Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería Informática

Dept. Teoría de la Señal, Telemática y Comunicaciones

Alumnos: Raúl Rodríguez Pérez, Pedro Iniesta López
Grupo: A2

Práctica 3 – Configuración de Red I y II (0.375 puntos + 0.375 puntos)

1.1 Realización práctica (parte I)

1) Compruebe todas las direcciones IP que tienen asignadas las diferentes interfaces de red de todos y cada uno de los dispositivos del escenario presentado en la Figura 1. ¿Cómo se llaman dichas interfaces? ¿Qué direcciones de red hay definidas? Deshabilite aquellas interfaces que no sean necesarias, es decir, todas aquellas que no correspondan ni a gestión ni a datos.

- **INTERFACES PC1:**

enp0s3 -> dirección de red: 10.0.2.15
enp0s8 -> dirección de red: 192.168.59.2
enp0s9 (datos) -> dirección de red: 33.1.1.2
enp0s10 (gestión) -> dirección de red: 192.168.1.1

```
administrador@pc1:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::3d00:5458:c3ab:e588  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:fd:98:cc  txqueuelen 1000  (Ethernet)
        RX packets 121086  bytes 170565649 (170.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8681  bytes 657290 (657.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.59.2  netmask 255.255.255.0  broadcast 192.168.59.255
        inet6 fe80::a00:27ff:fee1:2a66  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e1:2a:66  txqueuelen 1000  (Ethernet)
        RX packets 201  bytes 24426 (24.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 96  bytes 9898 (9.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s9: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 33.1.1.2  netmask 255.255.255.0  broadcast 33.1.1.255
        inet6 fe80::a00:27ff:fed6:9467  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d6:94:67  txqueuelen 1000  (Ethernet)
        RX packets 183  bytes 22594 (22.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 96  bytes 9874 (9.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.1  netmask 255.255.0.0  broadcast 192.168.255.255
        inet6 fe80::a00:27ff:feca:a0bb  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:ca:a0:bb  txqueuelen 1000  (Ethernet)
        RX packets 170  bytes 21754 (21.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 94  bytes 9750 (9.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **INTERFACES PC3:**

enp0s3 -> dirección de red: 10.0.2.15
enp0s8 -> dirección de red: 192.168.59.4
enp0s9 (datos) -> dirección de red: 33.1.2.2
enp0s10 (gestión) -> dirección de red: 192.168.1.3

```
administrador@pc3:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::175c:b708:4d5b:2f40  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1c:df:88  txqueuelen 1000  (Ethernet)
        RX packets 13066  bytes 18295335 (18.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1241  bytes 115818 (115.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.59.4  netmask 255.255.255.0  broadcast 192.168.59.255
        inet6 fe80::a00:27ff:fe7f:f27c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:7f:f2:7c  txqueuelen 1000  (Ethernet)
        RX packets 4  bytes 912 (912.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 80  bytes 8486 (8.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s9: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 33.1.2.2  netmask 255.255.255.0  broadcast 33.1.2.255
        inet6 fe80::a00:27ff:fe5d:dc9b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5d:dc:9b  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 79  bytes 8399 (8.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.3  netmask 255.255.0.0  broadcast 192.168.255.255
        inet6 fe80::a00:27ff:fe72:93f3  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:72:93:f3  txqueuelen 1000  (Ethernet)
```

- **INTERFACES R1_1:**

La red de gestión es la ether3 y las redes de datos son ether1, ether2 y ether4.

```
[admin@R11] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   33.1.1.1/24        33.1.1.0        ether2
 1   192.168.1.11/16    192.168.0.0     ether3
 2   172.16.1.1/24      172.16.1.0      ether4
 3   172.17.1.1/24      172.17.1.0      ether1
```

- **INTERFACES R1_2:**

La red de gestión es la ether3 y las redes de datos son ether1, ether2 y ether4.

```
[admin@R12] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   33.1.2.1/24        33.1.2.0        ether2
 1   192.168.1.12/16    192.168.0.0     ether3
 2   172.16.1.2/24      172.16.1.0      ether4
 3   172.18.1.2/24      172.18.1.0      ether1
```

- **INTERFACES R1_4:**

La red de gestión es la ether3 y las redes de datos son ether1 y ether4.

```
[admin@R14] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   172.17.1.4/24      172.17.1.0      ether1
 1   192.168.1.14/16    192.168.0.0     ether3
 2   172.18.1.4/24      172.18.1.0      ether4
```

Además de esto, hemos deshabilitado las redes enp0s3 y enp0s8 del PC_1 y el PC_ 3, haciendo uso de la sentencia 'ifdown enp0s3/8' . Esto es debido a que el enunciado nos pide deshabilitar las redes que no sean ni de gestión ni de datos, por lo que las únicas redes que dejamos habilitadas son la red enp0s9 (datos) y la red enp0s10 (gestión).

2) Introduzca las entradas de encaminamiento necesarias para comunicar PC_1 y PC_3 utilizando las subredes de datos. Compruebe la configuración con las utilidades `ping` y `traceroute`, y anote los resultados.

A raíz de la figura 1 que se encuentra en el pdf de esta práctica 3 de Fundamentos de Redes, hemos observado y premeditado, cual son los diferentes pasos que debemos realizar para comunicar PC_1 y PC_3 utilizando las subredes de datos.

Lo primero que deberíamos hacer es mirar red por red para ver si hay alguna coincidencia, es decir, coger nuestra ip destino e ir entrada por entrada mirando a ver si corresponde con alguna de las subredes que tenemos configuradas. En nuestro caso, la ip destino no corresponde con ninguna de las subredes, por lo que debemos enfocarlo de otra manera.

A continuación, tenemos que realizar dos sencillos pasos, que básicamente se basan en hacer que cualquier paquete que no pertenezca a mi red, sea reenviado por una pasarela por defecto. En el caso de nuestra figura 1, estas pasarelas van a ser; el router 1 para el PC_1 y el router 2 para el PC_ 3.

- **CREANDO PASARELA PC_1 -> R1_1**

```
administrador@pc1:~/Escritorio$ sudo route add default gw 33.1.1.1
SIOCADDRT: El archivo ya existe
administrador@pc1:~/Escritorio$ route -n
Tabla de rutas IP del núcleo
Destino         Pasarela        Genmask         Indic Métric Ref    Uso Interfa
z
0.0.0.0         33.1.1.1        0.0.0.0         UG    0      0        0 enp0s9
0.0.0.0         10.0.2.2        0.0.0.0         UG    101    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     101    0        0 enp0s3
33.1.1.0        0.0.0.0         255.255.255.0   U     103    0        0 enp0s9
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s10
192.168.0.0     0.0.0.0         255.255.0.0     U     100    0        0 enp0s10
192.168.59.0    0.0.0.0         255.255.255.0   U     102    0        0 enp0s8
administrador@pc1:~/Escritorio$
```

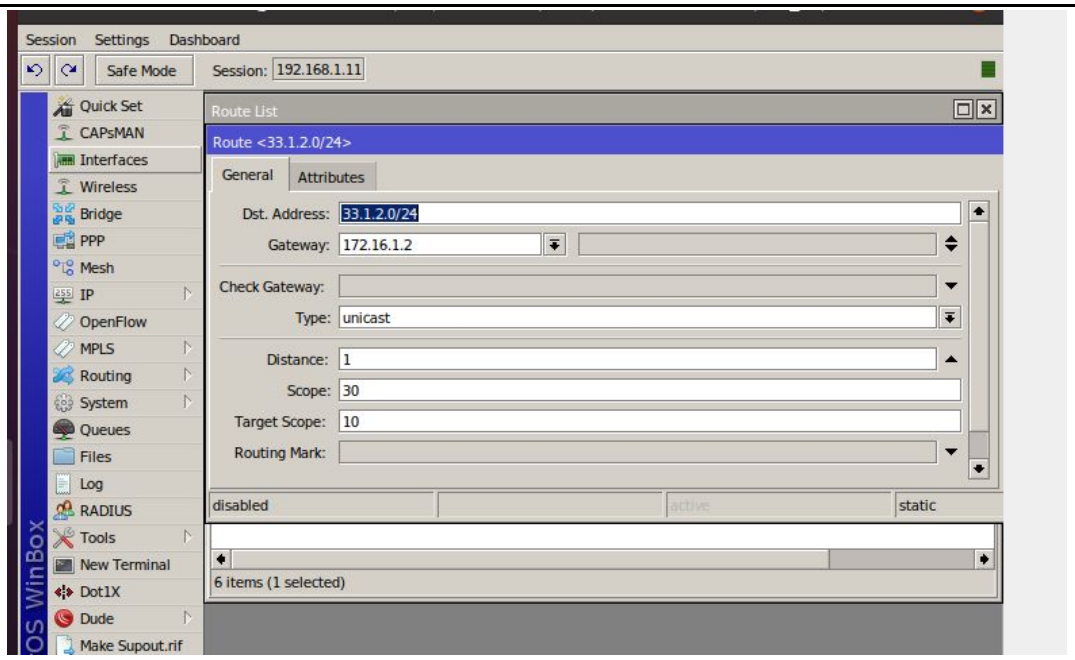
*En la primera sentencia pone que el archivo ya existe porque la captura fue tomada después de haberla ejecutado por primera vez

- **CREANDO PASARELA PC_3 -> R1_2**

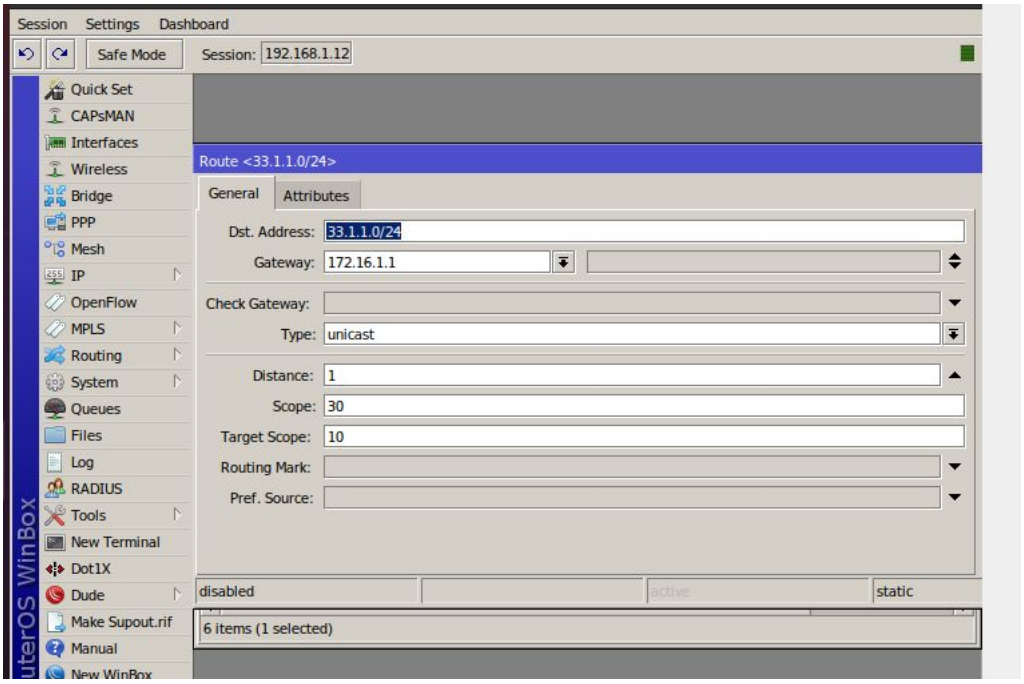
```
administrador@pc3:~$ sudo route add default gw 33.1.2.1
[sudo] contraseña para administrador:
administrador@pc3:~$ route -n
Tabla de rutas IP del núcleo
Destino         Pasarela        Genmask         Indic Métric Ref    Uso Interfaz
0.0.0.0         33.1.2.1        0.0.0.0         UG    0      0        0 enp0s9
0.0.0.0         10.0.2.2        0.0.0.0         UG    101    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     101    0        0 enp0s3
33.1.2.0        0.0.0.0         255.255.255.0   U     103    0        0 enp0s9
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp0s10
192.168.0.0     0.0.0.0         255.255.0.0     U     100    0        0 enp0s10
192.168.59.0    0.0.0.0         255.255.255.0   U     102    0        0 enp0s8
administrador@pc3:~$
```

Tras haber creado las pasarelas por defecto, ya tenemos el primer paso realizado, con este podemos decir que tenemos conexión entre el PC_1 - R1_1 y el PC_ 3 - R1_2. Lo único que nos quedaría por hacer es la conexión entre los routers, es decir, crear la pasarela entre ellos. Dicha pasarela la vamos a crear usando la aplicación de 'Wine'. Entrando en el apartado de IP->ROUTE, y gracias a la figura 1, conocemos las ip destino y las ip de los próximos saltos (GW) que tenemos que configurar y añadir a nuestros routers:

- **CREANDO PASARELA R1_1 -> R1_2**

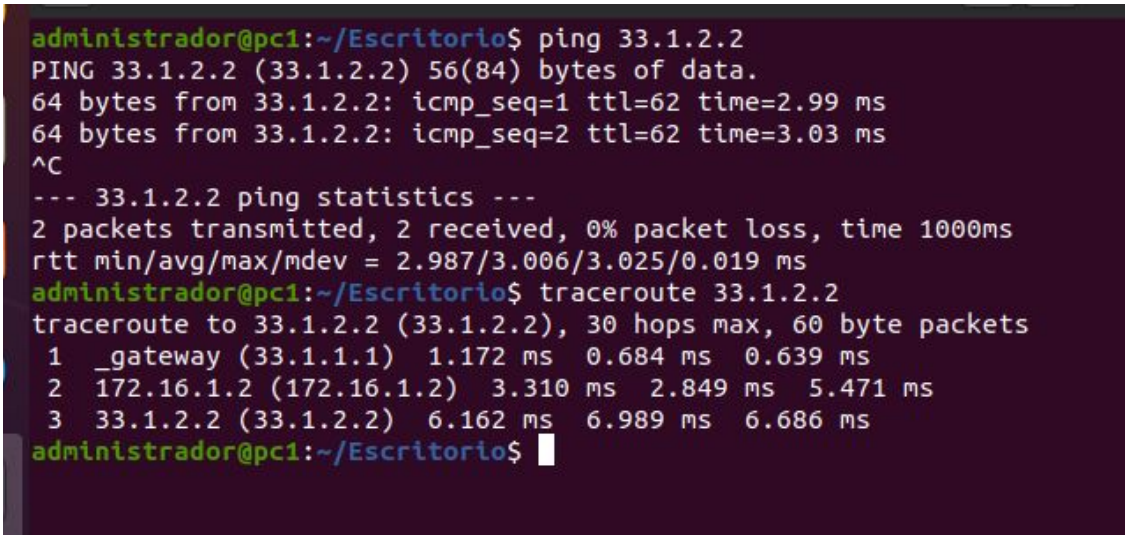


- **CREANDO PASARELA R1_2 -> R1_1**



Una vez hecho esto, ya tendríamos hecha nuestra conexión entre el PC_1 y el PC_ 3, puesto que, ya hemos creado y configurado todas las pasarelas necesarias para conectarnos entre las máquinas virtuales utilizando subredes de datos. Lo último que nos quedaría es probar que está todo correcto con el uso de utilidades como ping y traceroute

- **USO DE PING Y TRACEROUTE ENTRE PC_1 -> PC_3**



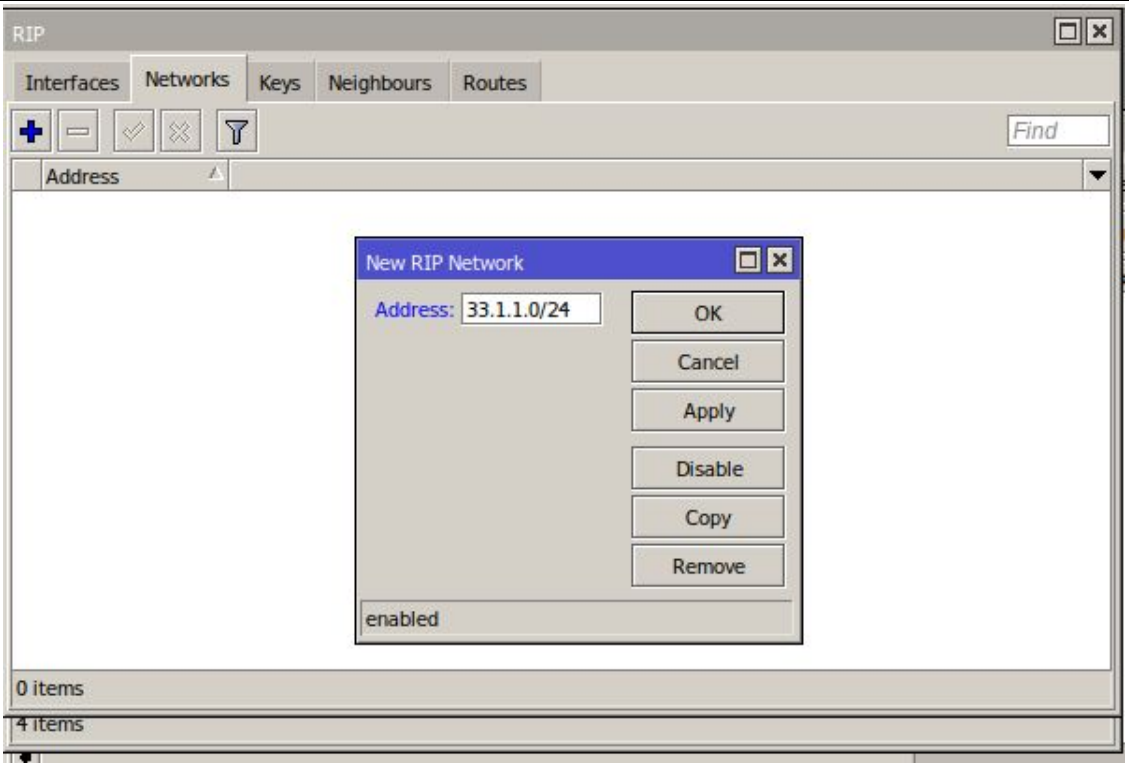
* Destacar que con la utilidad traceroute, nos aparece la ruta que han seguido los paquetes desde el PC_1, pasando por el router 1 y 2, y llegando al PC_ 3.

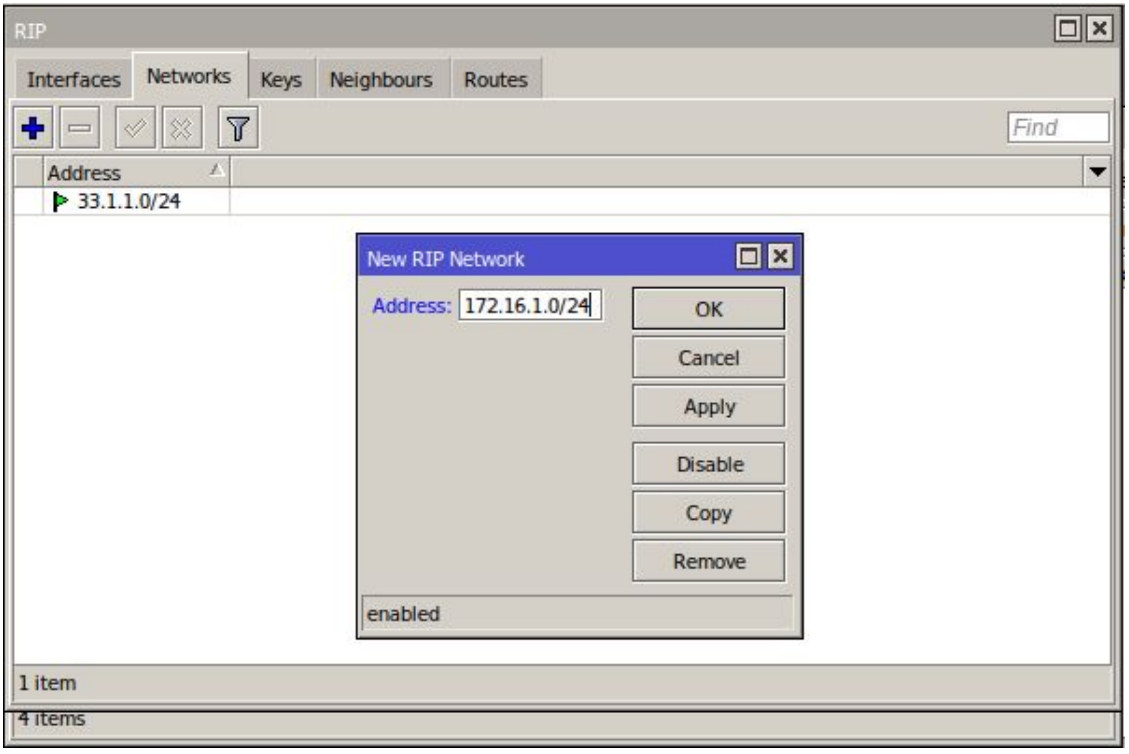
3) Configure RIP en todos y cada uno de los *routers.* Compruebe la tabla de encaminamiento tanto en el menú correspondiente en RIP como en el menú *IP->Routes.* ¿Tiene sentido lo que observa? Corrobórelo mediante la comprobación de la conectividad y saltos entre PC_1 y PC_3 con las utilidades `ping` y `traceroute` y anote los resultados.

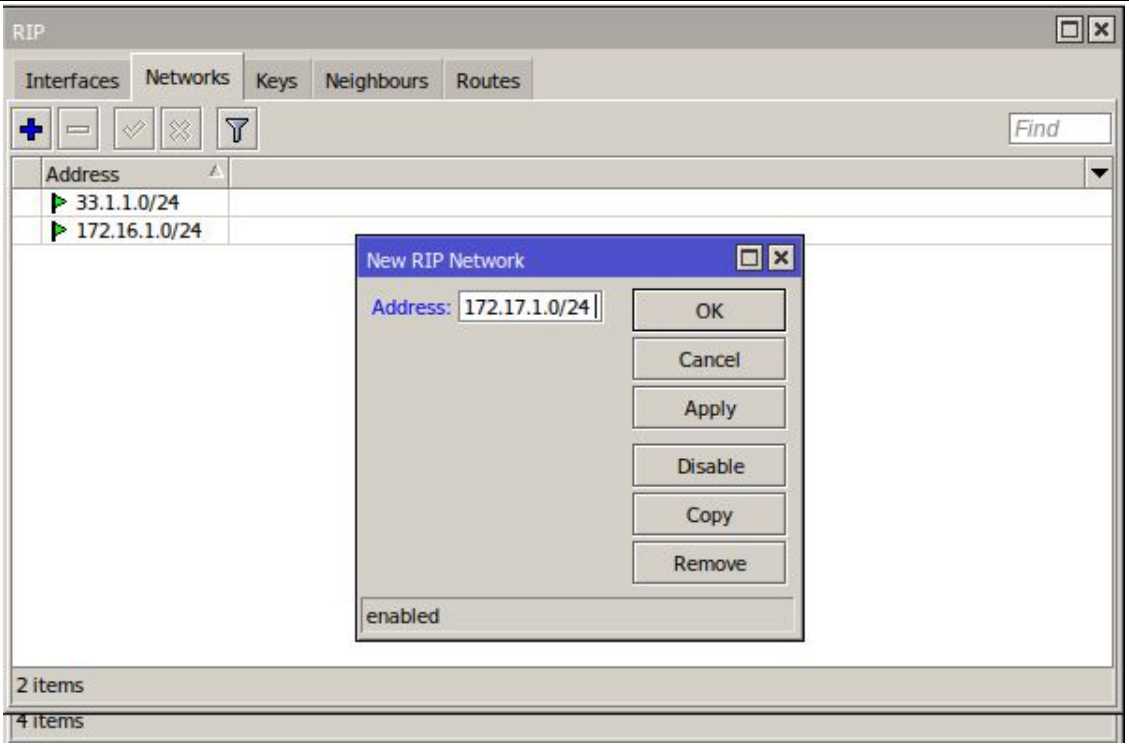
Para configurar el RIP en todos los routers tenemos que configurar a qué redes se conecta cada router. Para ello, con Winbox accederemos al menú Routing -> RIP -> Networks. Vamos a empezar por el R1_1.

R1_1

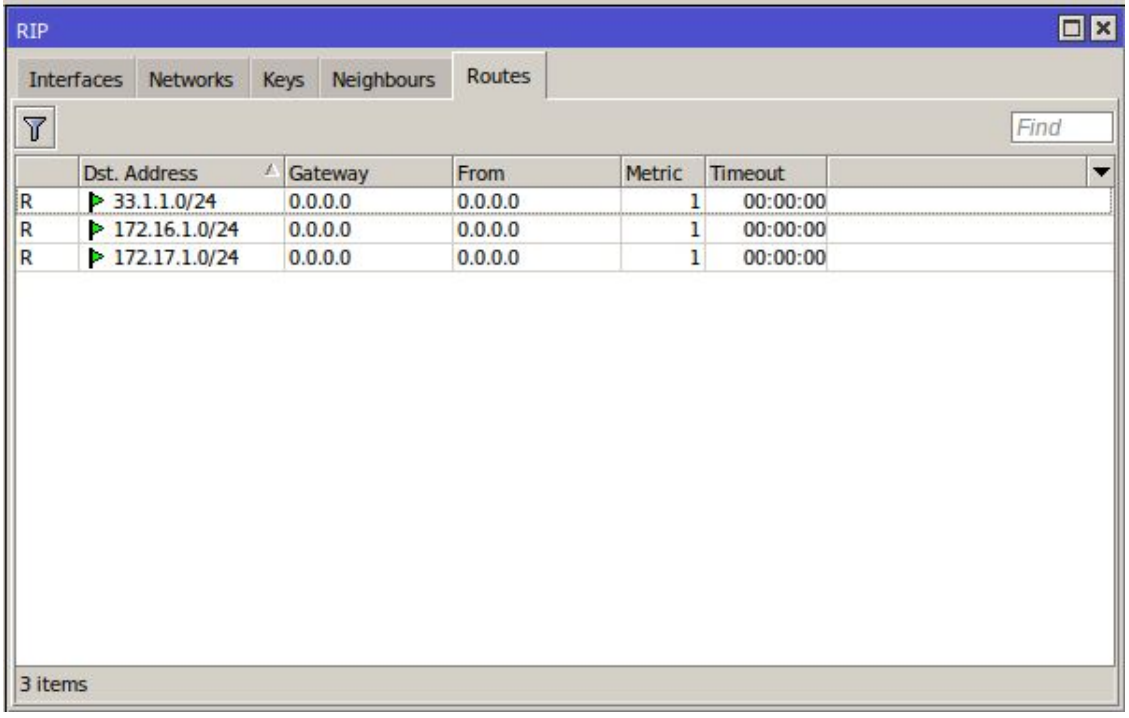
Si nos fijamos en el diagrama de la Práctica, podemos observar como el R1_1 está conectado con 3 redes de datos: 33.1.1.0/24, 172.16.1.0/24, 172.17.1.0/24. Añadimos estas redes a las Networks de RIP.


RIP
Interfaces
Networks
Keys
Neighbours
Routes
Find
Address
New RIP Network
Address: 33.1.1.0/24
OK
Cancel
Apply
Disable
Copy
Remove
enabled
0 items
4 items


RIP
Interfaces
Networks
Keys
Neighbours
Routes
Find
Address
33.1.1.0/24
New RIP Network
Address: 172.16.1.0/24
OK
Cancel
Apply
Disable
Copy
Remove
enabled
1 item
4 items



Una vez añadidas las distintas redes, podemos ver la tabla de routing de R1_1.

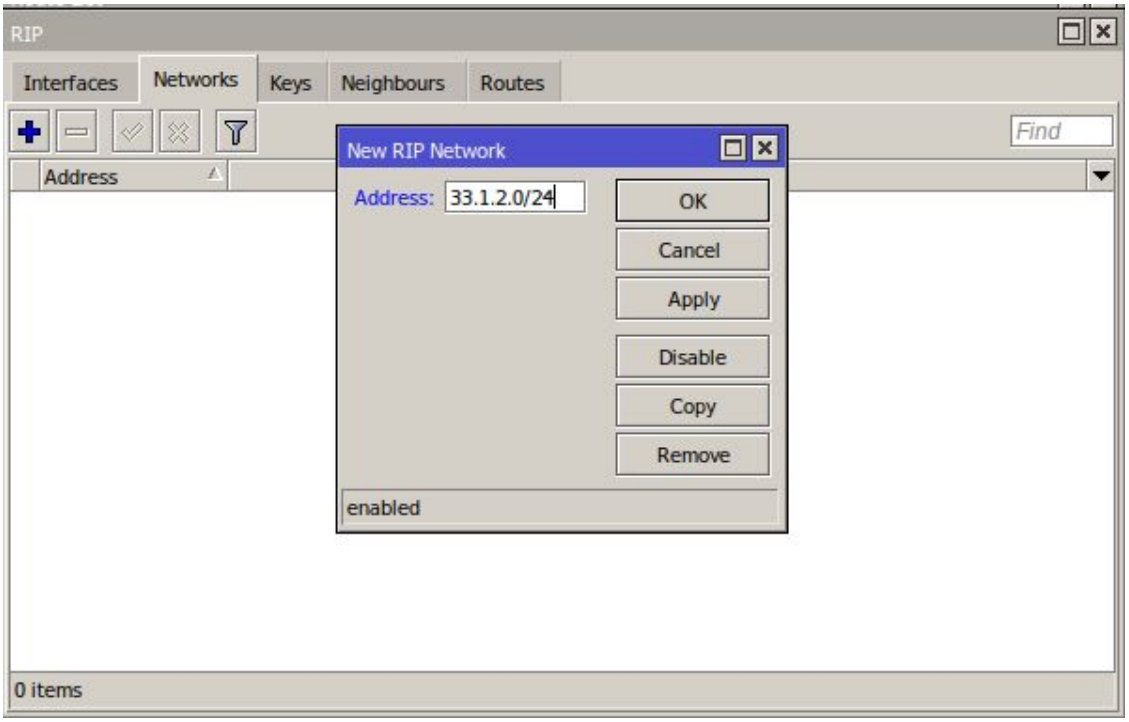


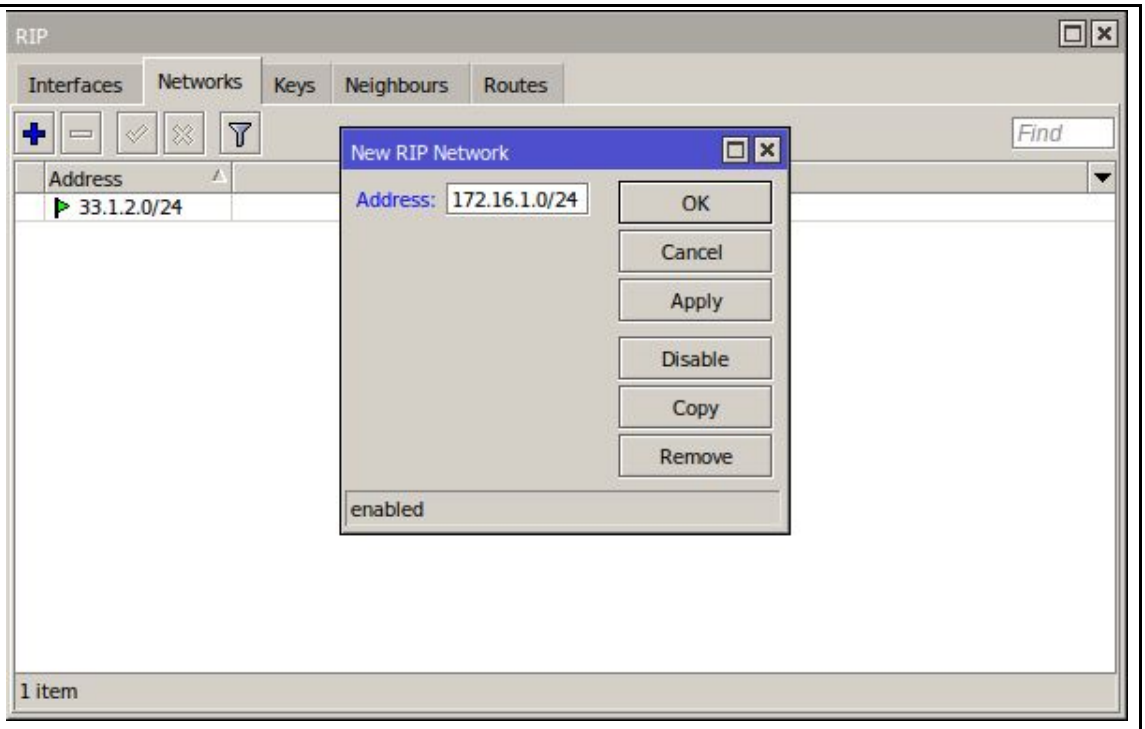
Dst Address nos indica a las direcciones que podemos llegar, from nos dice a través de qué red se accede a la dirección destino y metric nos da la cantidad de saltos que tenemos que dar hasta llegar al destino. RIP tomará el camino más corto para llegar.

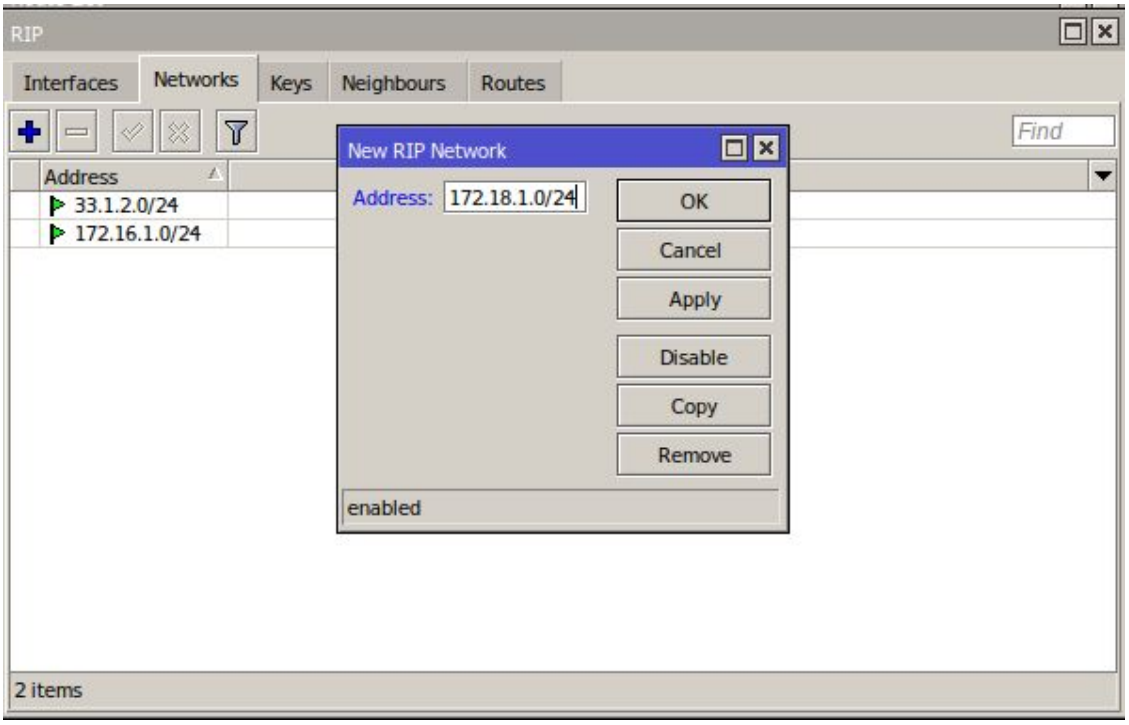
Como no hemos configurado aún las RIP del R1_2 y R1_4, el R1_1 solo puede llegar a sus subredes. Ahora añadimos las RIP del R1_2

R1_2

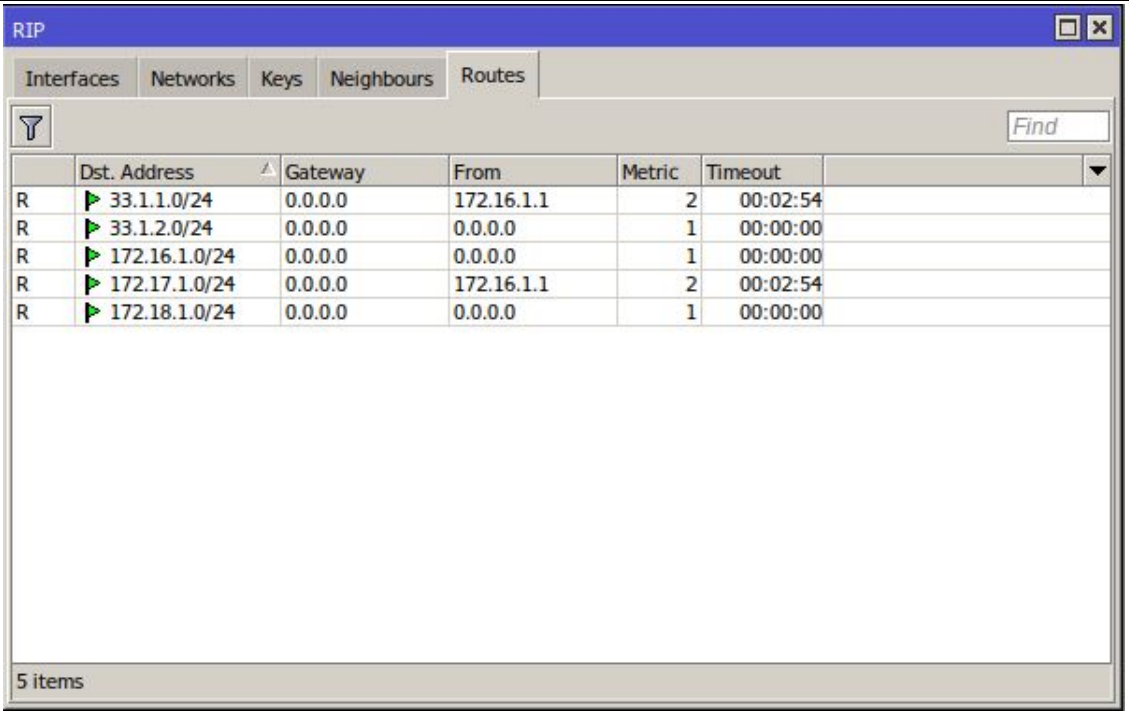
R1_2 está conectado con 3 redes de datos: 33.1.2.0/24, 172.16.1.0/24, 172.18.1.0/24. Añadimos estas redes a las Networks de RIP.







Una vez añadidas las distintas redes, podemos ver la tabla de routing de R1_2.



Vemos que podemos llegar a la red 33.1.1.0/24 a través del R1_1, es decir, hay conectividad desde el PC3 al PC1. También tenemos conectividad desde el PC1 al PC3. Vamos a comprobarlo.

```
administrador@pc1:~/Descargas$ ping 33.1.2.2
PING 33.1.2.2 (33.1.2.2) 56(84) bytes of data.
64 bytes from 33.1.2.2: icmp_seq=1 ttl=62 time=5.70 ms
64 bytes from 33.1.2.2: icmp_seq=2 ttl=62 time=3.29 ms
64 bytes from 33.1.2.2: icmp_seq=3 ttl=62 time=2.78 ms
^C
--- 33.1.2.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.777/3.920/5.696/1.272 ms
```

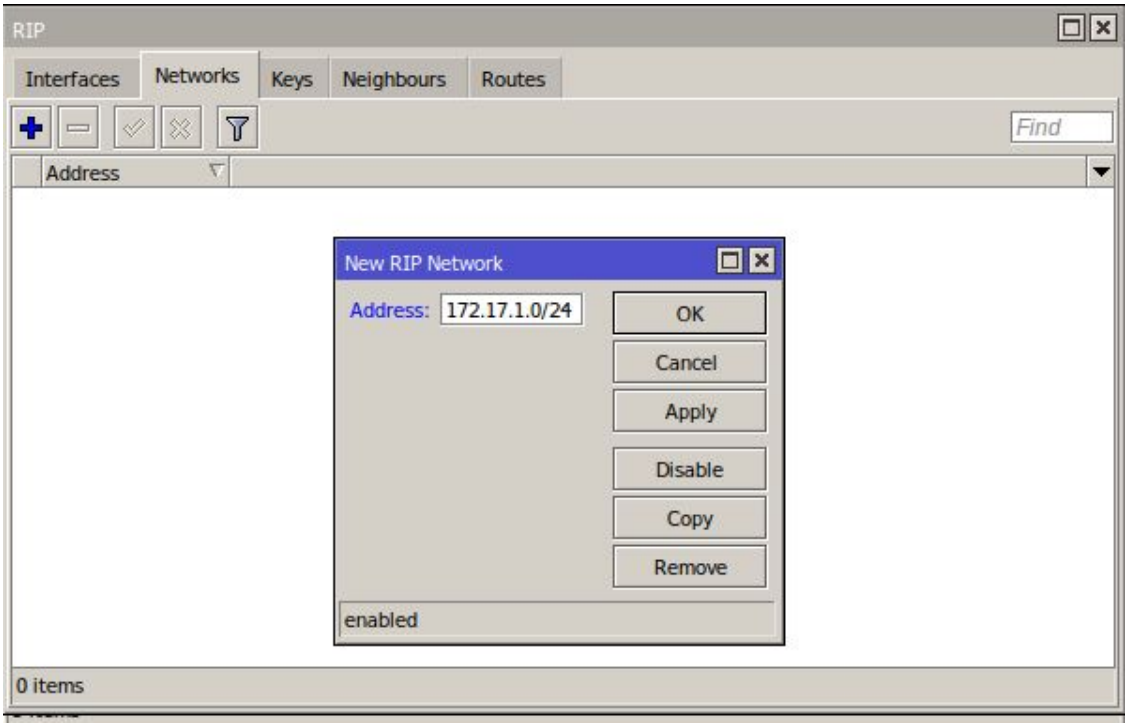
La ruta que sigue es desde PC1 al R1_1, de ahí pasa al R1_2 a través de la red 172.16.1.2, (red que tienen en común el R1_1 y el R2_2) y desde el R1_2 va al PC3.

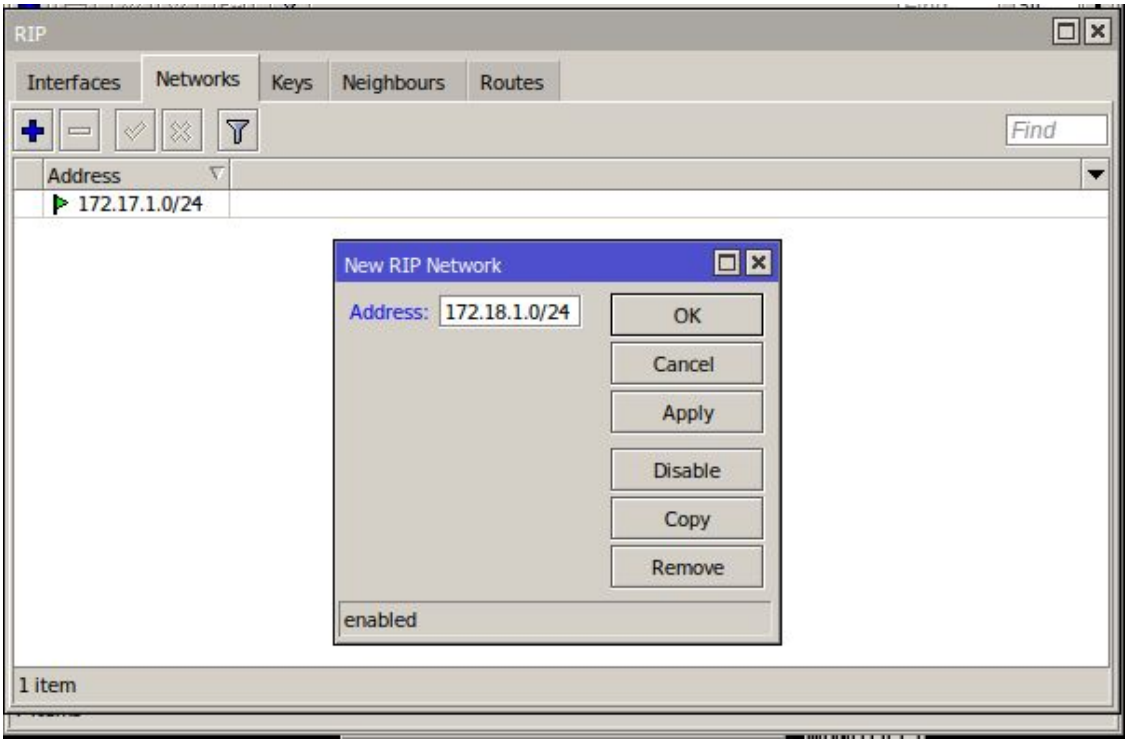
```
administrador@pc1:~/Descargas$ traceroute -I 33.1.2.2
traceroute to 33.1.2.2 (33.1.2.2), 30 hops max, 60 byte packets
 1  _gateway (33.1.1.1)  1.108 ms  0.705 ms  0.918 ms
 2  172.16.1.2 (172.16.1.2)  6.269 ms  5.788 ms  4.725 ms
 3  33.1.2.2 (33.1.2.2)  4.394 ms  6.055 ms  7.054 ms
```

Por último, añadimos la RIP del R1_4.

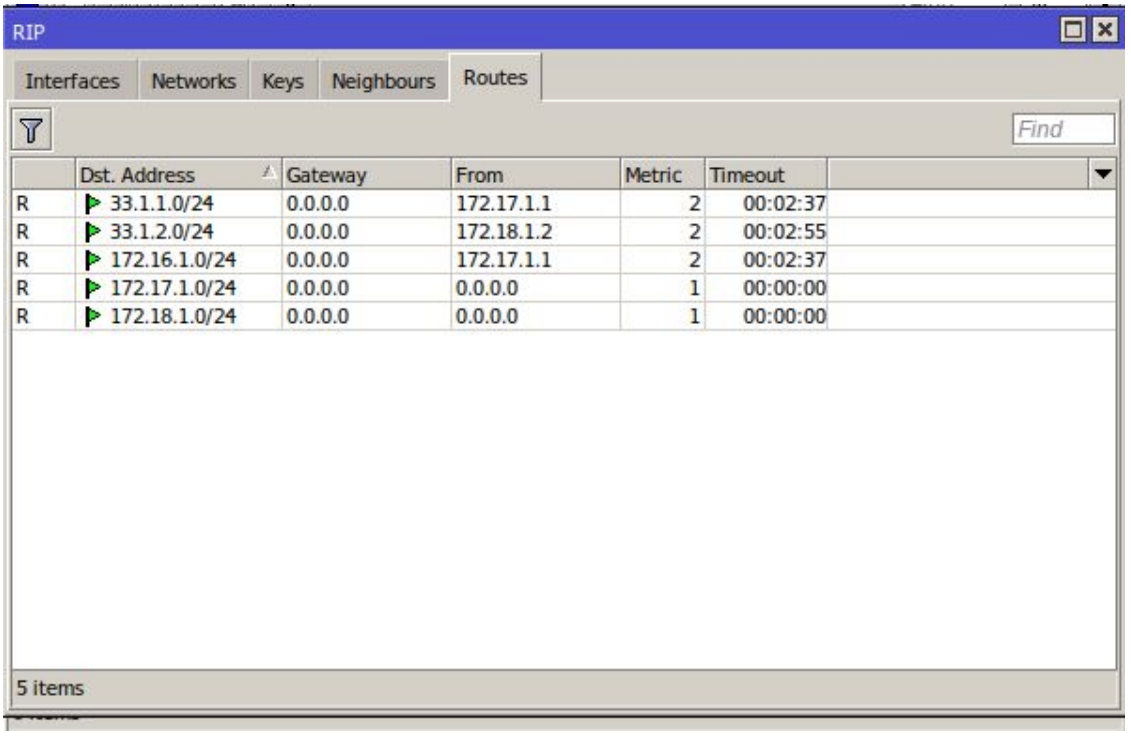
R1_4

R1_4 está conectado con 2 redes de datos: 172.17.1.0/24, 172.18.1.0/24. Añadimos estas redes a las Networks de RIP.





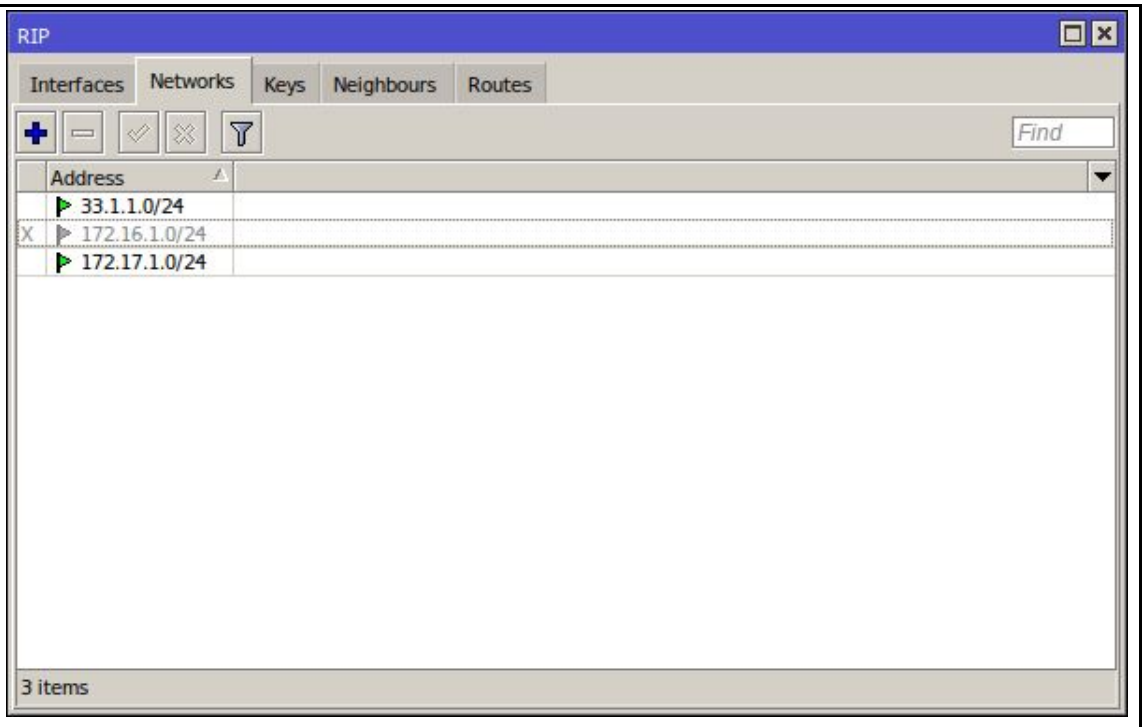
La tabla de routing es la siguiente:



No obstante, la conectividad entre PC1 y PC2 no va a cambiar su ruta, pues RIP elige el camino más corto. Como ir de PC1 a R1_1, de R1_1 a R1_2 y de R1_2 a PC3 es más corto que ir de PC1 a R1_1, de R1_1 a R1_4, de R1_4 a R1_2 y de R1_2 a PC3, elige la primera opción.

4) Deshabilite la interfaz de R1_1 que conecta con la red 172.16.1.0/24 y comprueba si se han producido modificaciones en las tablas de encaminamiento de los *routers.* ¿Qué camino se ha establecido para llegar desde PC_1 a PC_3? Apóyese de las herramientas `ping` y `traceroute` para corroborar lo anterior y anote los resultados.

Primero, desactivamos la interfaz R1_1 que conecta con R1_2.



Lo que debe pasar ahora es que para conectarse desde el PC1 al PC2, tenga que pasar del R1_1 al R1_4 y del R1_4 al R1_2. Esto se debe a que hemos desactivado la interfaz de R1_1 que conecta con R1_2. Vamos a ver si se siguen conectando con ping, y la ruta que sigue con traceroute.

```
administrador@pc1:~/Descargas$ ping 33.1.2.2
PING 33.1.2.2 (33.1.2.2) 56(84) bytes of data.
64 bytes from 33.1.2.2: icmp_seq=1 ttl=61 time=2.15 ms
64 bytes from 33.1.2.2: icmp_seq=2 ttl=61 time=5.26 ms
64 bytes from 33.1.2.2: icmp_seq=3 ttl=61 time=3.70 ms
^C
--- 33.1.2.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2011ms
rtt min/avg/max/mdev = 2.150/3.701/5.257/1.268 ms
```

Vemos que hay conexión, ahora vamos a ver la ruta que sigue.

```
administrador@pc1:~/Descargas$ traceroute -I 33.1.2.2
traceroute to 33.1.2.2 (33.1.2.2), 30 hops max, 60 byte packets
 1  _gateway (33.1.1.1)  1.545 ms  1.462 ms  1.367 ms
 2  172.17.1.4 (172.17.1.4)  2.908 ms  2.780 ms  2.660 ms
 3  172.18.1.2 (172.18.1.2)  6.252 ms  6.223 ms  6.197 ms
 4  33.1.2.2 (33.1.2.2)  11.171 ms  11.018 ms  10.985 ms
```

Podemos comprobar que sigue la ruta comentada anteriormente.

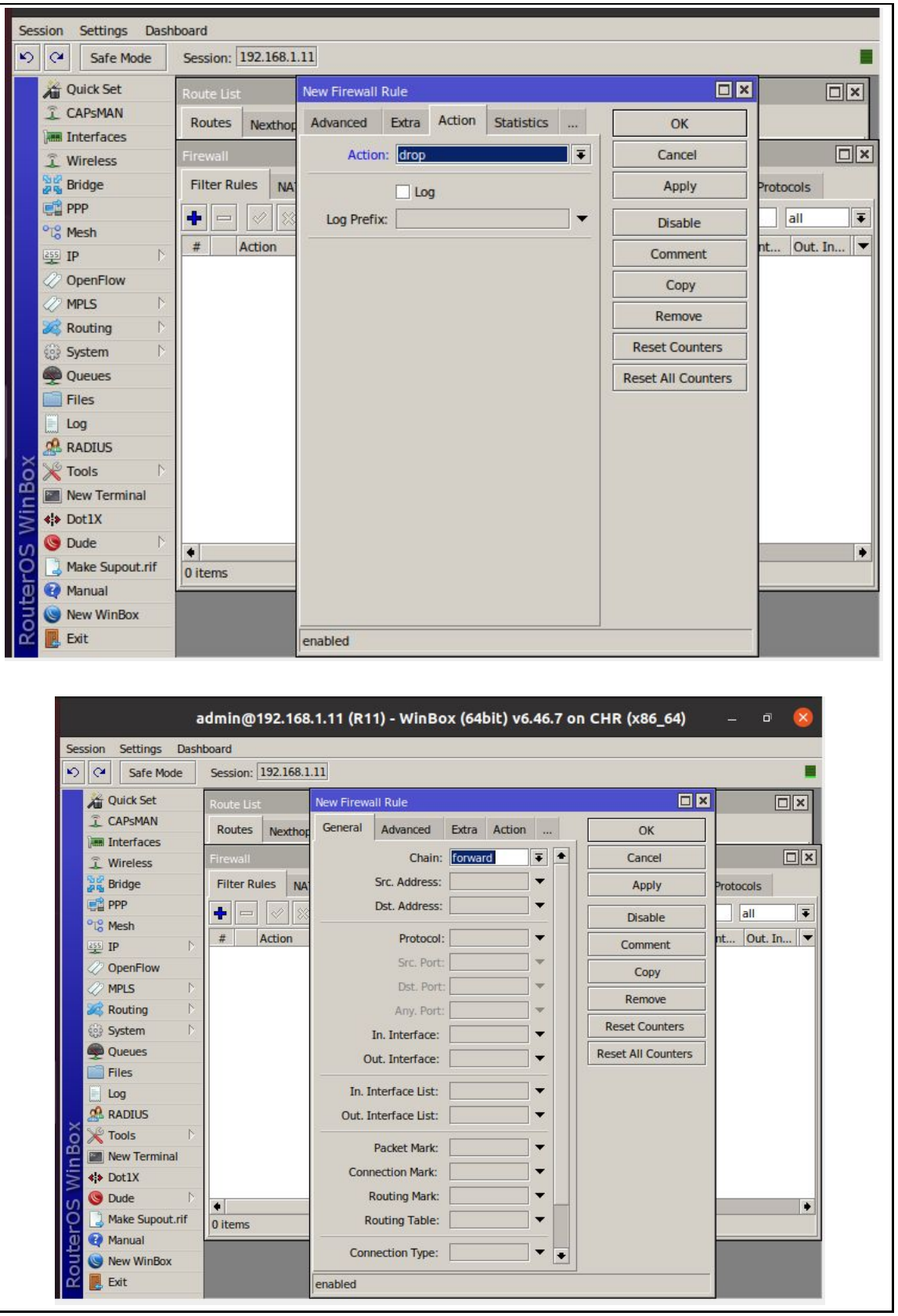
1.2 Realización práctica (parte II)

1) Configure R1_1 para que no reenvíe ningún tipo de tráfico (acción "drop"). Habitualmente, al configurar un cortafuegos, inicialmente se deniega cualquier acceso, y luego se añaden reglas para el tráfico que sí se desea dejar pasar. Compruebe que ahora no es posible establecer conexiones entre los PC.

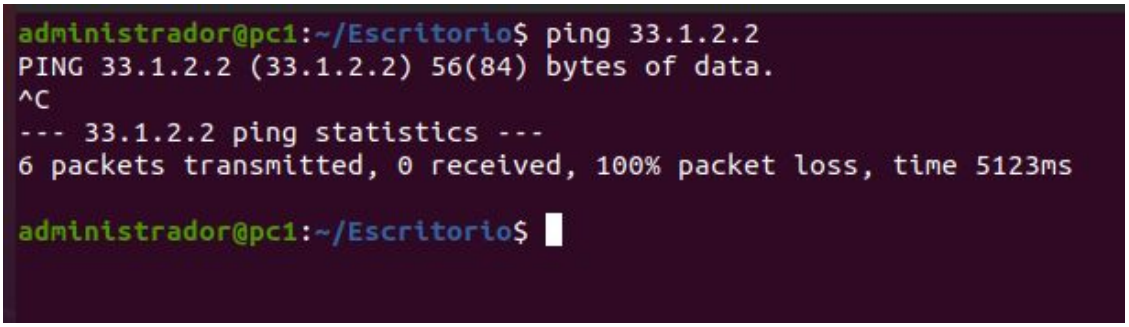
Comprobamos que se puede hacer ping desde el PC1 al PC3 antes de activar el firewall.

```
administrador@pc1:~/Escritorio$ ping 33.1.2.2
PING 33.1.2.2 (33.1.2.2) 56(84) bytes of data.
64 bytes from 33.1.2.2: icmp_seq=1 ttl=62 time=1.19 ms
64 bytes from 33.1.2.2: icmp_seq=2 ttl=62 time=28.8 ms
64 bytes from 33.1.2.2: icmp_seq=3 ttl=62 time=3.81 ms
^C
--- 33.1.2.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2011ms
rtt min/avg/max/mdev = 1.190/11.266/28.798/12.442 ms
administrador@pc1:~/Escritorio$
```

Abrimos el Winbox, nos conectamos al R1_1, vamos a IP->Firewall->Añadir->Action y seleccionamos drop. Con esta acción denegamos cualquier acceso.

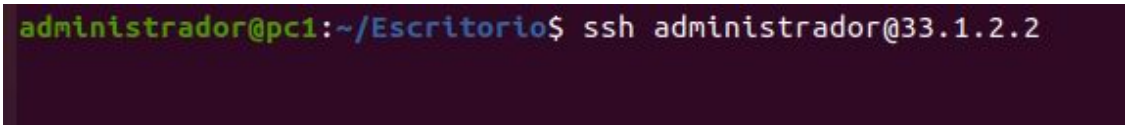

Session Settings Dashboard
Safe Mode
Session: 192.168.1.11
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
OpenFlow
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
Dude
Make Supout.rif
Manual
New WinBox
Exit
RouterOS WinBox
Route List
Routes
Nexthop
Firewall
Filter Rules
Action
0 items
New Firewall Rule
Advanced
Extra
Action
Statistics
Action: drop
Log
Log Prefix:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
enabled
Protocols
all
Out. In...
admin@192.168.1.11 (R11) - WinBox (64bit) v6.46.7 on CHR (x86_64)
General
Chain: forward
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
In. Interface:
Out. Interface:
In. Interface List:
Out. Interface List:
Packet Mark:
Connection Mark:
Routing Mark:
Routing Table:
Connection Type:

Podemos comprobar que ya no hay conexión entre el PC1 y el PC3 ya que el firewall deniega cualquier acceso, menos aquellos que especifiquemos. Como no hay nada especificado de momento, no hay conexión.

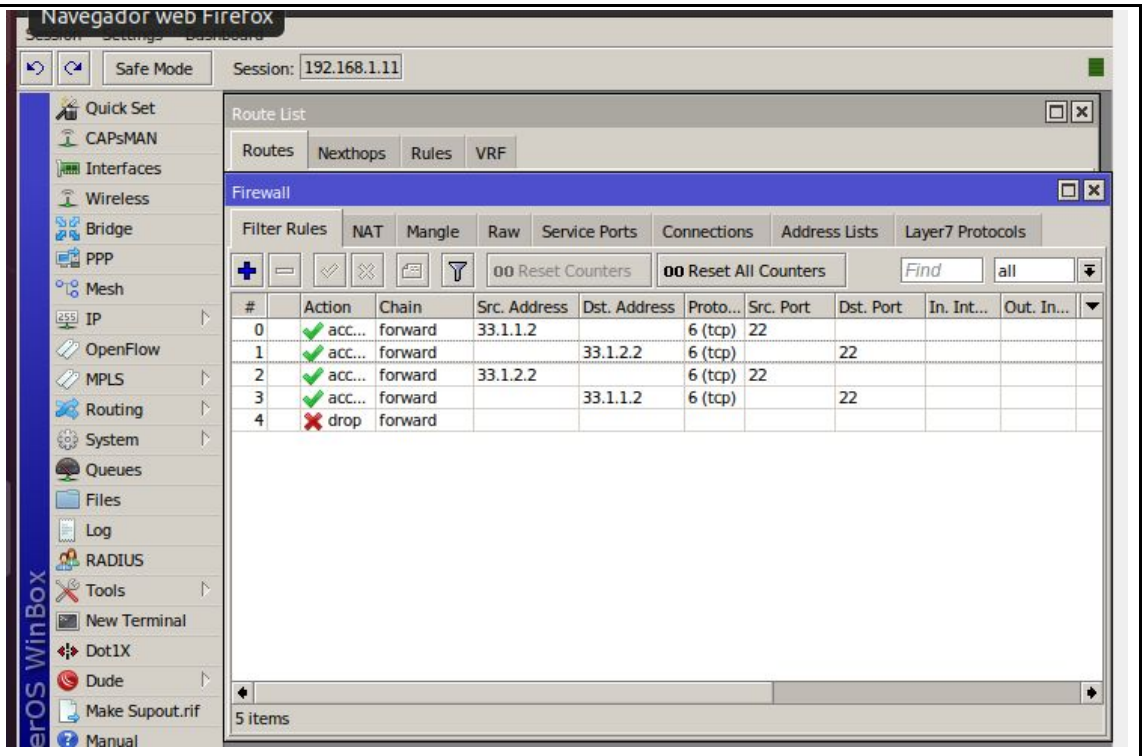


2) A continuación, configure el cortafuegos de R1_1 para que permita a otros ordenadores conectarse únicamente al servidor de SSH del PC_2.

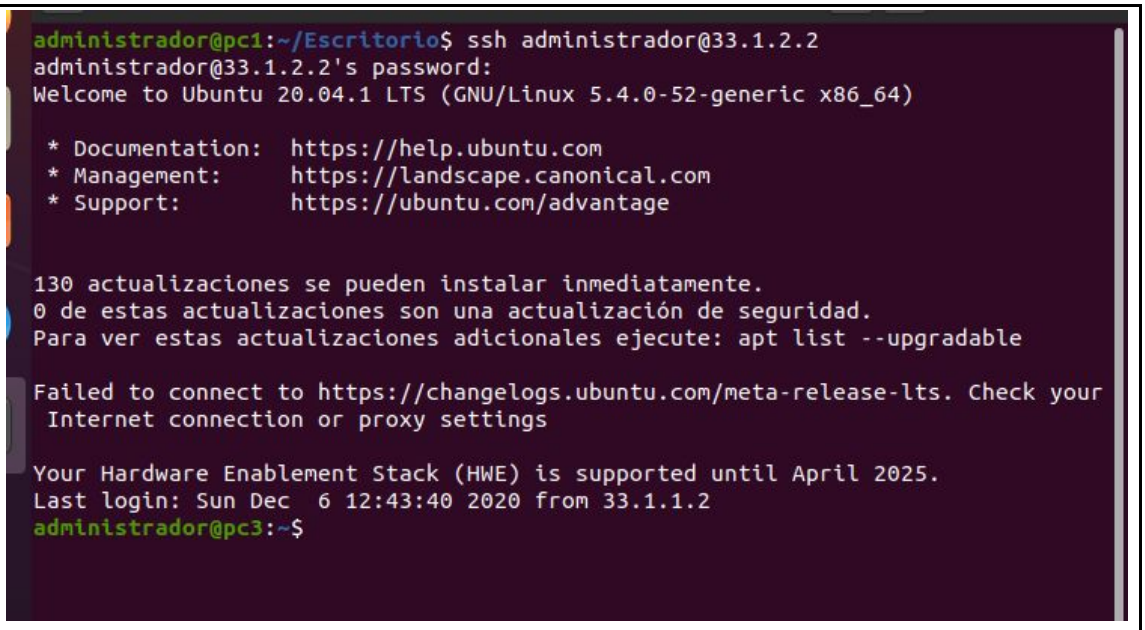
Una vez activado el firewall, no deberíamos poder conectarnos del PC1 al PC3. Lo comprobamos:



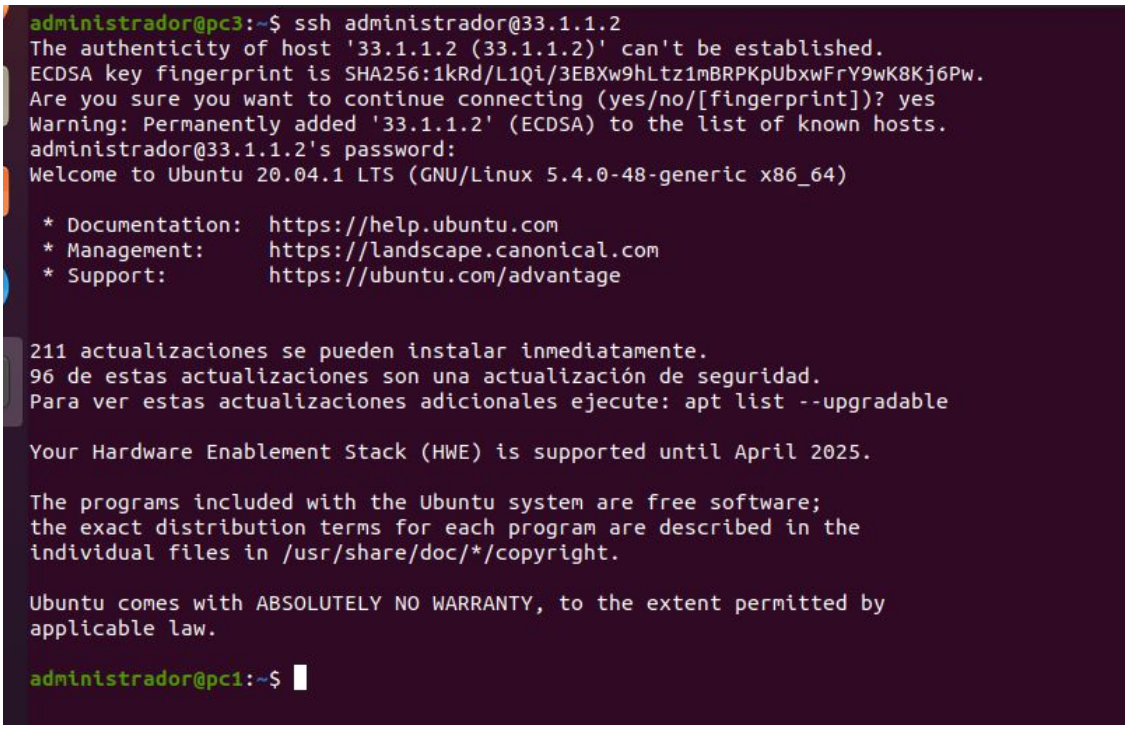
Para que podamos conectarnos del PC1 al PC3 y del PC3 al PC1. Especificamos al firewall las conexiones que queremos que se establezcan. Para conectarnos del PC1 al PC3, utilizamos 2 primeras reglas. Para establecer la conexión del PC3 al PC1, utilizamos las 2 siguientes. Es importante que el drop esté al final, de otro modo no funcionará.



Comprobamos que nos podemos conectar desde el PC1 al PC3 mediante ssh

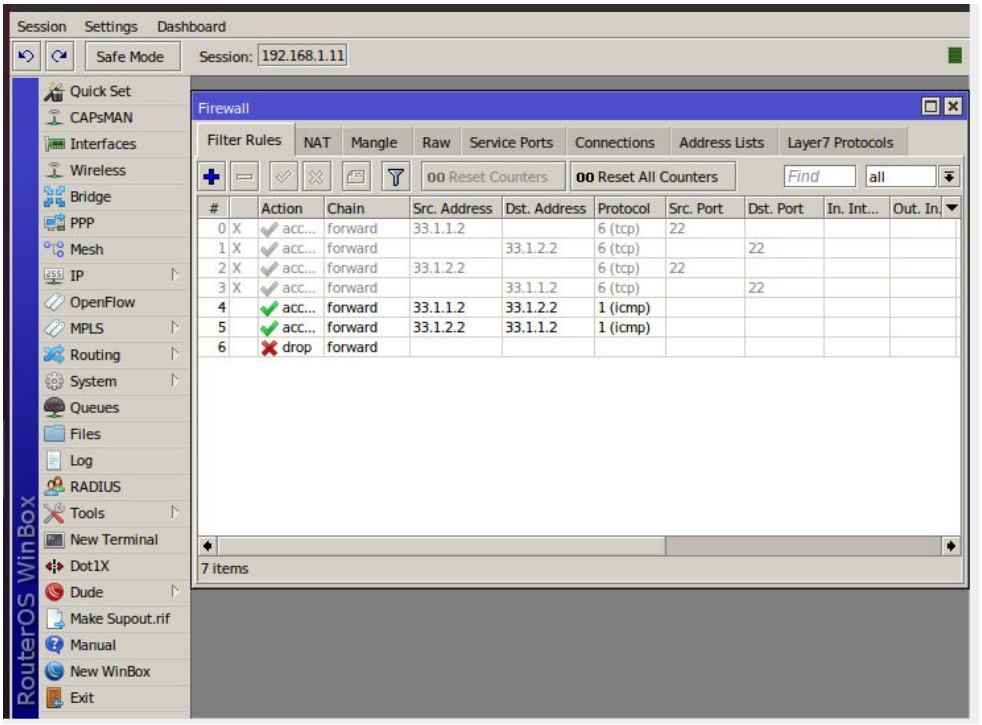


Vemos que también nos podemos conectar desde el PC3 al PC1.

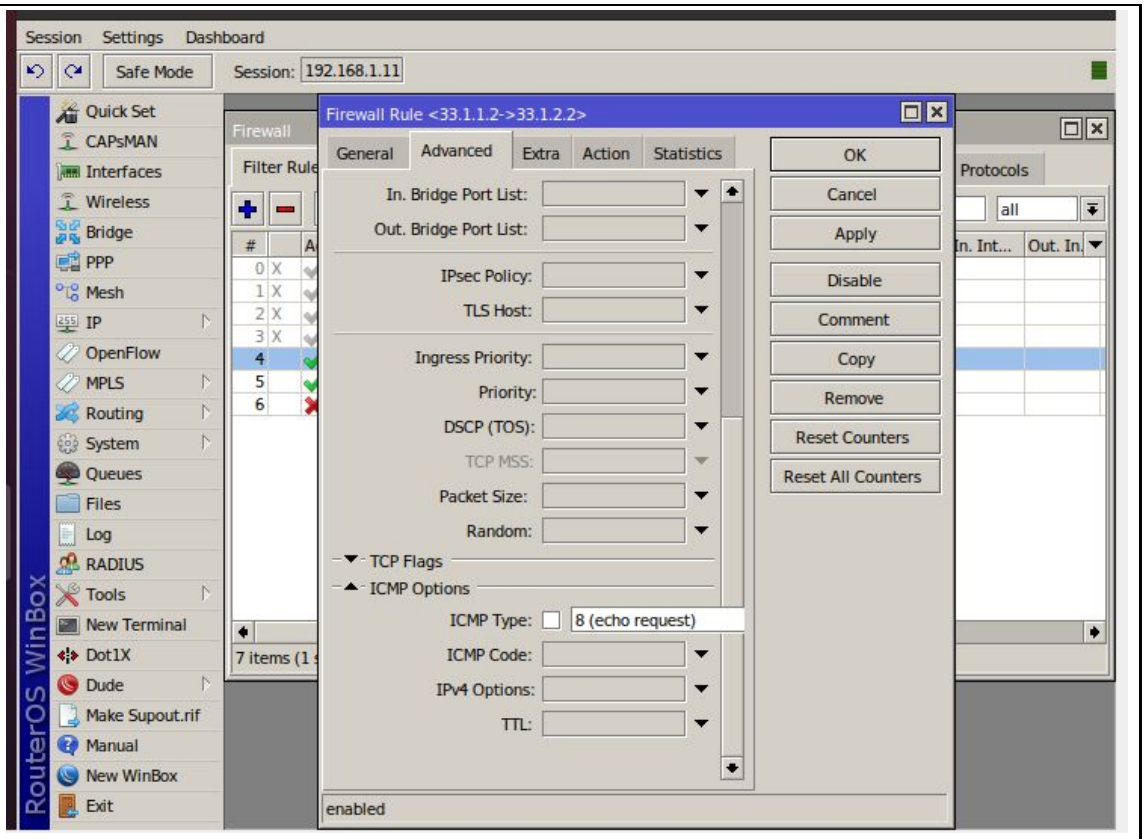


3) (Opcional) Configure el mismo *router* para que permita hacer ping de un ordenador a otro, pero no en sentido contrario.

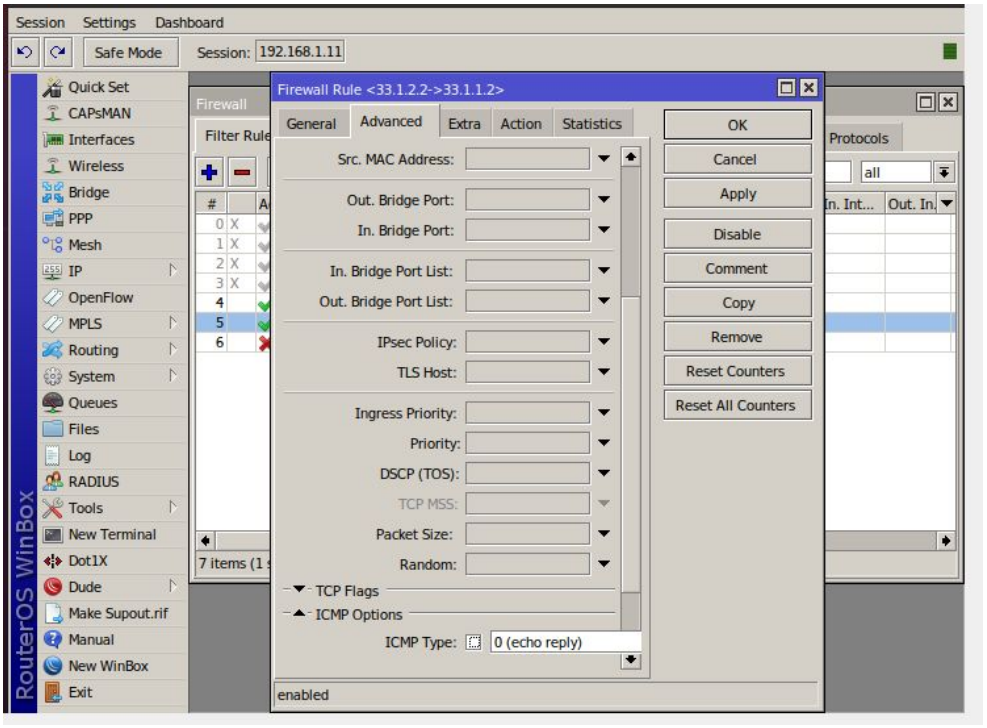
Ahora, queremos que haya conexión del PC1 al PC3 pero no al revés. Para ello, creamos una regla que nos acepte la conexión del PC1 al PC3 con protocolo icmp y otra que acepte la conexión del PC3 al PC1 con el mismo protocolo. Aquí podemos verlo.



Abrimos la regla que establece la conexión de PC1 al PC3, nos vamos a Advanced->ICMP Options->ICMP Type y la cambiamos a 8(echo request). Con esto, podremos hacer ping desde esta dirección.



A continuación, tenemos que impedir la conexión del PC3 al PC1. Para ello, abrimos la regla que conecta PC3 con PC1, nos vamos a Advanced->ICMP Options->ICMP Type y comprobamos que está puesto '0 (echo reply)'. Con esto conseguimos que no se pueda hacer ping desde PC3 al PC1.



Así conseguimos hacer ping a PC3 pero impedir que nos hagan una petición. Seguimos teniendo activada la regla drop para impedir peticiones de conexiones no deseadas.

Comprobamos que podemos conectarnos del PC1 al PC3:

```
administrador@pc1:~/Escritorio$ ping 33.1.2.2
PING 33.1.2.2 (33.1.2.2) 56(84) bytes of data.
64 bytes from 33.1.2.2: icmp_seq=1 ttl=62 time=5.69 ms
64 bytes from 33.1.2.2: icmp_seq=2 ttl=62 time=1.67 ms
64 bytes from 33.1.2.2: icmp_seq=3 ttl=62 time=0.991 ms
64 bytes from 33.1.2.2: icmp_seq=4 ttl=62 time=8.26 ms
^C
--- 33.1.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.991/4.151/8.260/2.974 ms
administrador@pc1:~/Escritorio$
```

Pero no podemos conectarnos del PC3 al PC1:

```
administrador@pc3:~$ ping 33.1.1.2
PING 33.1.1.2 (33.1.1.2) 56(84) bytes of data.
^C
--- 33.1.1.2 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4103ms

administrador@pc3:~$
```