



Universidad de Granada

Fundamentos de Redes

3º del Grado en Ingeniería  
Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

## Práctica 3 – Configuración de Red I y II

(0.375 puntos + 0.375 puntos)

Santiago Muñoz Castro y Raúl Castro Moreno

---

### 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.

*En el dispositivo **PC\_1** , al realizar el comando **ip address**, nos proporciona la siguiente información sobre las direcciones IP e interfaces.*



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería

#### Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

```
administrador@pci:~$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt 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 g
roup default qlen 1000
    link/ether 08:00:27:fd:98:cc brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 84801sec preferred_lft 84801sec
    inet6 fe80::3d00:5458:c3ab:e588/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:e6:cd:3c brd ff:ff:ff:ff:ff:ff
    inet 33.1.1.2/24 brd 33.1.1.255 scope global noprefixroute enp0s9
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee6:cd3c/64 scope link
        valid_lft forever preferred_lft forever
4: enp0s10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:e7:b1:dc brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/16 brd 192.168.255.255 scope global noprefixroute enp0s10
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee7:b1dc/64 scope link
        valid_lft forever preferred_lft forever
administrador@pci:~$
```

Se puede observar que tenemos las direcciones IP de **192.168.1.1** , **33.1.1.2** y la **10.0.2.15**( y aparte la de loopback) . Las dos primeras mencionadas son las que nos interesan y aparecen en la **Figura 1**, que corresponden a las interfaces de gestión y datos respectivamente. Puesto que la última no es necesaria, la vamos a deshabilitar con el comando **ifconfig enp0s3 down** .



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería

#### Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

```
root@pc1: /home/administrador
root@pc1:/home/administrador# ifconfig enp0s3 down
root@pc1:/home/administrador# ip address
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> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 08:00:27:fd:98:cc brd ff:ff:ff:ff:ff:ff
3: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e6:cd:3c brd ff:ff:ff:ff:ff:ff
    inet 33.1.1.2/24 brd 33.1.1.255 scope global noprefixroute enp0s9
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee6:cd3c/64 scope link
        valid_lft forever preferred_lft forever
4: enp0s10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e7:b1:dc brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/16 brd 192.168.255.255 scope global noprefixroute enp0s10
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee7:b1dc/64 scope link
        valid_lft forever preferred_lft forever
root@pc1:/home/administrador#
```

#### PC\_1:

- enp0s9**, la cual su dirección de red definida es “**33.1.1.2**”. Está en la red de **datos**.
- enp0s10**, la cual su dirección de red definida es “**192.168.1.1**”. Está en la red de **gestión**.
- lo**: Se refiere a loopback, que es una interfaz de red especial que el sistema utiliza para referirse a él mismo la cual su dirección de red definida es “**127.0.0.1**”.

*Ahora vamos a realizar lo mismo con el **PC\_3**.*



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería

#### Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

```
root@pc3: /home/administrador
root@pc3:/home/administrador# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt 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 g
roup default qlen 1000
    link/ether 08:00:27:1c:df:88 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86269sec preferred_lft 86269sec
    inet6 fe80::175c:b708:4d5b:2f40/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:90:26:54 brd ff:ff:ff:ff:ff:ff
    inet 33.1.2.2/24 brd 33.1.2.255 scope global noprefixroute enp0s9
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe90:2654/64 scope link
        valid_lft forever preferred_lft forever
4: enp0s10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:21:ae:1b brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/16 brd 192.168.255.255 scope global noprefixroute enp0s10
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe21:ae1b/64 scope link
        valid_lft forever preferred_lft forever
```

Se puede observar que tenemos las direcciones IP de **192.168.1.3** , **33.1.2.2** y la **10.0.2.15**( y aparte la de loopback) . Al igual que en el PC\_1, realizamos lo mismo: **ifconfig enp0s3 down** .





Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería

#### Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

```
root@pc3: /home/administrador
root@pc3:/home/administrador# ifconfig enp0s3 down
root@pc3:/home/administrador# ip address
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> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 08:00:27:1c:df:88 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86109sec preferred_lft 86109sec
3: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:90:26:54 brd ff:ff:ff:ff:ff:ff
    inet 33.1.2.2/24 brd 33.1.2.255 scope global noprefixroute enp0s9
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe90:2654/64 scope link
        valid_lft forever preferred_lft forever
4: enp0s10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:21:ae:1b brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/16 brd 192.168.255.255 scope global noprefixroute enp0s10
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe21:ae1b/64 scope link
        valid_lft forever preferred_lft forever
root@pc3:/home/administrador#
```

#### PC\_3:

-**enp0s9**, la cual su dirección de red definida es “**33.1.2.2**”. Está en la red de **datos**.

-**enp0s10**, la cual su dirección de red definida es “**192.168.1.3**”. Está en la red de **gestión**.

-**lo**: Se refiere a loopback, que es una interfaz de red especial que el sistema utiliza para referirse a él mismo la cual su dirección de red definida es “**127.0.0.1**”.

*Ahora vamos a comprobar los routers. Empezamos con el router **R1\_1**. Vamos a seguir los siguientes pasos para obtener sus distintas direcciones IP y nombre de interfaces.*

*Hay que saber que si pulsamos la tecla **TAB**, obtenemos los distintos directorios(en azul) y comandos (en morado) admitidos en el directorio actual.*

```
[admin@R11] >
caps-man  dude      ipv6      port      routing   tool      import    redo
certificate file      log       ppp       snmp      user      password  undo
console   interface mpls     queue    special-login beep      ping
disk      ip        openflow radius    system    export    quit
```



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería

#### Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

De aquí queremos ir al directorio ip, por lo que ponemos **ip** y pulsamos “**enter**” para viajar a dicho sitio.

```
[admin@R11] > ip
[admin@R11] /ip>
accounting  dhcp-client  firewall      neighbor     route        socks         upnp
address     dhcp-relay   hotspot      packing      service      ssh           export
arp         dhcp-server  ipsec        pool         settings     tftp
cloud       dns          kid-control  proxy        smb          traffic-flow
```

Una vez en ip hacemos lo mismo que antes pero ponemos **address**.

```
[admin@R11] /ip> address
[admin@R11] /ip address>
add comment disable edit enable export find print remove set
```

Este directorio solo tiene comandos, del cual vamos a usar el de **print** para que nos muestre toda la información que buscamos.

```
[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
```

Podemos observar que aparecen las 4 direcciones de IP que salen en la Figura 1, por lo que no deshabilitamos ninguna.

#### R1\_1:

- ether2** ,la cual su dirección de red definida es “**33.1.1.1**”. Está en la red de **datos**.
- ether3** ,la cual su dirección de red definida es “**192.168.1.11**”. Está en la red de **gestión**.
- ether4** ,la cual su dirección de red definida es “**172.16.1.1**”. Está en la red de **datos** y en la **datosubred1**.
- ether1** ,la cual su dirección de red definida es “**172.17.1.1**”. Está en la red de **datos** y en la **datosubred2**.

*Repetimos los mismos pasos para los demás routers :*



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería

#### Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

R1\_2:

```
[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
[admin@R12] /ip address>
```

*Al igual que antes, se puede observar que aparecen las 4 direcciones de IP que salen en la Figura 1, por lo que no deshabilitamos ninguna.*

R1\_2:

- ether2 ,la cual su dirección de red definida es “33.1.2.1”. Está en la red de **datos**.
- ether3 ,la cual su dirección de red definida es “192.168.1.12”. Está en la red de **gestión**.
- ether4 ,la cual su dirección de red definida es “172.16.1.2”. Está en la red de **datos** y en la **datosubred1**.
- ether1 ,la cual su dirección de red definida es “172.18.1.2”. Está en la red de **datos** y en la **datosubred3**.

R1\_4:

```
[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
```

*Finalmente, comprobamos que aparecen las 4 direcciones de IP que salen en la Figura 1, por lo que no deshabilitamos ninguna.*

R1\_4:

- ether1 ,la cual su dirección de red definida es “172.17.1.4”. Está en la red de **datos** y en la **datosubred2**.
- ether3 ,la cual su dirección de red definida es “192.168.1.14”. Está en la red de **gestión**.
- ether4 ,la cual su dirección de red definida es “172.18.1.4”. Está en la red de **datos** y en la **datosubred3**.



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería

#### Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

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 `tracert`, y anote los resultados.

*Para introducir las entradas de encaminamiento necesarias para comunicar PC\_1 y PC\_3 vamos a utilizar winbox.*

*Primero abrimos Winbox mediante wine( para poder ejecutar aplicaciones de windows en Linux), y se nos abre la siguiente ventana.*

```
root@pc1:/home/administrador# wine Descargas/winbox64.exe
creating Window Class routers_null
creating Window Class routers_connect
DPI=96
EMS=13
ERROR: bad bmp format id=2329
biPlanes=1, biBitCount=1, biCompression=0
ERROR: bad bmp format id=3329
biPlanes=1, biBitCount=1, biCompression=0
creating Window Class routers_dbl_canvas
rescaledDPI starting-dpi=96, zoom=0 result=96
  discovery started
rescaning
connecting to 127.255.255.255
connecting to 33.1.1.255
connecting to 192.168.255.255
sendto old: No such file or directory
loadConfig C:\users\root\Application Data\Mikrotik\Winbox\Addresses.cdb
□
```





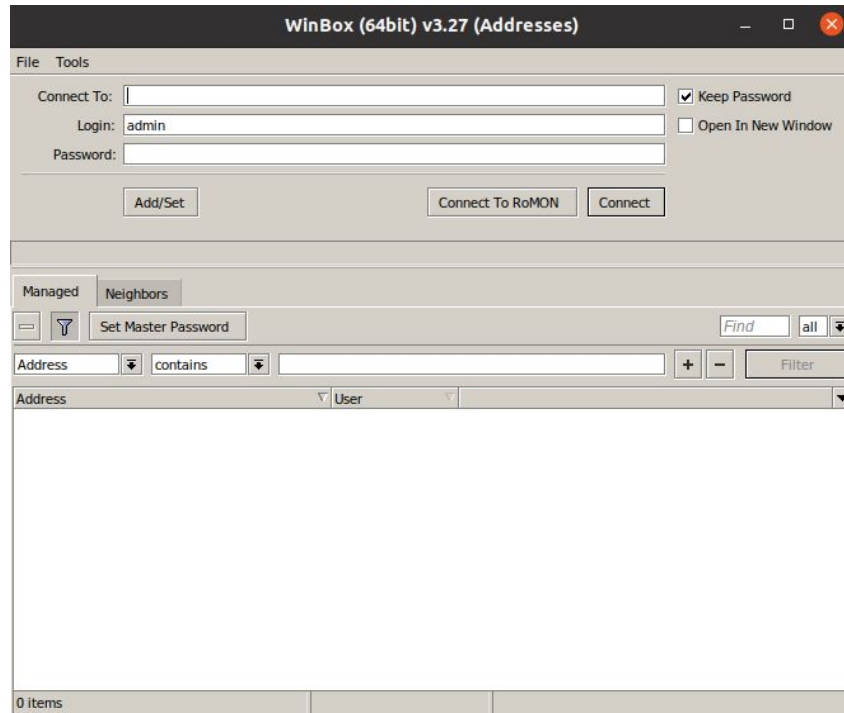
Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones



*Una vez en WinBox, vamos a la pestañita de Neighbors y seleccionamos el router R1\_1 por la red de datos( es decir, la que tiene la dirección ip correspondiente en la red de datos, y no de gestión). Ponemos en connect to, la dirección MAC o la dirección IP de esa interfaz de red, y el usuario y contraseña del R1\_1 ( no tienen contraseña los routers que estamos utilizando ),y presionamos Connect.*



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

WinBox (64bit) v3.27 (Addresses)

File Tools

Connect To: 08:00:27:14:49:CB ☒ Keep Password

Login: admin ☐ Open In New Window

Password:

Add/Set Connect To RoMON Connect

Managed Neighbors

Refresh Find all

MAC Address	IP Address	Identity	Version	Board	Uptime
08:00:27:01:79:56	192.168.1.14	R14	6.46.7 (lo...	CHR	00:42:47
08:00:27:14:49:CB	33.1.1.1	R11	6.46.7 (lo...	CHR	02:13:04
08:00:27:53:61:E1	192.168.1.12	R12	6.46.7 (lo...	CHR	00:50:41
08:00:27:F0:F4:DD	192.168.1.11	R11	6.46.7 (lo...	CHR	02:13:04

Dentro de la conexión, en el menú de la izquierda, vamos a IP, y seleccionamos Routes.

admin@08:00:27:14:49:CB (R11) - WinBox (64bit) v6.46.7 on CHR (x86\_64)

Session Settings Dashboard

Safe Mode Session: 08:00:27:14:49:CB

RouterOS WinBox

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Mesh
- IP
  - ARP
  - Accounting
  - Addresses
  - Cloud
  - DHCP Client
  - DHCP Relay
  - DHCP Server
  - DNS
  - Firewall
  - Hotspot
  - IPsec
  - Kid Control
  - Neighbors
  - Packing
  - Pool
  - Routes
  - SMB
  - SNMP
  - Services
  - Settings
  - Socks
  - TFTP
  - Traffic Flow
  - UPnP
  - Web Proxy
- OpenFlow
- MPLS
- Routing
- System
- Queues
- Files
- Log
- RADIUS
- Tools
- New Terminal
- Dot1X
- Dude
- Make Supout.rif
- More



Universidad de Granada

## Fundamentos de Redes

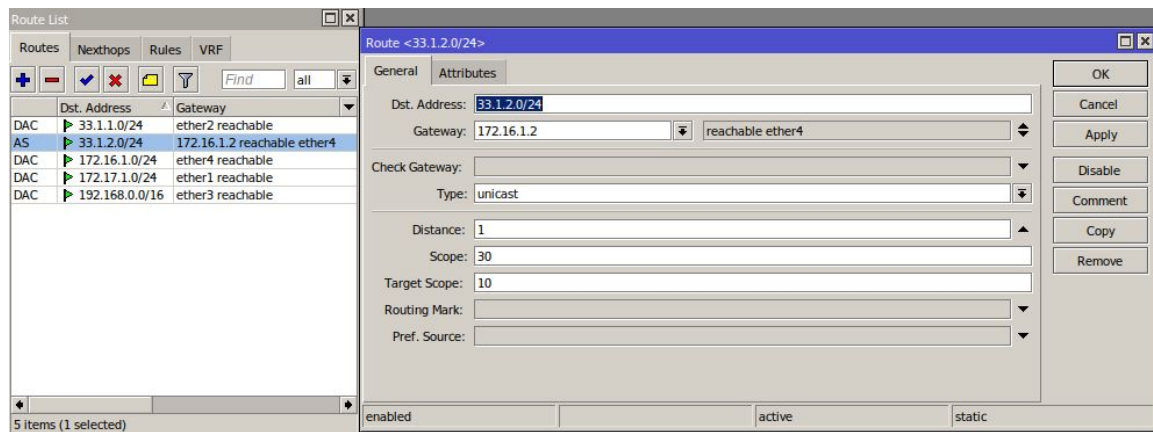
### 3º del Grado en Ingeniería

#### Informática

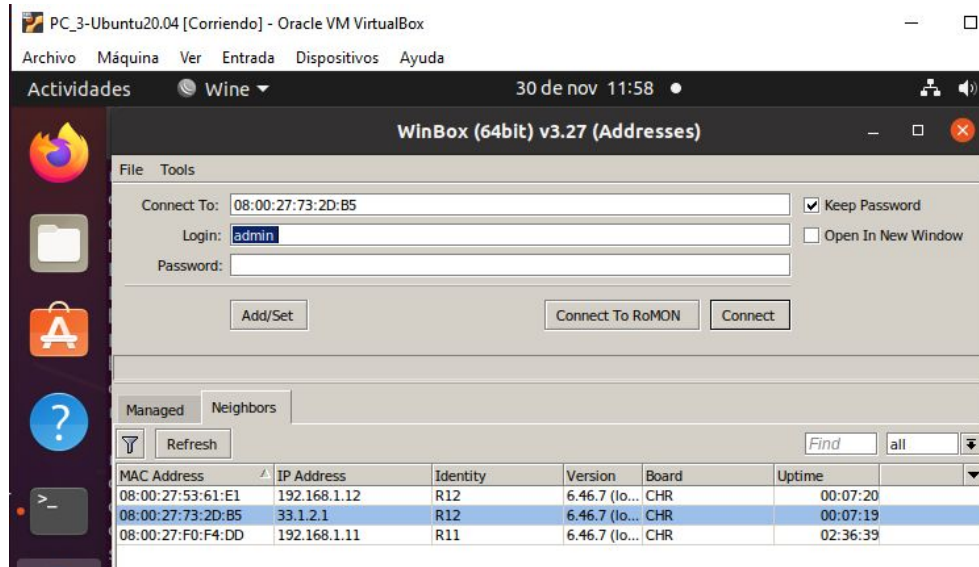


Dept. Teoría de la Señal,  
Telemática y Comunicaciones

En el siguiente menú, pulsamos el símbolo “+” azul para poder añadir un nuevo encaminamiento. En la siguiente pestaña que se nos abre, escribimos la dirección IP de destino (red de datos del PC\_3) y la gateway (R1\_2), para aplicar los cambios pulsamos el botón “OK”.



Realizamos los mismos pasos para el R1\_2, poniendo la dirección de destino IP, la de la red de datos del PC\_1, y la gateway del R1\_1, quedando al final así.





Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

Route List				
Routes				
Nexthops Rules VRF				
Find all				
	Dst. Address	Gateway	Distance	Routing Mar
AS	33.1.1.0/24	172.16.1.1 reachable ether4	1	
DAC	33.1.2.0/24	ether2 reachable	0	
DAC	172.16.1.0/24	ether4 reachable	0	
DAC	172.18.1.0/24	ether1 reachable	0	
DAC	192.168.0.0/16	ether3 reachable	0	

Route <33.1.1.0/24>	
General Attributes	
Dst. Address:	33.1.1.0/24
Gateway:	172.16.1.1 reachable ether4
Check Gateway:	
Type:	unicast
Distance:	1
Scope:	30
enabled	active static

Ahora, antes de probar la funcionalidad de **ping** o **traceroute**, debemos añadir las pasarelas por defecto en las tablas de enrutamiento de los PC para que vayan al router al que están conectados.

```
root@pc1:/home/administrador# route add default gw 33.1.1.1
root@pc1:/home/administrador#
```

```
root@pc3:/home/administrador# route add default gw 33.1.2.1
root@pc3:/home/administrador#
```





Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería

#### Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

*Finalmente comprobamos que funciona utilizando ping tanto desde PC\_1 a PC\_3, como desde PC\_3 a PC\_1.*

```
root@pc1:/home/administrador# route add default gw 33.1.1.1
root@pc1:/home/administrador# 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=1.85 ms
64 bytes from 33.1.2.2: icmp_seq=2 ttl=62 time=1.07 ms
64 bytes from 33.1.2.2: icmp_seq=3 ttl=62 time=1.29 ms
64 bytes from 33.1.2.2: icmp_seq=4 ttl=62 time=1.27 ms
64 bytes from 33.1.2.2: icmp_seq=5 ttl=62 time=1.17 ms
64 bytes from 33.1.2.2: icmp_seq=6 ttl=62 time=1.36 ms
64 bytes from 33.1.2.2: icmp_seq=7 ttl=62 time=1.08 ms
64 bytes from 33.1.2.2: icmp_seq=8 ttl=62 time=1.13 ms
64 bytes from 33.1.2.2: icmp_seq=9 ttl=62 time=0.863 ms
^C
--- 33.1.2.2 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8013ms
rtt min/avg/max/mdev = 0.863/1.231/1.851/0.258 ms
```

```
root@pc3:/home/administrador# ping 33.1.1.2
PING 33.1.1.2 (33.1.1.2) 56(84) bytes of data.
64 bytes from 33.1.1.2: icmp_seq=1 ttl=62 time=1.10 ms
64 bytes from 33.1.1.2: icmp_seq=2 ttl=62 time=1.18 ms
64 bytes from 33.1.1.2: icmp_seq=3 ttl=62 time=1.09 ms
64 bytes from 33.1.1.2: icmp_seq=4 ttl=62 time=1.21 ms
64 bytes from 33.1.1.2: icmp_seq=5 ttl=62 time=1.19 ms
64 bytes from 33.1.1.2: icmp_seq=6 ttl=62 time=1.21 ms
64 bytes from 33.1.1.2: icmp_seq=7 ttl=62 time=1.27 ms
^C
--- 33.1.1.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6006ms
rtt min/avg/max/mdev = 1.086/1.177/1.268/0.059 ms
```

*Y ahora comprobamos lo que nos muestra traceroute de PC\_1 a PC\_3 y viceversa.*

```
root@pc1:/home/administrador# traceroute 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) 0.307 ms 0.282 ms 0.270 ms
 2 172.16.1.2 (172.16.1.2) 0.529 ms 0.519 ms 0.620 ms
 3 33.1.2.2 (33.1.2.2) 1.265 ms 1.255 ms 1.244 ms
root@pc1:/home/administrador#
```

```
root@pc3:/home/administrador# traceroute 33.1.1.2
traceroute to 33.1.1.2 (33.1.1.2), 30 hops max, 60 byte packets
 1 _gateway (33.1.2.1) 0.431 ms 0.407 ms 0.396 ms
 2 172.16.1.1 (172.16.1.1) 16.905 ms 16.884 ms 16.871 ms
 3 33.1.1.2 (33.1.1.2) 0.838 ms 0.829 ms 1.180 ms
root@pc3:/home/administrador#
```



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería

#### Informática



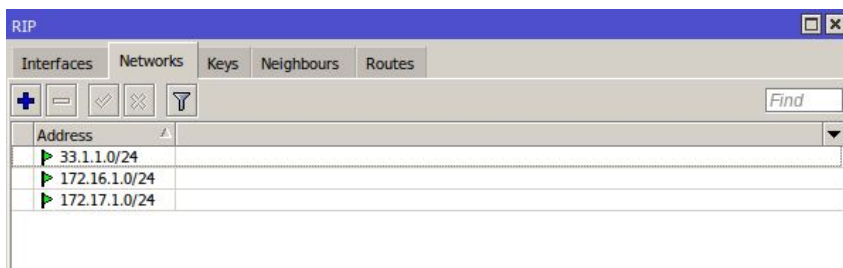
Dept. Teoría de la Señal,  
Telemática y Comunicaciones

3.

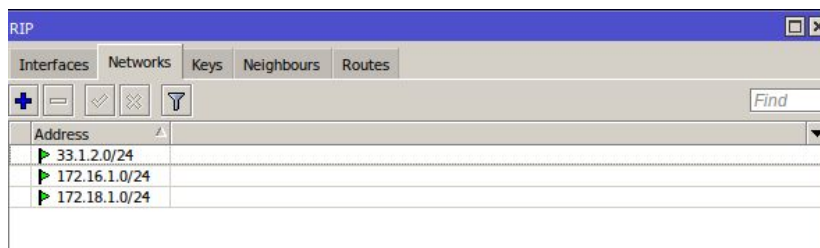
Configure RIP en todos y cada uno de los *routers*. Compruebe la tabla de encaminamiento tanto en el menú correspondiente en RIP como en el menú *IP->Routes*. ¿Tiene sentido lo que observa? Corroborarlo mediante la comprobación de la conectividad y saltos entre PC\_1 y PC\_3 con las utilidades `ping` y `traceroute` y anote los resultados.

Vamos en el WinBox en cada router vamos a la pestaña **Routing->RIP**, y en la ventana que se nos abre, en la pestaña **Networks**, añadimos todas las interfaces de redes que tenga cada router.

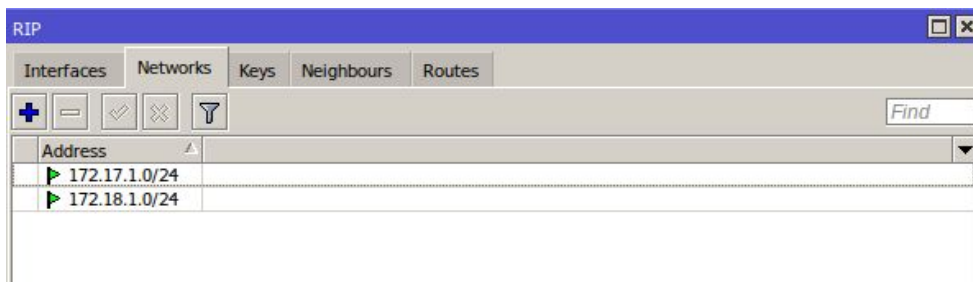
En R1\_1



En R1\_2



En R1\_4





Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería

#### Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

*Y como podemos observar tanto desde el PC\_1 al PC\_3 y viceversa, la configuración RIP elige la ruta más corta (con menos saltos).*

```
root@pc1:/home/administrador# traceroute 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)  0.744 ms  0.714 ms  0.705 ms
 2 172.16.1.2 (172.16.1.2)  1.437 ms  1.432 ms  1.425 ms
 3 33.1.2.2 (33.1.2.2)  2.195 ms  2.150 ms  2.139 ms
root@pc1:/home/administrador#
```

```
root@pc3:/home/administrador# traceroute 33.1.1.2
traceroute to 33.1.1.2 (33.1.1.2), 30 hops max, 60 byte packets
 1 _gateway (33.1.2.1)  0.394 ms  0.376 ms  0.364 ms
 2 172.16.1.1 (172.16.1.1)  0.717 ms  0.710 ms  0.696 ms
 3 33.1.1.2 (33.1.1.2)  1.011 ms  0.999 ms  0.988 ms
```



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería

#### Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

4.

Deshabilite la interfaz de R1\_1 que conecta con la red 172.16.1.0/24 y compruebe 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.

*Para deshabilitar la interfaz 172.16.1.0/24, vamos en el WinBox al menú IP->Addresses, seleccionamos la red y pulsamos la "X" para deshabilitarla.*

Address List			
<div><div><div></div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div><div></div></div></div> <div>Find</div>			
	Address	Network	Interface
	<div></div> 33.1.1.1/24	33.1.1.0	ether2
X	172.16.1.1/24	172.16.1.0	ether4
	<div></div> 172.17.1.1/24	172.17.1.0	ether1
	<div></div> 192.168.1.11/16	192.168.0.0	ether3

*Una vez deshabilitada, probamos el comando `traceroute` para ir de PC\_1 a PC\_3 y viceversa.*

```
root@pc1:/home/administrador# traceroute 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)  0.364 ms  0.443 ms  0.531 ms
 2 172.17.1.4 (172.17.1.4)  1.094 ms  1.085 ms  1.032 ms
 3 172.18.1.2 (172.18.1.2)  1.015 ms  1.004 ms  0.992 ms
 4 33.1.2.2 (33.1.2.2)  1.263 ms  1.841 ms  1.793 ms
```





Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

```
root@pc3:/home/administrador# traceroute 33.1.1.2
traceroute to 33.1.1.2 (33.1.1.2), 30 hops max, 60 byte packets
 1  _gateway (33.1.2.1)  0.388 ms  0.367 ms  0.356 ms
 2  172.18.1.4 (172.18.1.4)  0.694 ms  0.686 ms  0.634 ms
 3  172.17.1.1 (172.17.1.1)  0.959 ms  0.951 ms  0.941 ms
 4  33.1.1.2 (33.1.1.2)  1.461 ms  1.455 ms  1.408 ms
```

*Se puede observar que el camino que toma es R1\_1 -> R1\_4 -> R1\_2. Esto es debido a que el encaminamiento dinámico que hace RIP, una vez ha perdido el camino más corto posible al deshabilitar la red, ha buscado el siguiente más corto (y en este caso el otro único camino posible que había).*



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería

#### Informática



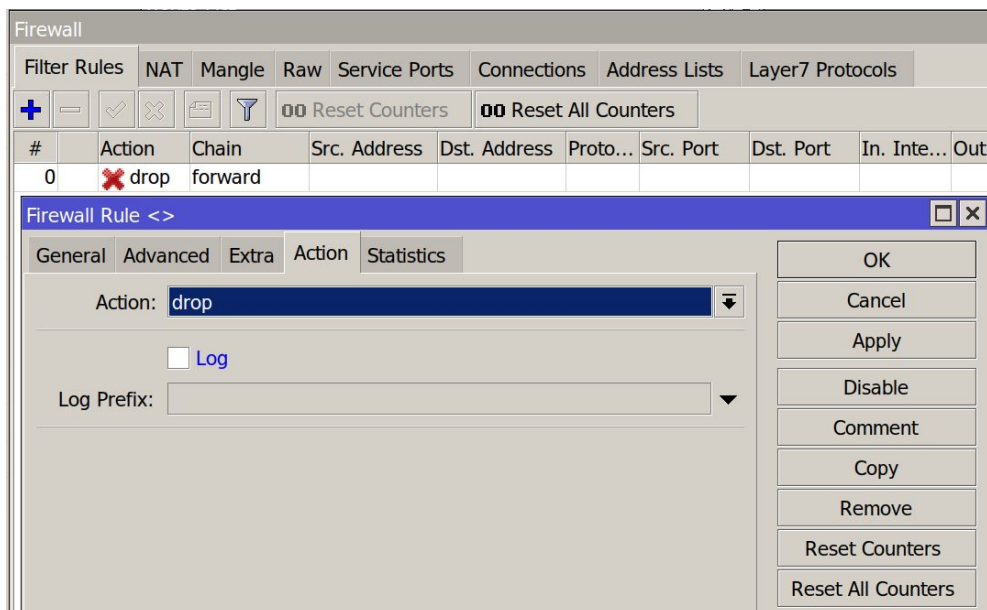
Dept. Teoría de la Señal,  
Telemática y Comunicaciones

## 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 si se desea dejar pasar. Compruebe que ahora no es posible establecer conexiones entre los PC.

*Primero nos conectamos a R1\_1 desde winbox, accedemos al firewall siguiendo en menú el siguiente camino: "IP->Firewall", una vez situados aquí añadimos un nuevo cortafuegos con chain "forward" para aplicar dicho firewall a aquellos paquetes que debe reenviar el router según sus tablas de encaminamiento. En la pestaña action elegimos la opción "drop" para descartar los paquetes que llegan al router R1\_1.*



*Aquí se puede observar que una vez establecido el firewall con la acción drop, descarta todos los paquetes y no nos permite conectarnos con el PC\_3.*

```
root@pc1:/home/administrador# ping 33.1.2.2
PING 33.1.2.2 (33.1.2.2) 56(84) bytes of data.
^C
--- 33.1.2.2 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4087ms
```



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería

#### Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

2.

A continuación, configure el cortafuegos de R1\_1 para que permita a otros ordenadores conectarse únicamente al servidor de SSH del PC\_2.

*Para configurar el firewall de manera que conecten los ordenadores mediante SSH, tendremos que añadir **4 nuevas reglas** en las que todas tendrán como **Action un accept** y de **Chain un forward**. También, todas usan el protocolo **6(tcp)**. Ahora, a 2 de ellas les tendremos que poner la **dirección de origen del paquete y el puerto de origen** y a las otras 2, la **dirección de destino de los paquetes y el puerto de destino**. Puesto que vamos a usar SSH, en los puertos que tengamos que rellenar, **vamos a poner siempre el puerto 22**( ya que el protocolo SSH transporta sus mensajes sobre TCP y utiliza el puerto 22). Por último, debemos **arrastrar el drop hacia abajo del todo**, puesto que el orden de las reglas importa, y si estuviera arriba, no dejaría pasar ningún paquete por lo que las reglas que hemos establecido no serviría ninguna. En la siguiente imagen, se ve cómo tiene que quedar el firewall.*

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port
0	✓ acc...	forward	33.1.1.2		6 (tcp)	22	
1	✓ acc...	forward		33.1.2.2	6 (tcp)		22
2	✓ acc...	forward	33.1.2.2		6 (tcp)	22	
3	✓ acc...	forward		33.1.1.2	6 (tcp)		22
4	✗ drop	forward					

Por último podemos comprobar que solo podemos conectarnos a PC\_3 por ssh introduciendo el comando **“ssh administrador@33.1.2.2”**

```
root@pc1:/home/administrador# ssh administrador@33.1.2.2
administrador@33.1.2.2's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-48-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

133 actualizaciones se pueden instalar inmediatamente.
0 de estas actualizaciones son una actualización de seguridad.
Para ver estas actualizaciones adicionales ejecute: apt list --upgradable

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2025.
*** Es necesario reiniciar el sistema ***
Last login: Mon Nov 30 15:27:45 2020 from 33.1.1.2
administrador@pc3:~$
```



Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

3.

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

(Hemos deshabilitado lo realizado en el ejercicio 2 para realizar este ejercicio)

Vamos a crear 2 reglas, con **Action=accept** y **Chain=forward**, y las 2 con protocolo **1(ICMP)**. La primera será con la dirección IP del **PC\_1** como **origen** y la segunda, con **PC\_3** como **destino**. En estas 2 reglas deberemos ir a la pestaña de **Advanced**, y abajo del todo, **desplegar ICMP Options**, donde nos saldrá **ICMP Type**. Deberemos de **poner 8 (echo request)**, permitiendo así el ping desde el **PC\_1** al **PC\_3**.

▲ ICMP Options

ICMP Type: ☐ 8 (echo request) ▼

ICMP Code: ▼

IPv4 Options: ▼

TTL: ▼

Después de esto crearemos otras 2 más iguales que las anteriores, pero el **origen** en una será el **PC\_3** y el **destino** el **PC\_1**, y por último, en estas 2 reglas deberemos poner el **ICMP Type** con **0(echo reply)**, restringiendo así el uso del ping del **PC\_3** al **PC\_1**.

▲ ICMP Options

ICMP Type: ☐ 0 (echo reply) ▼

ICMP Code: ▼

IPv4 Options: ▼

TTL: ▼





Universidad de Granada

## Fundamentos de Redes

### 3º del Grado en Ingeniería

#### Informática



Dept. Teoría de la Señal,  
Telemática y Comunicaciones

*Finalmente debería quedarnos esto después de volver a desplazar el drop hacia el final, para que permita usar las reglas que acabamos de crear:*

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inte...
0	X acc...	forward	33.1.1.2		6 (tcp)	22		
1	X acc...	forward		33.1.2.2	6 (tcp)		22	
2	X acc...	forward	33.1.2.2		6 (tcp)	22		
3	X acc...	forward		33.1.1.2	6 (tcp)		22	
4	✓ acc...	forward	33.1.1.2		1 (ic...			
5	✓ acc...	forward		33.1.2.2	1 (ic...			
6	✓ acc...	forward	33.1.2.2		1 (ic...			
7	✓ acc...	forward		33.1.1.2	1 (ic...			
8	✗ drop	forward						

*Aquí podemos observar que el cortafuegos funciona correctamente, ya que nos permite hacer ping al PC\_3 pero desde este último no podemos hacer ping al PC\_1.*

```
root@pc1:/home/administrador# 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=1.12 ms
64 bytes from 33.1.2.2: icmp_seq=2 ttl=62 time=1.10 ms
64 bytes from 33.1.2.2: icmp_seq=3 ttl=62 time=1.15 ms
64 bytes from 33.1.2.2: icmp_seq=4 ttl=62 time=1.03 ms
64 bytes from 33.1.2.2: icmp_seq=5 ttl=62 time=1.22 ms
^C
--- 33.1.2.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.034/1.124/1.222/0.061 ms
root@pc1:/home/administrador#
```

```
root@pc3:/home/administrador# 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 ---
3 packets transmitted, 0 received, 100% packet loss, time 2039ms

root@pc3:/home/administrador#
```