para detectar tráfico de aplicacións peer-to-peer [Captura de pantalla]
- Instala un cliente de Bittorrent na máquina cliente3 [Captura de pantalla]
- Comproba en server que se detecta o tráfico de Bittorrent procedente de cliente3 [Captura de pantalla]

Resposta

a) Realiza unha conexión ssh á maquina server [Captura de pantalla]

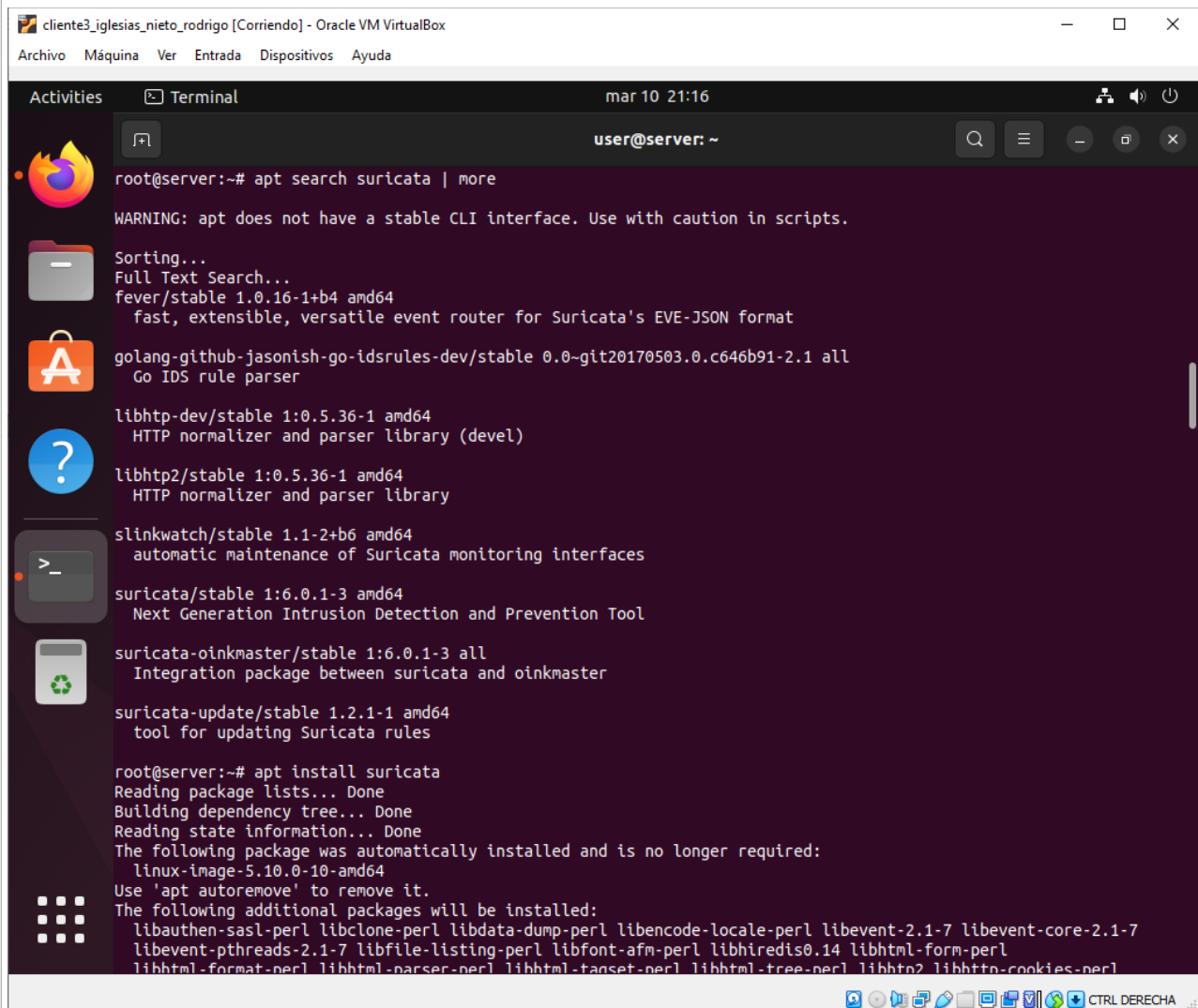
The screenshot shows a terminal window titled 'cliente3_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox'. The terminal displays the following text:

```
user@cliente3:~$ ssh user@192.168.250.1
user@192.168.250.1's password:
Linux server 5.10.0-12-amd64 #1 SMP Debian 5.10.103-1 (2022-03-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Mar 10 21:11:42 2023 from 192.168.250.103
user@server:~$
```


b) Instala Suricata na máquina server por medio de ssh [Captura de pantalla]



```
cliente3_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

Activities Terminal mar 10 21:16 user@server: ~

root@server:~# apt search suricata | more
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Sorting...
Full Text Search...
fever/stable 1.0.16-1+b4 amd64
  fast, extensible, versatile event router for Suricata's EVE-JSON format

golang-github-jasonish-go-idsrules-dev/stable 0.0~git20170503.0.c646b91-2.1 all
  Go IDS rule parser

libhttp-dev/stable 1:0.5.36-1 amd64
  HTTP normalizer and parser library (devel)

libhttp2/stable 1:0.5.36-1 amd64
  HTTP normalizer and parser library

slinkwatch/stable 1.1-2+b6 amd64
  automatic maintenance of Suricata monitoring interfaces

suricata/stable 1:6.0.1-3 amd64
  Next Generation Intrusion Detection and Prevention Tool

suricata-oinkmaster/stable 1:6.0.1-3 all
  Integration package between suricata and oinkmaster

suricata-update/stable 1.2.1-1 amd64
  tool for updating Suricata rules

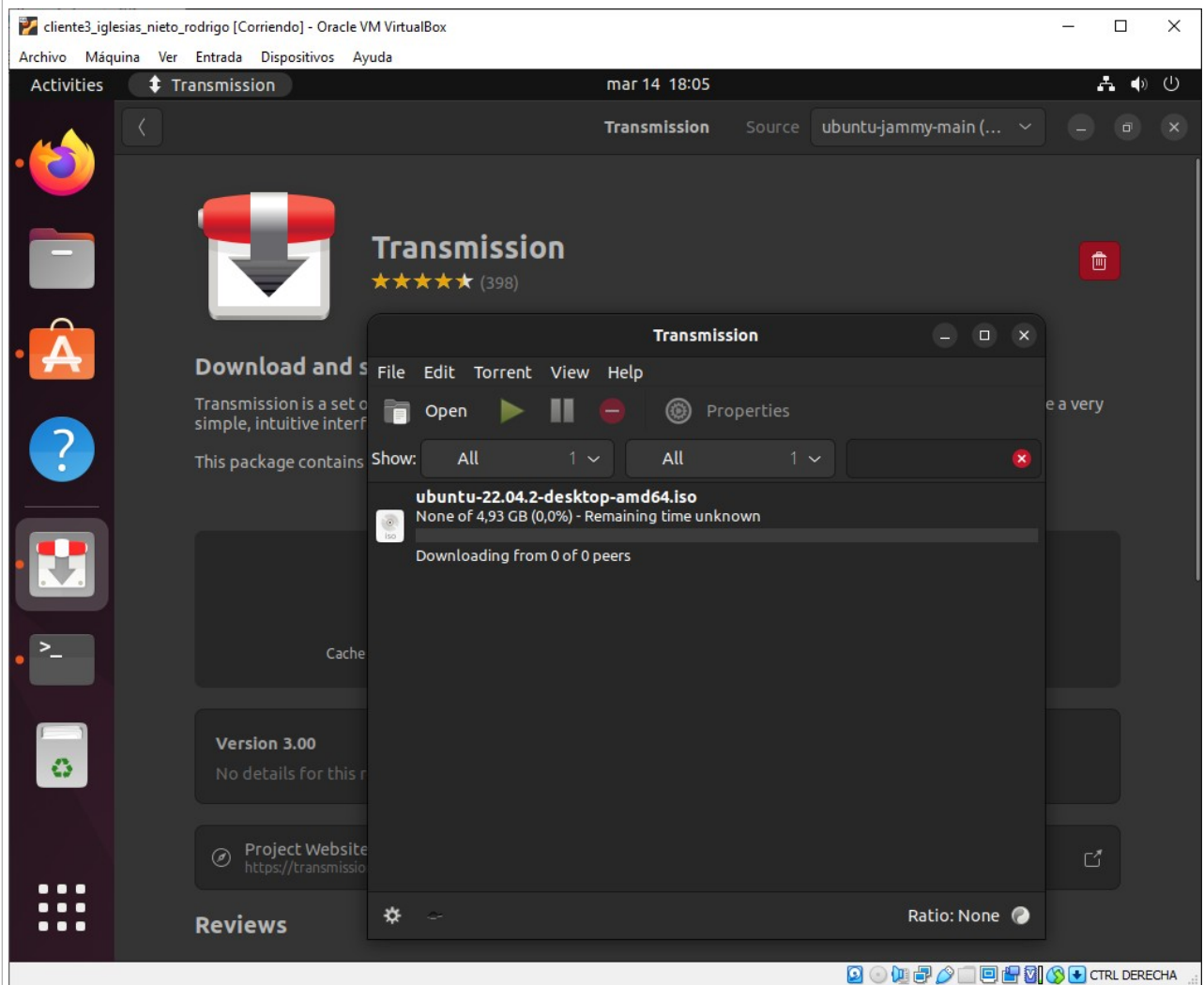
root@server:~# apt install suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  linux-image-5.10.0-10-amd64
Use 'apt autoremove' to remove it.
The following additional packages will be installed:
  libauthen-sasl-perl libclone-perl libdata-dump-perl libencode-locale-perl libevent-2.1-7 libevent-core-2.1-7
  libevent-pthreads-2.1-7 libfile-listing-perl libfont-afm-perl libhiredis0.14 libhtml-form-perl
  libhtml-format-perl libhtml-parser-perl libhtml-tagset-perl libhtml-tree-perl libhttp2 libhttp-cookie-perl
```

c) Configura Suricata para detectar tráfico de aplicaciones peer-to-peer [Captura de pantalla]

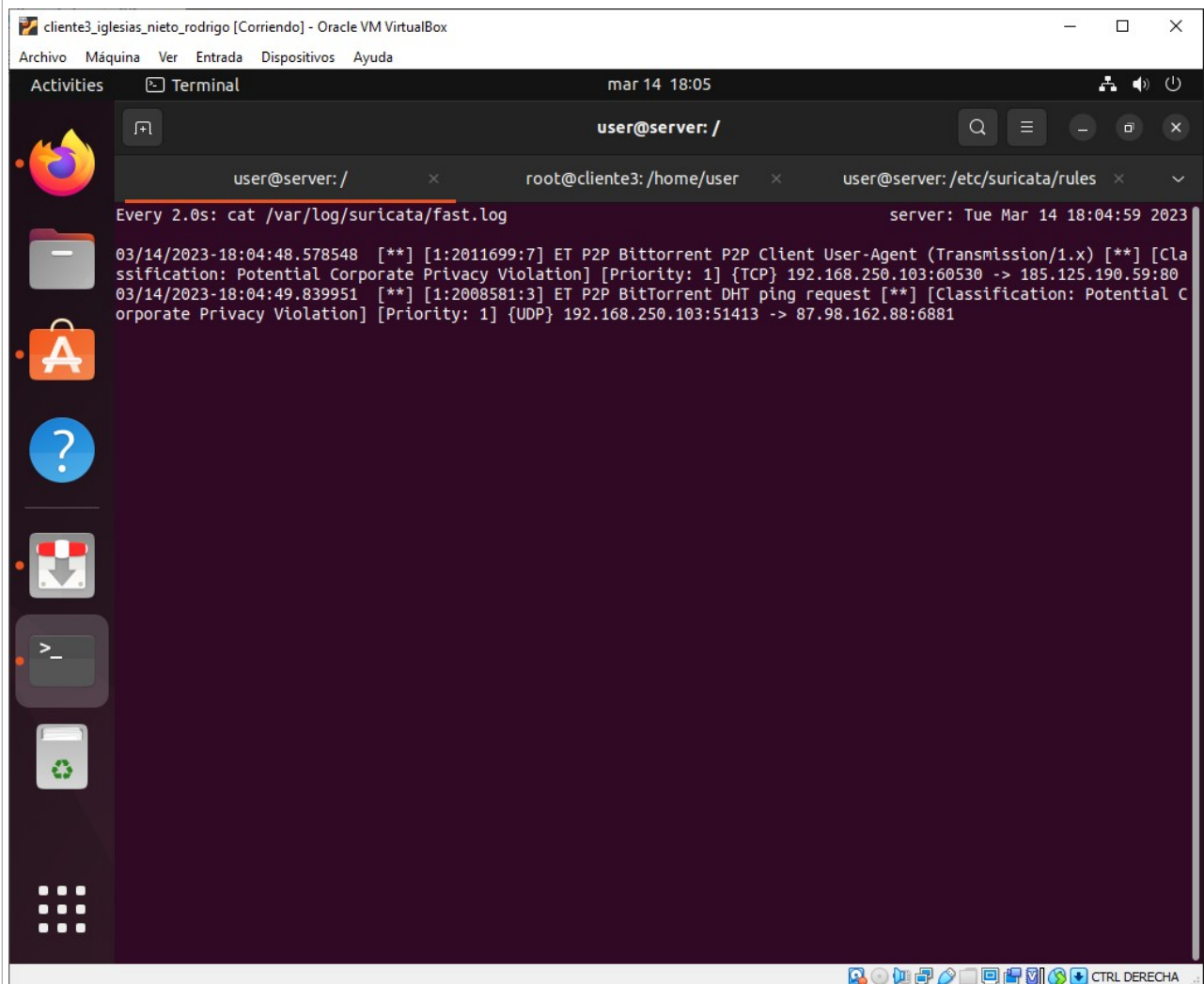
```
cliente3_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Activities Terminal mar 14 17:37
user@server: ~
user@server: ~
user@cliente3: ~
user@server: ~
14/3/2023 -- 17:34:50 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-6.0.1/emerging.rules.tar
14/3/2023 -- 17:34:53 - <Info> -- Done.
14/3/2023 -- 17:34:54 - <Info> -- Fetching https://openinfosecfoundation.org/rules/trafficid/trafficid.rules.
14/3/2023 -- 17:34:54 - <Info> -- Done.
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.rules
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-events.rules
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/dhcp-events.rules
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events.rules
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.rules
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/http-events.rules
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/ipsec-events.rules
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/kerberos-events.rules
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rules
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/nfs-events.rules
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.rules
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/smb-events.rules
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/sntp-events.rules
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/stream-events.rules
14/3/2023 -- 17:34:54 - <Info> -- Loading distribution rule file /etc/suricata/rules/tls-events.rules
14/3/2023 -- 17:34:54 - <Info> -- Ignoring file rules/emerging-deleted.rules
14/3/2023 -- 17:34:58 - <Info> -- Loaded 41301 rules.
14/3/2023 -- 17:34:58 - <Info> -- Disabled 14 rules.
14/3/2023 -- 17:34:58 - <Info> -- Enabled 0 rules.
14/3/2023 -- 17:34:58 - <Info> -- Modified 0 rules.
14/3/2023 -- 17:34:58 - <Info> -- Dropped 0 rules.
14/3/2023 -- 17:34:58 - <Info> -- Enabled 131 rules for flowbit dependencies.
14/3/2023 -- 17:34:58 - <Info> -- Backing up current rules.
14/3/2023 -- 17:35:03 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 41301; enabled: 3
3351; added: 27; removed 0; modified: 1343
14/3/2023 -- 17:35:03 - <Info> -- Writing /var/lib/suricata/rules/classification.config
14/3/2023 -- 17:35:03 - <Info> -- Testing with suricata -T.
14/3/2023 -- 17:35:46 - <Info> -- Done.
root@server:~#
```

```
cliente3_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Activities Terminal mar 14 18:01
Firefox Web Browser
user@server: /etc/suricata
root@cliente3: /home/user
user@server: /etc/suricata/rules
13/3/2023 -- 18:19:54 - <Info> -- time elapsed 246589.047s
13/3/2023 -- 18:20:00 - <Info> -- Alerts: 0
14/3/2023 -- 17:33:16 - <Notice> -- This is Suricata version 6.0.1 RELEASE running in SYSTEM mode
14/3/2023 -- 17:33:16 - <Info> -- CPUs/cores online: 2
14/3/2023 -- 17:33:16 - <Info> -- Found an MTU of 1500 for 'enp0s8'
14/3/2023 -- 17:33:16 - <Info> -- Found an MTU of 1500 for 'enp0s8'
14/3/2023 -- 17:33:16 - <Info> -- fast output device (regular) initialized: fast.log
14/3/2023 -- 17:33:16 - <Info> -- eve-log output device (regular) initialized: eve.json
14/3/2023 -- 17:33:16 - <Info> -- stats output device (regular) initialized: stats.log
14/3/2023 -- 17:33:16 - <Warning> -- [ERRCODE: SC_ERR_NO_RULES(42)] - No rule files match the pattern /etc/suricata/
rules/suricata.rules
14/3/2023 -- 17:33:16 - <Warning> -- [ERRCODE: SC_ERR_NO_RULES_LOADED(43)] - 1 rule files specified, but no rules we
re loaded!
14/3/2023 -- 17:33:16 - <Info> -- Threshold config parsed: 0 rule(s) found
14/3/2023 -- 17:33:16 - <Info> -- 0 signatures processed, 0 are IP-only rules, 0 are inspecting packet payload, 0 in
spect application layer, 0 are decoder event only
14/3/2023 -- 17:33:16 - <Info> -- Going to use 2 thread(s)
14/3/2023 -- 17:33:16 - <Info> -- Using unix socket file '/var/run/suricata-command.socket'
14/3/2023 -- 17:33:16 - <Notice> -- all 2 packet processing threads, 4 management threads initialized, engine starte
d.
14/3/2023 -- 17:33:16 - <Info> -- All AFP capture threads are running.
14/3/2023 -- 18:00:17 - <Notice> -- Signal Received. Stopping engine.
14/3/2023 -- 18:00:17 - <Info> -- time elapsed 1620.383s
14/3/2023 -- 18:00:17 - <Info> -- Alerts: 0
14/3/2023 -- 18:00:17 - <Info> -- cleaning up signature grouping structure... complete
14/3/2023 -- 18:00:17 - <Notice> -- Stats for 'enp0s8': pkts: 155800, drop: 0 (0.00%), invalid checksum: 0
14/3/2023 -- 18:00:17 - <Notice> -- This is Suricata version 6.0.1 RELEASE running in SYSTEM mode
14/3/2023 -- 18:00:17 - <Info> -- CPUs/cores online: 2
14/3/2023 -- 18:00:17 - <Info> -- Found an MTU of 1500 for 'enp0s8'
14/3/2023 -- 18:00:17 - <Info> -- Found an MTU of 1500 for 'enp0s8'
14/3/2023 -- 18:00:17 - <Info> -- fast output device (regular) initialized: fast.log
14/3/2023 -- 18:00:17 - <Info> -- eve-log output device (regular) initialized: eve.json
14/3/2023 -- 18:00:17 - <Info> -- stats output device (regular) initialized: stats.log
14/3/2023 -- 18:00:28 - <Info> -- 1 rule files processed, 33351 rules successfully loaded, 0 rules failed
14/3/2023 -- 18:00:28 - <Info> -- Threshold config parsed: 0 rule(s) found
14/3/2023 -- 18:00:29 - <Info> -- 33354 signatures processed, 1211 are IP-only rules, 5205 are inspecting packet pay
load, 26740 inspect application layer, 184 are decoder event only
root@server:/var/log/suricata#
```


d) Instala un cliente de Bittorrent (Transmission) na máquina cliente3 [Captura de pantalla]



e) Comprueba en server que se detecta o tráfico de Bittorrent procedente de cliente3 [Captura de pantalla]



cliente3_iglesias_nieto_rodrigo [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Activities Terminal mar 14 18:05

user@server: /

user@server: / x root@cliente3: /home/user x user@server: /etc/suricata/rules x

Every 2.0s: cat /var/log/suricata/fast.log server: Tue Mar 14 18:04:59 2023

```
03/14/2023-18:04:48.578548  [**] [1:2011699:7] ET P2P Bittorrent P2P Client User-Agent (Transmission/1.x) [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 192.168.250.103:60530 -> 185.125.190.59:80
03/14/2023-18:04:49.839951  [**] [1:2008581:3] ET P2P BitTorrent DHT ping request [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {UDP} 192.168.250.103:51413 -> 87.98.162.88:6881
```