

Práctica NAT

Sumario

Esquema de la red.....	2
Activa el NAT en la máquina A.....	2
Conéctate a B por medio de escritorio remoto, desde tu PC físico.....	4
Conéctate a B desde el equipo B de otro compañero.....	6
Convierte a B en un servidor de ficheros (carpetas compartidas).....	8
Haz que A y C puedan ser administrados mediante SSH desde la red del aula.....	13
Comprueba el NAT con tcpdump.....	14

Esquema de la red

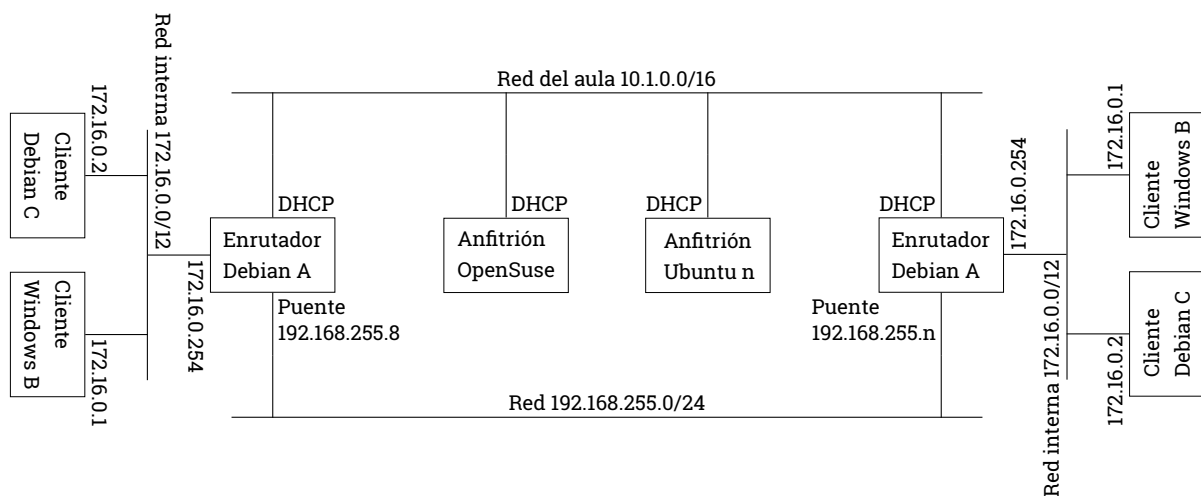


Figura 1: Diagrama de conexiones de red, nosotros somos el anfitrión OpenSuse

Activa el NAT en la máquina A

Todos los comandos que vayamos ejecutando los vamos a ir guardando en un *script* para que se vayan guardando al reiniciar y que así se efectúen también todos los anteriores, ya que son necesarios.

Primero, activamos el enrutamiento en el enrutador Debian con el siguiente comando:

```
root@enrutador-debian:/home/alumno # sysctl net.ipv4.ip_forward=1
```

Después, vaciamos nuestra tabla NAT –y la vaciaremos al realizar cada prueba–:

```
root@enrutador-debian:/home/alumno # iptables -t nat -F
```

Añadimos las entradas NAT para los dos adaptadores puente –el eth0, que está en la red 10.1.0.0/16 y el eth1, en la 192.168.255.0/24–:

```
root@enrutador-debian:/home/alumno # iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
root@enrutador-debian:/home/alumno # iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

Finalmente, comprobamos que tanto el cliente Debian como el cliente Windows tienen acceso a internet.

- En el cliente Debian:

```
root@cliente-debian:/home/alumno # mtr 8.8.8.8
My traceroute [v0.85]
cliente-debian (0.0.0.0) Tue Apr 2 08:54:22 2019
Keys: Help Display mode Restart statistics Order of fields quit
          Packets
Host      Loss%  Snt   Last   Avg   Best  Wrst  StDev
1. 172.16.0.254      0.0%  14    1.0    1.1    0.9    1.4    0.0
2. 10.1.0.1          0.0%  14    1.6    4.2    1.6   32.2    8.1
3. 25.red-80-58-67.staticip.rima-td 0.0%  14    4.8    5.3    3.8    8.6    1.1
4. 25.red-80-58-121.staticip.rima-t 0.0%  14    8.7    7.0    5.4   10.5    1.4
5. 240.red-80-58-88.staticip.rima-t 7.1%  14    7.0    6.9    5.0   14.1    2.3
6. 94.red-81-46-8.customer.static.c 0.0%  14    5.1    7.4    4.8   23.3    4.7
7. ???
8. 209.85.149.88     0.0%  14    5.3    7.3    5.3   17.0    2.9
9. ???
10. 74.125.253.196    0.0%  13    6.4    6.2    5.6    6.8    0.0
11. 108.170.232.25    0.0%  13    8.6    7.9    5.8   15.7    2.4
12. google-public-dns-a.google.com 0.0%  13    5.4    5.8    4.6    6.4    0.3
```

- En el cliente Windows:

```
Seguimiento de ruta a google-public-dns-a.google.com [8.8.8.8]
sobre un máximo de 30 saltos:
0 WIN-074RNEACROF [172.16.0.1]
1 172.16.0.254
2 10.1.0.1
3 25.red-80-58-67.staticip.rima-tde.net [80.58.67.25]
4 25.red-80-58-121.staticip.rima-tde.net [80.58.121.25]
5 240.red-80-58-88.staticip.rima-tde.net [80.58.88.240]
6 94.red-81-46-8.customer.static.ccgg.telefonica.net [81.46.8.94]
7 * * *
Procesamiento de estadísticas durante 150 segundos...
Origen hasta aquí Este Nodo/Vínculo
Salto RTT Perdido/Enviado = Pct Perdido/Enviado = Pct Dirección
0 WIN-074RNEACROF [172.16.0.1]
1 0ms 0/ 100 = 0% 0/ 100 = 0% 172.16.0.254
2 1ms 0/ 100 = 0% 0/ 100 = 0% 10.1.0.1
3 --- 100/ 100 =100% 0/ 100 = 0% 25.red-80-58-
67.staticip.rima-tde.net [80.58.67.25]
4 --- 100/ 100 =100% 0/ 100 = 0% 25.red-80-58-
121.staticip.rima-tde.net [80.58.121.25]
5 --- 100/ 100 =100% 0/ 100 = 0% 240.red-80-58-
88.staticip.rima-tde.net [80.58.88.240]
```

```
6 --- 100/ 100 =100% 0/ 100 = 0% |
8.customer.static.cgg.telefonica.net [81.46.8.94]

Traza completa.
```

Conéctate a B por medio de escritorio remoto, desde tu PC físico

Abrimos el puerto que emplea RDP (*Remote Desktop Protocol*), el cual es el 3389, e insertamos como destino al cliente Windows (172.16.0.1):

```
root@enrutador-debian:/home/alumno # iptables -t nat -A PREROUTING -p tcp --dport 3389 -i eth0 -j DNAT --to 172.16.0.1:3389
```

Activamos el escritorio remoto en Windows:

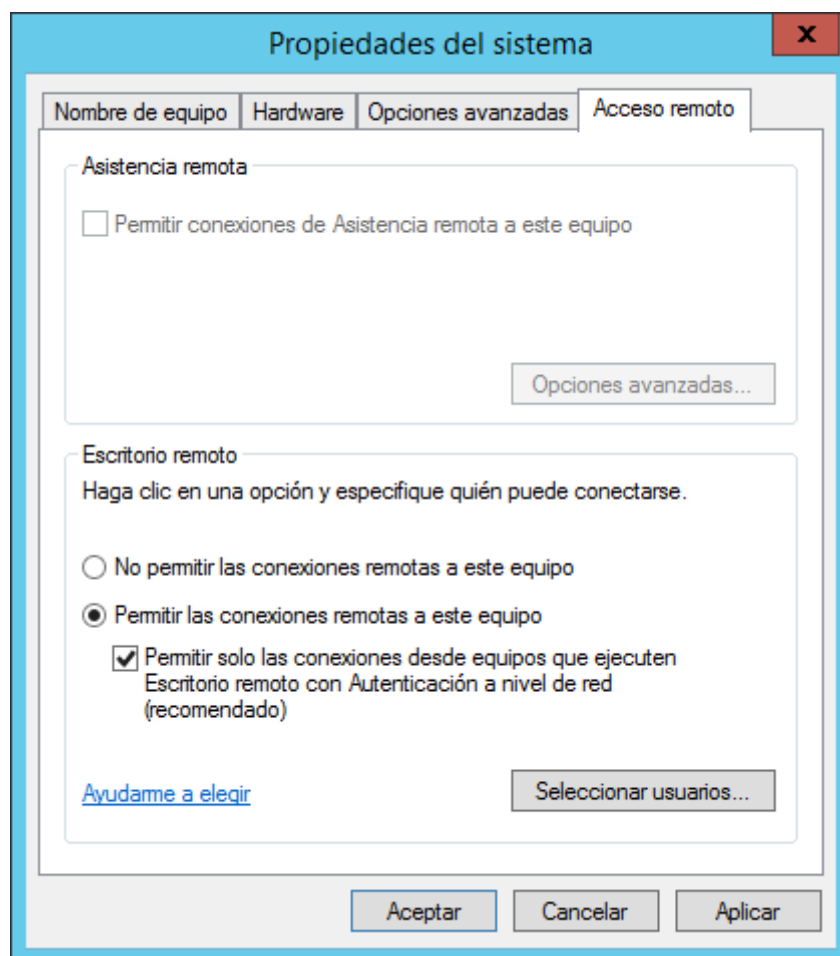


Figura 2: Se activa haciendo clic derecho en «Este equipo» → «Propiedades» → «Permitir las conexiones remotas a este equipo»

Habilitamos algún usuario para que pueda conectarse por medio de escritorio remoto:

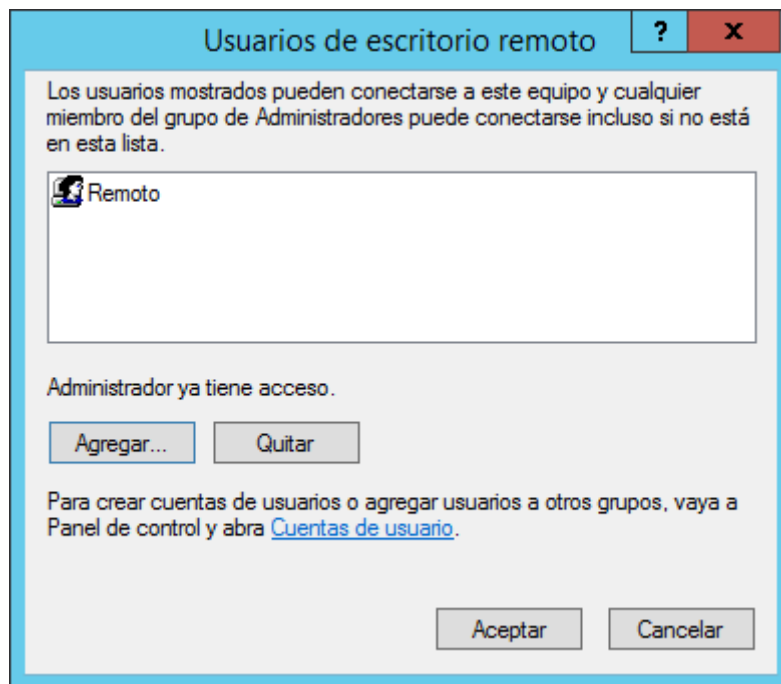


Figura 3: Usuario «Remoto» agregado correctamente. Para esto, en la figura anterior hacemos clic en «Seleccionar usuarios...» y, después, sobre «Agregar...»

Abrimos el programa Remmina y realizamos los preparativos para la conexión:

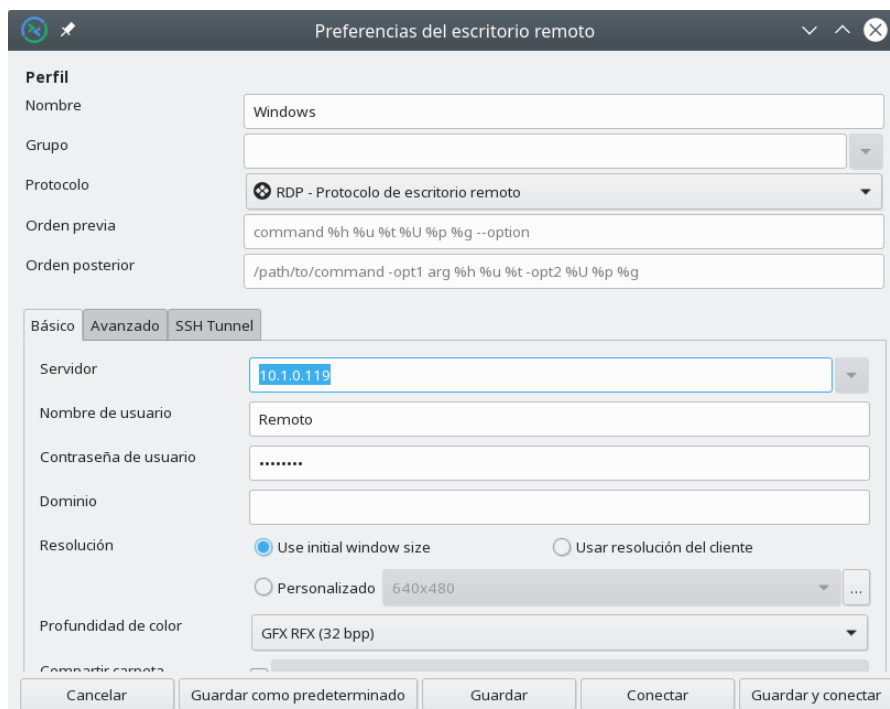


Figura 4: Configuración de la conexión en Remmina. Como nos conectamos desde la red del aula (10.1.0.0/16), hay que poner el adaptador del enrutador que se encuentra en esta, el 10.1.0.119

Seleccionamos «Conectar» y habremos accedido correctamente a nuestro cliente:

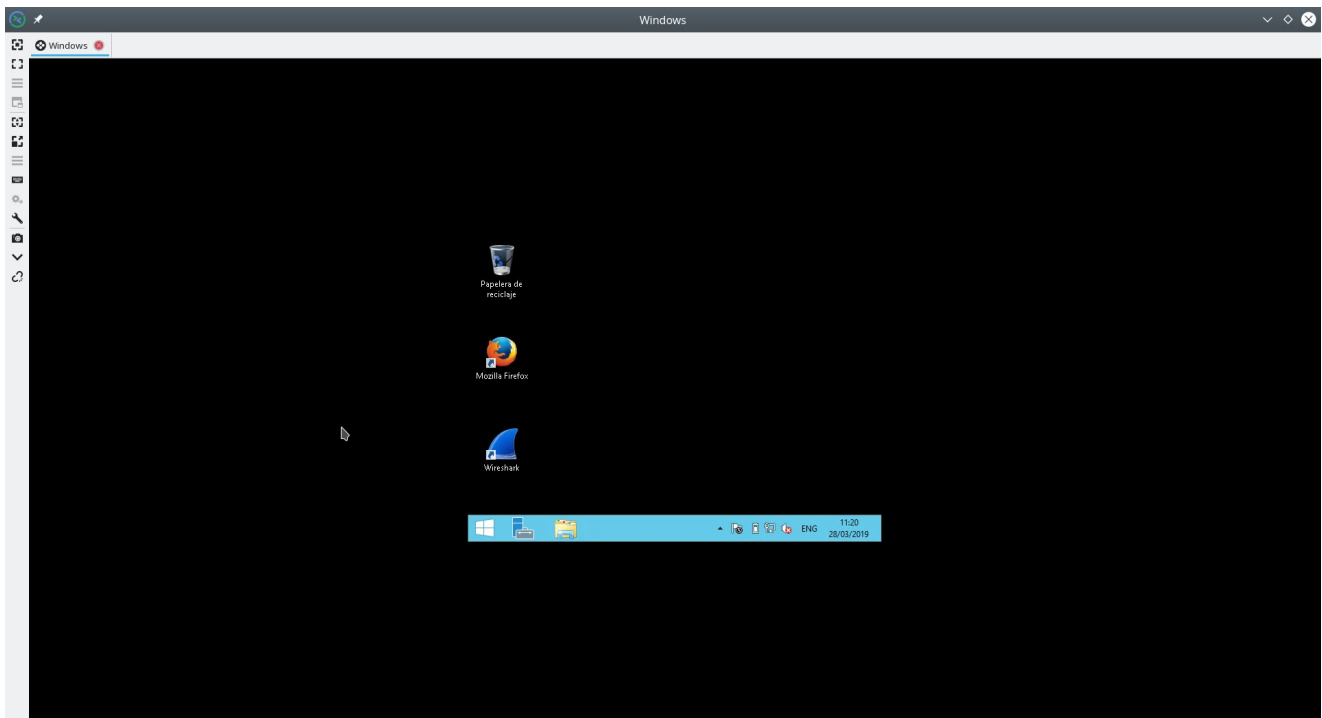


Figura 5: Conexión de escritorio remoto establecida exitosamente con nuestro cliente Windows

Conéctate a B desde el equipo B de otro compañero

Abrimos el puerto que emplea RDP en el adaptador eth1, el cual está en la red 192.168.255.0/24, y ponemos como destino a nuestro cliente Windows:

```
root@enrutador-debian:/home/alumno # iptables -t nat -A PREROUTING -p tcp --dport 3389 -i eth1 -j DNAT --to 172.16.0.1:3389
```

En el cliente Windows buscamos por «Conexión a Escritorio remoto» y escribimos la dirección del enrutador donde se encuentra el cliente Windows al que nos queremos conectar, en nuestro caso en la 192.168.255.7:

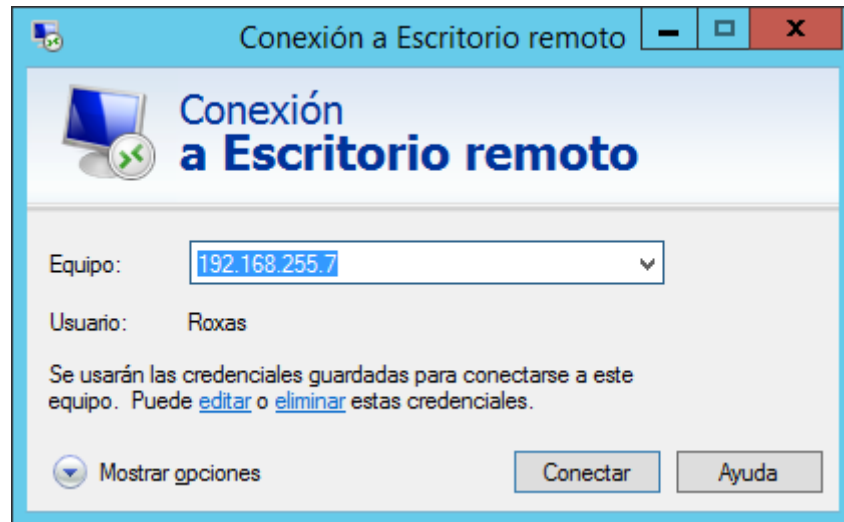


Figura 6: Estableciendo la conexión de escritorio remoto

Cuando pulsemos en «Conectar», se nos pedirá introducir el usuario y contraseña con el que queremos acceder, lo introduciremos y nos habremos conectado a él exitosamente:

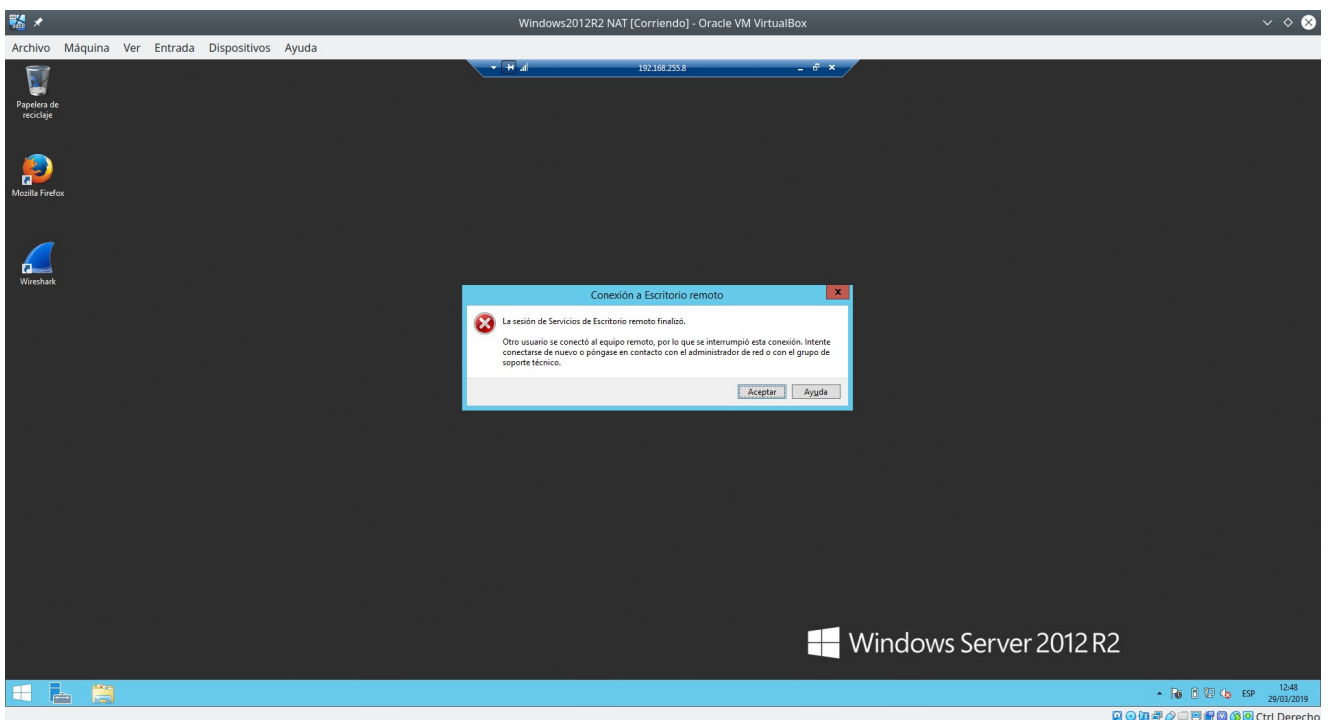


Figura 7: Conexión establecida desde nuestro cliente Windows al cliente Windows que se encuentra tras el enrutador con la dirección 192.168.255.7. Al tomar la captura, justamente dicho cliente Windows, desde otro usuario, había accedido a nuestro cliente, por lo que se finalizó la sesión de escritorio remoto

Convierte a B en un servidor de ficheros (carpetas compartidas)

Para poder convertir nuestra máquina Windows en un servidor de ficheros, lo primero que hay que hacer es abrir los puertos pertinentes, concretamente el 135, 136, 137, 138, 139, 389 y 445, tanto de TCP como de UDP, y en los dos adaptadores en puente, ya que tiene que ser posible acceder desde cualquier red externa. Nuestro destino, como anteriormente, será nuestro cliente Windows:

```
iptables -t nat -A PREROUTING -p tcp --dport 135 -i eth0 -j DNAT --to 172.16.0.1:135
iptables -t nat -A PREROUTING -p tcp --dport 136 -i eth0 -j DNAT --to 172.16.0.1:136
iptables -t nat -A PREROUTING -p tcp --dport 137 -i eth0 -j DNAT --to 172.16.0.1:137
iptables -t nat -A PREROUTING -p tcp --dport 138 -i eth0 -j DNAT --to 172.16.0.1:138
iptables -t nat -A PREROUTING -p tcp --dport 139 -i eth0 -j DNAT --to 172.16.0.1:139
iptables -t nat -A PREROUTING -p tcp --dport 389 -i eth0 -j DNAT --to 172.16.0.1:389
iptables -t nat -A PREROUTING -p tcp --dport 445 -i eth0 -j DNAT --to 172.16.0.1:445
iptables -t nat -A PREROUTING -p udp --dport 135 -i eth0 -j DNAT --to 172.16.0.1:135
iptables -t nat -A PREROUTING -p udp --dport 136 -i eth0 -j DNAT --to 172.16.0.1:136
iptables -t nat -A PREROUTING -p udp --dport 137 -i eth0 -j DNAT --to 172.16.0.1:137
iptables -t nat -A PREROUTING -p udp --dport 138 -i eth0 -j DNAT --to 172.16.0.1:138
iptables -t nat -A PREROUTING -p udp --dport 139 -i eth0 -j DNAT --to 172.16.0.1:139
iptables -t nat -A PREROUTING -p udp --dport 389 -i eth0 -j DNAT --to 172.16.0.1:389
iptables -t nat -A PREROUTING -p udp --dport 445 -i eth0 -j DNAT --to 172.16.0.1:445

iptables -t nat -A PREROUTING -p tcp --dport 135 -i eth1 -j DNAT --to 172.16.0.1:135
iptables -t nat -A PREROUTING -p tcp --dport 136 -i eth1 -j DNAT --to 172.16.0.1:136
iptables -t nat -A PREROUTING -p tcp --dport 137 -i eth1 -j DNAT --to 172.16.0.1:137
iptables -t nat -A PREROUTING -p tcp --dport 138 -i eth1 -j DNAT --to 172.16.0.1:138
iptables -t nat -A PREROUTING -p tcp --dport 139 -i eth1 -j DNAT --to 172.16.0.1:139
iptables -t nat -A PREROUTING -p tcp --dport 389 -i eth1 -j DNAT --to 172.16.0.1:389
iptables -t nat -A PREROUTING -p tcp --dport 445 -i eth1 -j DNAT --to 172.16.0.1:445
iptables -t nat -A PREROUTING -p udp --dport 135 -i eth1 -j DNAT --to 172.16.0.1:135
iptables -t nat -A PREROUTING -p udp --dport 136 -i eth1 -j DNAT --to 172.16.0.1:136
```



```
iptables -t nat -A PREROUTING -p udp --dport 137 -i eth1 -j DNAT --to 172.16.0.1:137
iptables -t nat -A PREROUTING -p udp --dport 138 -i eth1 -j DNAT --to 172.16.0.1:138
iptables -t nat -A PREROUTING -p udp --dport 139 -i eth1 -j DNAT --to 172.16.0.1:139
iptables -t nat -A PREROUTING -p udp --dport 389 -i eth1 -j DNAT --to 172.16.0.1:389
iptables -t nat -A PREROUTING -p udp --dport 445 -i eth1 -j DNAT --to 172.16.0.1:445
```

Ahora, en el cliente Windows, nos dirigimos a «Panel de control» → «Opciones de carpeta» y desactivamos la opción «Usar el Asistente para compartir (recomendado)»:

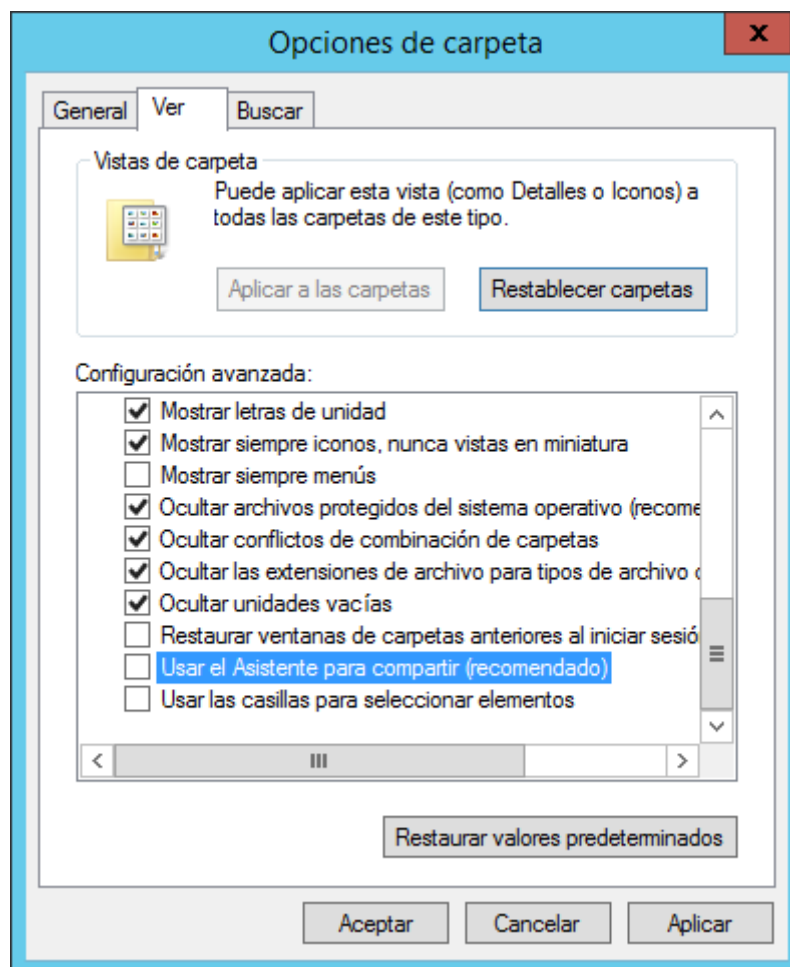


Figura 8: Asistente para compartir desactivado correctamente en las opciones de carpeta, en la pestaña «Ver»

Ahora, creamos una carpeta para compartirla y añadiremos los usuarios que queramos con todos los permisos:

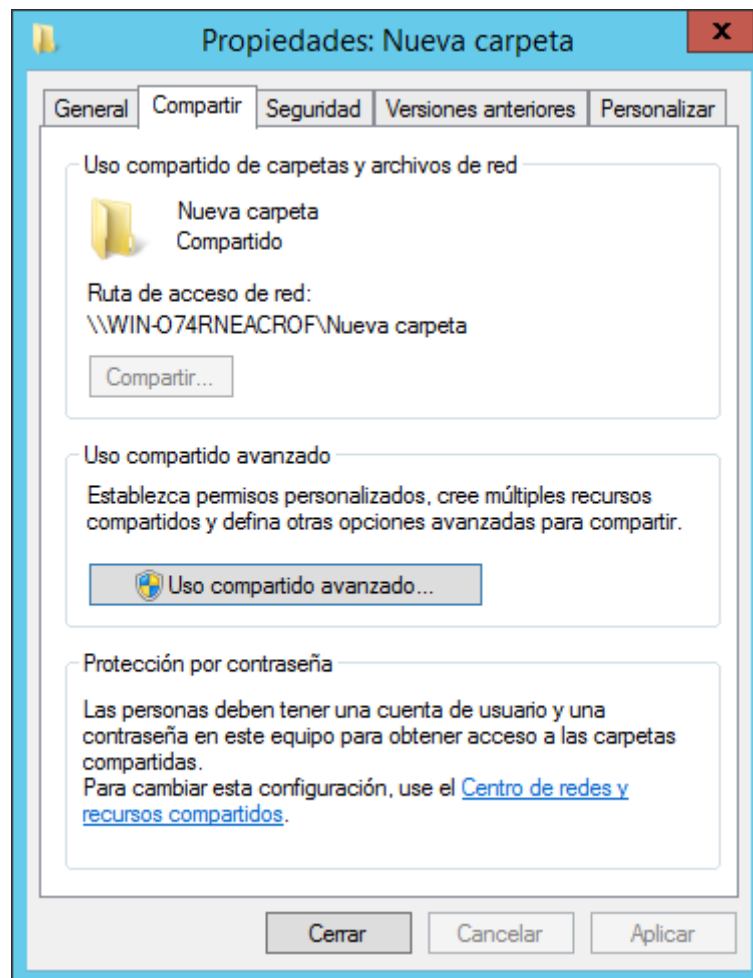


Figura 9: Para poder compartir una carpeta, hay que hacer clic derecho sobre la misma y seleccionar «Compartir con». Nos aparecerá este menú

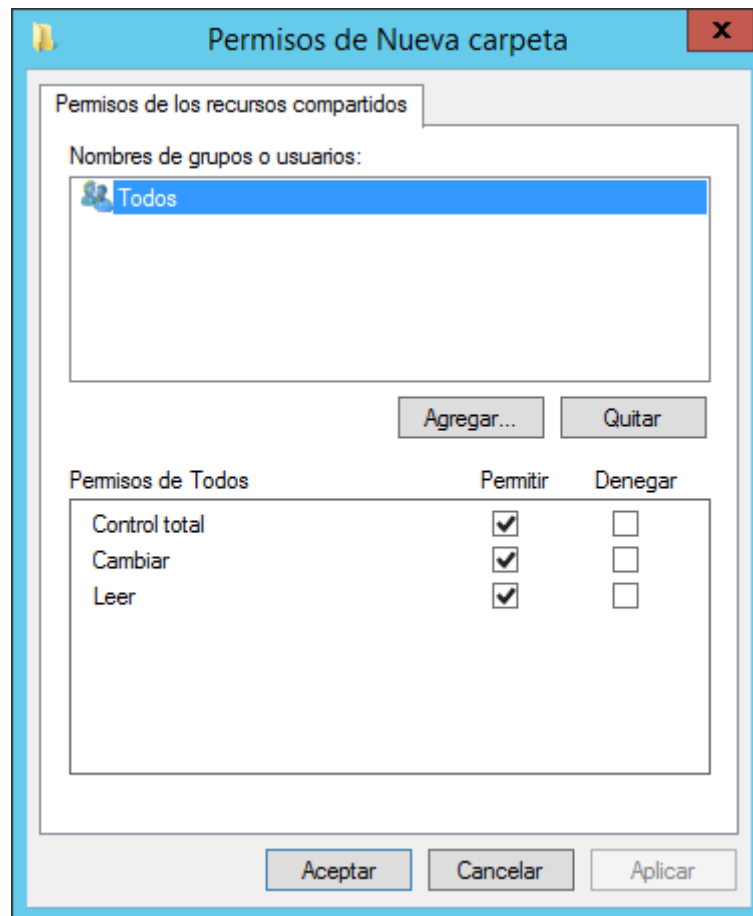


Figura 10: Después, seleccionamos «Uso compartido avanzado...» y pulsamos sobre «Agregar». Añadimos todos los usuarios y todos los permisos, o aquellos que prefiramos

En nuestra carpeta compartida, quien se conecte ya puede crear carpetas o archivos:

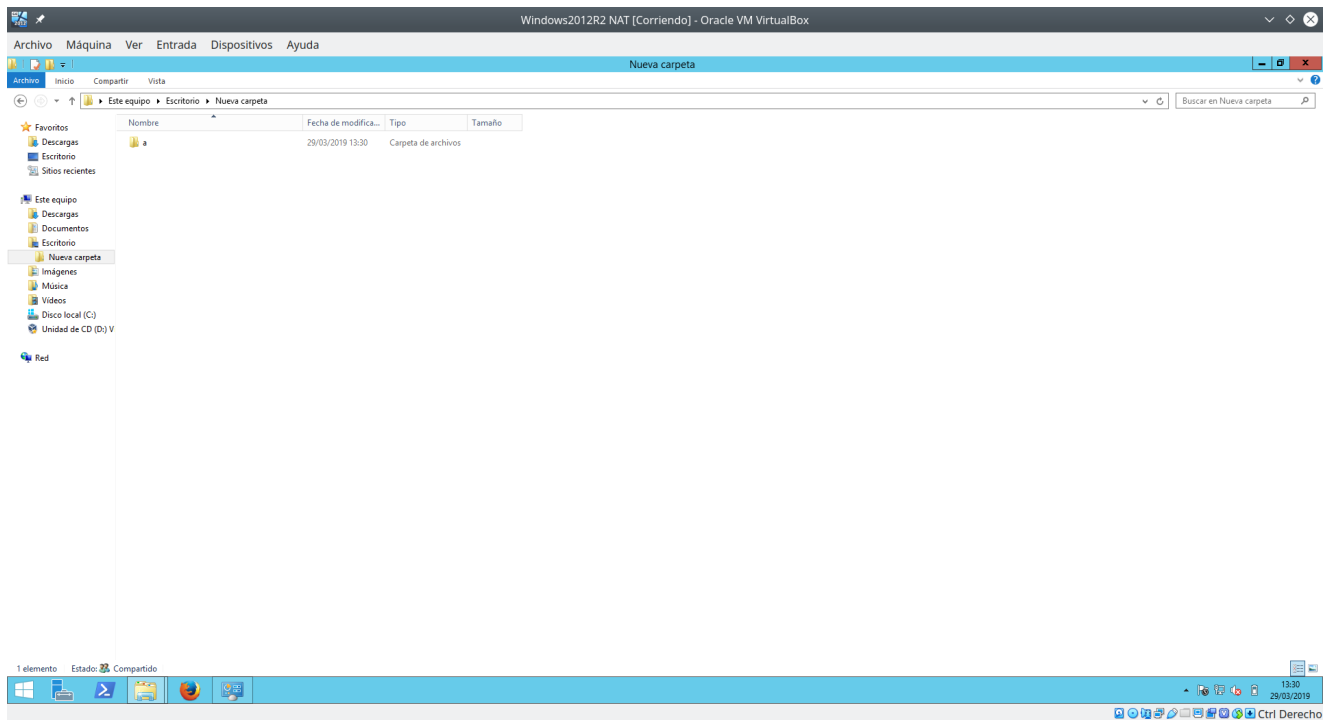


Figura 11: Un compañero creando exitosamente un directorio en nuestra carpeta compartida

Y nosotros nos podemos conectar a la de un compañero para crear una también:

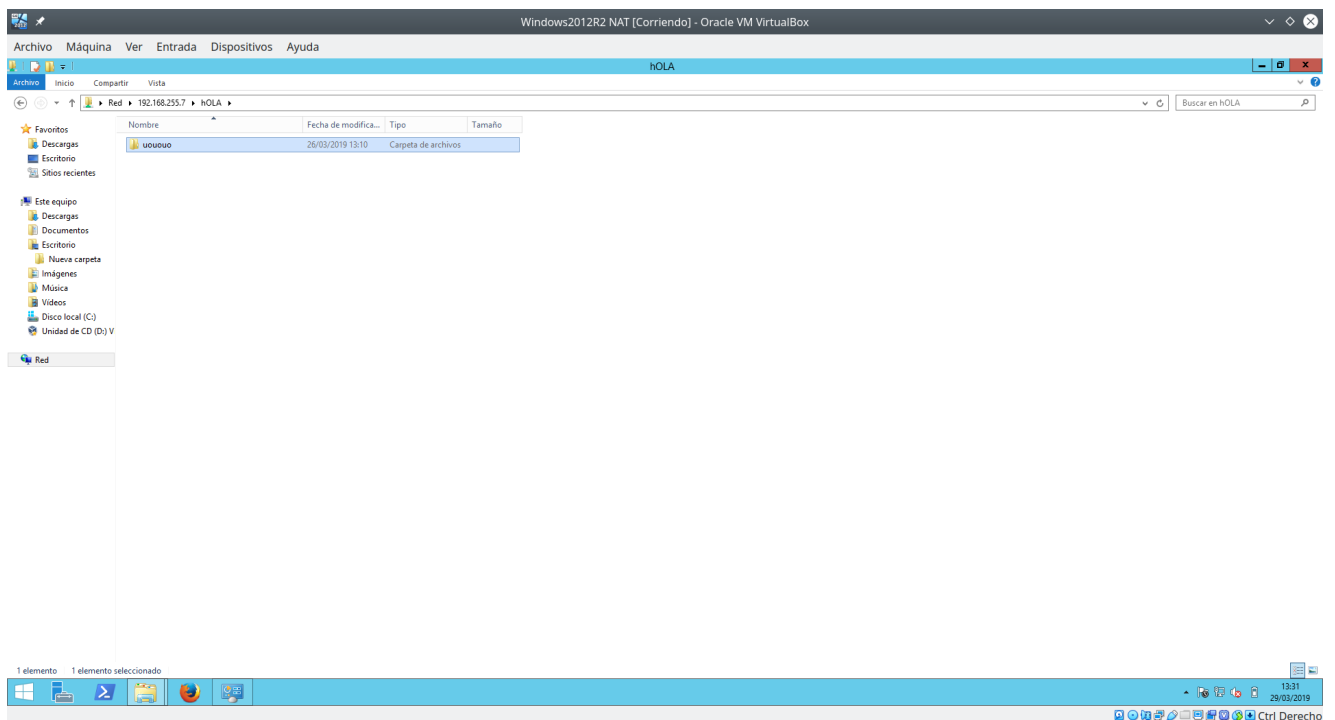


Figura 12: Conectándonos correctamente a la carpeta compartida de un compañero y creando un directorio

Haz que A y C puedan ser administrados mediante SSH desde la red del aula

Primero, instalamos openssh-server en nuestras dos máquinas Debian:

```
apt-get install openssh-server
```

Después, abrimos un puerto de redireccionamiento, en nuestro caso el 22022 al de SSH, el puerto 22, para que por el mismo nos podamos conectar al cliente Debian, ya que por el de SSH lo usaremos para conectarnos con el enrutador:

```
root@enrutador-debian:/home/alumno # iptables -t nat -A PREROUTING -p tcp --dport 22022 -j DNAT --to 172.16.0.2:22
```

Finalmente, nos conectamos simultáneamente al cliente y al enrutador Debian:

```
lg-gram-opensuse:/home/lg-gram # ssh -p 22022 alumno@10.1.0.119
alumno@10.1.0.119's password:
```

```
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.
```

```
You have mail.
```

```
Last login: Tue Apr  2 08:26:46 2019 from 192.168.255.200
```

```
alumno@cliente-debian:~$
```

```
lg-gram-opensuse:/home/lg-gram # ssh alumno@10.1.0.119
alumno@10.1.0.119's password:
```

```
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.
```

```
You have new mail.  
Last login: Tue Apr  2 11:56:39 2019  
  
alumno@enrutador-debian:~$
```

```
[0] 0: bash*
```

```
"lg-gram-opensuse" 12:43 02-abr-19
```

Comprueba el NAT con tcpdump

Comprobando en el enrutador Debian la traducción NAT. Arriba, está la tarjeta de red conectada a la red del aula y, abajo, la de la interna. Al enviar el cliente Windows una solicitud al servidor 8.8.8.8, esta le llega a la tarjeta interna del enrutador y hace una traducción NAT, poniendo su dirección de la red puente conectada a la red del aula (10.1.0.119) como origen de la solicitud. Cuando la respuesta del servidor 8.8.8.8 llega, el enrutador deshace la traducción y esta se la envía al cliente Windows por la red interna:

```
root@enrutador-debian:/home/alumno # tcpdump icmp -n -i eth0  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes  
09:23:31.163937 IP 10.1.0.119 > 8.8.8.8: ICMP echo request, id 1, seq 1235, length  
40  
09:23:32.185906 IP 10.1.0.119 > 8.8.8.8: ICMP echo request, id 1, seq 1236, length  
40  
09:23:33.202022 IP 10.1.0.119 > 8.8.8.8: ICMP echo request, id 1, seq 1237, length  
40  
09:23:34.232723 IP 10.1.0.119 > 8.8.8.8: ICMP echo request, id 1, seq 1238, length  
40
```

```
root@enrutador-debian:/home/alumno # tcpdump icmp -n -i eth2  
09:23:32.190135 IP 8.8.8.8 > 172.168.0.1: ICMP echo reply, id 1, seq 1236, length  
40  
09:23:33.201961 IP 172.16.0.1 > 8.8.8.8: ICMP echo request, id 1, seq 1237, length  
40  
09:23:33.206064 IP 8.8.8.8 > 172.168.0.1: ICMP echo reply, id 1, seq 1237, length  
40  
09:23:34.232657 IP 172.16.0.1 > 8.8.8.8: ICMP echo request, id 1, seq 1238, length  
40  
09:23:34.237077 IP 8.8.8.8 > 172.168.0.1: ICMP echo reply, id 1, seq 1238, length  
40
```

```
[0] 0: tcpdump*
```

```
"enrutador-debian" 09:23 02-abr-19
```