Práctica 1.4. Protocolo IPv6

Objetivos

En esta práctica se estudian los aspectos básicos del protocolo IPv6, el manejo de los diferentes tipos de direcciones y mecanismos de configuración. Además se analizarán las características más importantes del protocolo ICMP versión 6.

Activar el **portapapeles bidireccional** (menú Dispositivos) en las máquinas virtuales.

Usar la opción de Virtualbox (menú Ver) para realizar **capturas de pantalla**.

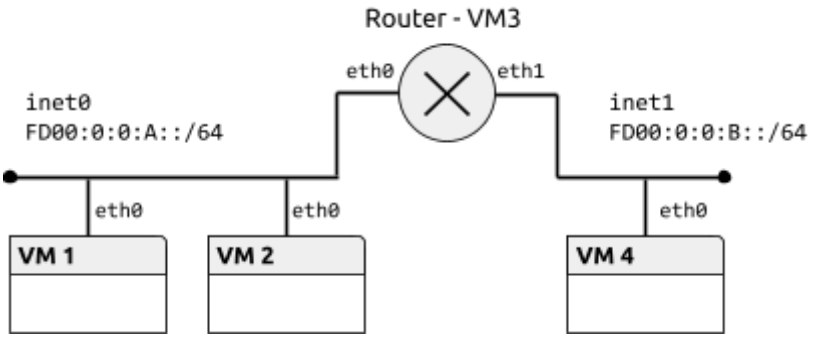
La **contraseña** del usuario `cursoredes` es `cursoredes`.

Contenidos

- Preparación del entorno para la práctica
- Direcciones de enlace local
- Direcciones ULA
- Encaminamiento estático
- Configuración persistente
- Autoconfiguración. Anuncio de prefijos
- ICMPv6

Preparación del entorno para la práctica

Configuraremos la topología de red que se muestra en la siguiente figura:



El fichero de configuración de la topología tendría el siguiente contenido:

```
netprefix inet
machine 1 0 0
machine 2 0 0
machine 3 0 0 1 1
machine 4 0 1
```

Direcciones de enlace local

Una dirección de enlace local es únicamente válida en la subred que está definida. Ningún encaminador dará salida a un datagrama con una dirección de enlace local como destino. El prefijo de formato para estas direcciones es `fe80::/10`.

Ejercicio 1 [VM1, VM2]. Activar el interfaz `eth0` en VM1 y VM2. Comprobar las direcciones de enlace local que tienen asignadas con el comando `ip`.

En VM1:

```
[cursoredes@localhost ~]$ 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:b7:a7:54 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::a00:27ff:feb7:a754/64 scope link
       valid_lft forever preferred_lft forever
```

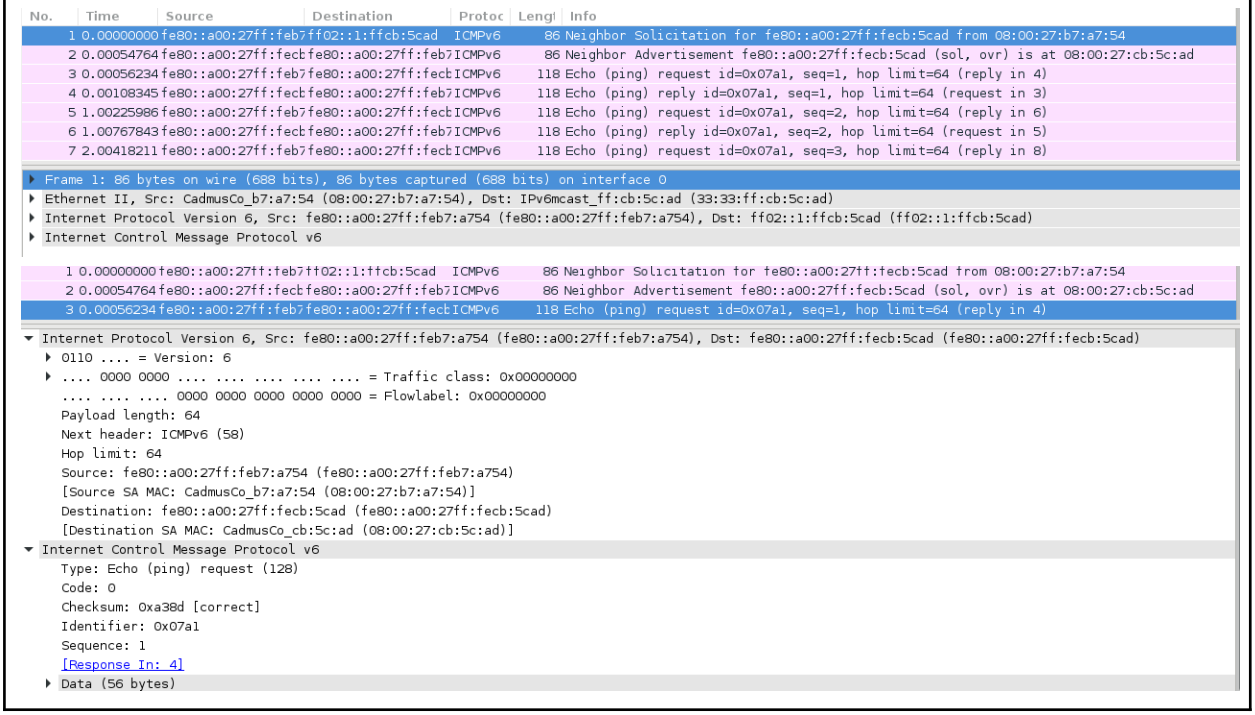
En VM2:

```
[cursoredes@localhost ~]$ 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:cb:5c:ad brd ff:ff:ff:ff:ff:ff
    inet6 fe80::a00:27ff:fecb:5cad/64 scope link
       valid_lft forever preferred_lft forever
```

Ejercicio 2 [VM1, VM2]. Comprobar la conectividad entre VM1 y VM2 con la orden `ping6` (o `ping -6`). Cuando se usan direcciones de enlace local, y **sólo en ese caso**, es necesario especificar el interfaz origen, añadiendo `%<nombre_interfaz>` a la dirección. Consultar las opciones del comando `ping6` en la página de manual. Observar el tráfico generado con Wireshark, especialmente los protocolos encapsulados en cada datagrama y los parámetros del protocolo IPv6.

En VM1:

```
[cursoredes@localhost ~]$ ping6 fe80::a00:27ff:fecb:5cad%eth0
```



Ejercicio 3 [Router, VM4]. Activar el interfaz de VM4 y los dos interfaces de Router. Comprobar la conectividad entre Router y VM1, y entre Router y VM4 usando la dirección de enlace local.

En VM3:

```
[cursoredes@localhost ~]$ 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
qlen 1000
   link/ether 08:00:27:0f:bf:73 brd ff:ff:ff:ff:ff:ff
   inet6 fe80::a00:27ff:fe0f:bf73/64 scope link
      valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
qlen 1000
   link/ether 08:00:27:d1:3b:c9 brd ff:ff:ff:ff:ff:ff
   inet6 fe80::a00:27ff:fed1:3bc9/64 scope link
      valid_lft forever preferred_lft forever
```

En VM4:
[cursoredes@localhost ~]$ ping6 -c 1 fe80::a00:27ff:fed1:3bc9%eth0
PING fe80::a00:27ff:fed1:3bc9%eth0(fe80::a00:27ff:fed1:3bc9%eth0) 56 data bytes
64 bytes from fe80::a00:27ff:fed1:3bc9%eth0: icmp_seq=1 ttl=64 time=0.442 ms

--- fe80::a00:27ff:fed1:3bc9%eth0 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.442/0.442/0.442/0.000 ms

En VM1:
[cursoredes@localhost ~]$ ping6 -c 1 fe80::a00:27ff:fe0f:bf73%eth0
PING fe80::a00:27ff:fe0f:bf73%eth0(fe80::a00:27ff:fe0f:bf73%eth0) 56 data bytes
64 bytes from fe80::a00:27ff:fe0f:bf73%eth0: icmp_seq=1 ttl=64 time=0.867 ms

--- fe80::a00:27ff:fe0f:bf73%eth0 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.867/0.867/0.867/0.000 ms

Para saber más... En el protocolo IPv4 también se reserva el bloque `169.254.0.0/16` para direcciones de enlace local, cuando no es posible la configuración de los interfaces por otras vías. Los detalles se describen en el RFC 3927.

Direcciones ULA

Una dirección ULA (*Unique Local Address*) puede usarse dentro de una organización, de forma que los encaminadores internos del sitio deben encaminar los datagramas con una dirección ULA como destino. El prefijo de formato para estas direcciones es `fc00::/7`.

Ejercicio 4 [VM1, VM2]. Configurar VM1 y VM2 para que tengan una dirección ULA en la red `fd00:0:0:a::/64` con el comando `ip`. La parte de identificador de interfaz puede elegirse libremente, siempre que no coincida para ambas máquinas. Incluir la longitud del prefijo al fijar las direcciones.

En VM1:
[cursoredes@localhost ~]$ sudo ip a add fd00:0:0:a::1/64 dev eth0
En VM2:
[cursoredes@localhost ~]$ sudo ip a add fd00:0:0:a::2/64 dev eth0

Ejercicio 5 [VM1, VM2]. Comprobar la conectividad entre VM1 y VM2 con la orden `ping6` usando la nueva dirección. Observar los mensajes intercambiados con Wireshark.

En VM1:

[cursoredes@localhost ~]$ ping6 -c 1 fd00:0:0:a::2

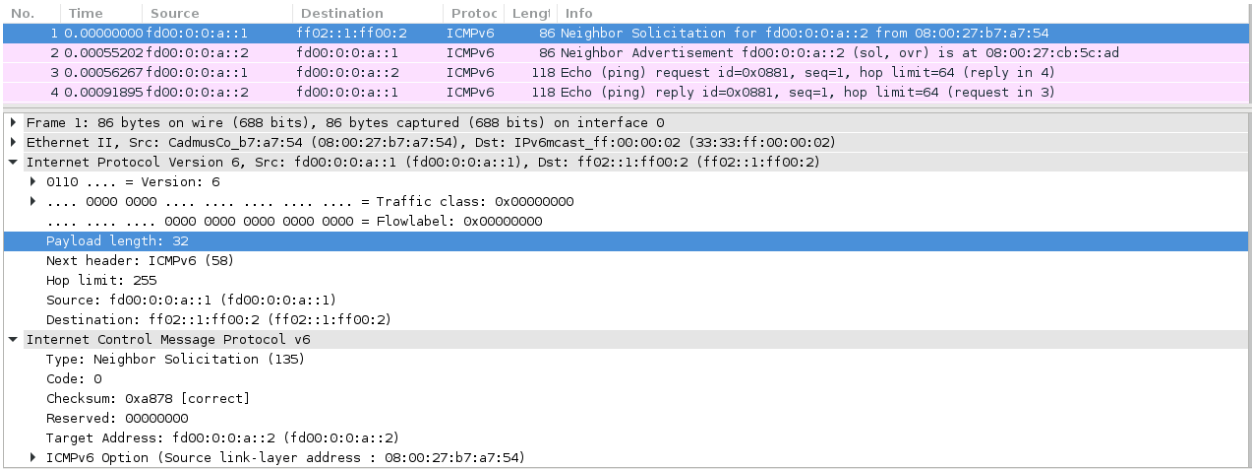
PING fd00:0:0:a::2(fd00:0:0:a::2) 56 data bytes

64 bytes from fd00:0:0:a::2: icmp_seq=1 ttl=64 time=0.941 ms

--- fd00:0:0:a::2 ping statistics ---

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 0.941/0.941/0.941/0.000 ms



Ejercicio 6 [Router, VM4]. Configurar direcciones ULA en los dos interfaces de Router (redes `fd00:0:0:a::/64` y `fd00:0:0:b::/64`) y en el de VM4 (red `fd00:0:0:b::/64`). Elegir el identificador de interfaz de forma que no coincida dentro de la misma red.

En VM3:
[cursoredes@localhost ~]$ sudo ip a add fd00:0:0:a::3/64 dev eth0
[cursoredes@localhost ~]$ sudo ip a add fd00:0:0:b::1/64 dev eth1

En VM4:
[cursoredes@localhost ~]$ sudo ip a add fd00:0:0:b::2/64 dev eth0

Ejercicio 7 [Router]. Comprobar la conectividad entre Router y VM1, y entre Router y VM4 usando direcciones ULA. Comprobar además que VM1 no puede alcanzar a VM4.

En VM1:
[cursoredes@localhost ~]$ ping6 -c 1 fd00:0:0:a::3
PING fd00:0:0:a::3(fd00:0:0:a::3) 56 data bytes
64 bytes from fd00:0:0:a::3: icmp_seq=1 ttl=64 time=0.904 ms

--- fd00:0:0:a::3 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.904/0.904/0.904/0.000 ms

[cursoredes@localhost ~]$ ping6 -c 1 fd00:0:0:b::2
connect: Network is unreachable

En VM4:
[cursoredes@localhost ~]$ ping6 -c 1 fd00:0:0:b::1
PING fd00:0:0:b::1(fd00:0:0:b::1) 56 data bytes
64 bytes from fd00:0:0:b::1: icmp_seq=1 ttl=64 time=1.00 ms

--- fd00:0:0:b::1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.007/1.007/1.007/0.000 ms

Encaminamiento estático

Según la topología que hemos configurado en esta práctica, Router debe encaminar el tráfico entre las redes `fd00:0:0:a::/64` y `fd00:0:0:b::/64`. En esta sección vamos a configurar un encaminamiento estático basado en las rutas que fijaremos manualmente en todas las máquinas.

Ejercicio 8 [VM1, Router]. Consultar las tablas de rutas en VM1 y Router con el comando `ip route`. Consultar la página de manual del comando para seleccionar las rutas IPv6.

Ip -6 route

Ejercicio 9 [Router]. Para que Router actúe efectivamente como encaminador, hay que activar el reenvío de paquetes (*packet forwarding*). De forma temporal, se puede activar con el comando `sysctl -w net.ipv6.conf.all.forwarding=1`.

Ejercicio 10 [VM1, VM2, VM4]. Finalmente, hay que configurar la tabla de rutas en las máquinas virtuales. Añadir la dirección correspondiente de Router como ruta por defecto con el comando `ip route`. Comprobar la conectividad entre VM1 y VM4 usando el comando `ping6`.

En VM1 y VM2:
[cursoredes@localhost ~]$ sudo ip route add default via fd00:0:0:a::3
En VM4:
[cursoredes@localhost ~]$ sudo ip route add default via fd00:0:0:b::1

Ejercicio 11 [VM1, Router, VM4]. Abrir Wireshark en Router e iniciar dos capturas, una en cada interfaz de red. Borrar la tabla de vecinos en VM1 y Router (con `ip neigh flush dev <interfaz>`). Usar la orden `ping6` entre VM1 y VM4. Completar la siguiente tabla con todos los mensajes hasta el primer ICMP Echo Reply:

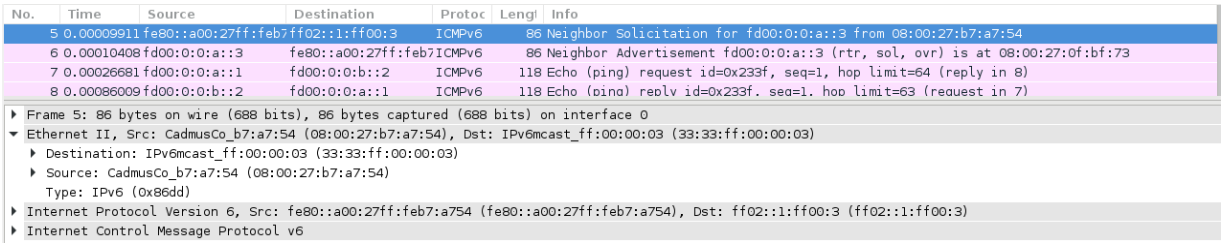
Red `fd00:0:0:a::/64` - Router (eth0)

MAC Origen	MAC Destino	IPv6 Origen	IPv6 Destino	ICMPv6 Tipo
08:00:27:b7:a7:54	33:33:ff:00:00:03	fe80::a00:27ff:feb7:a754	ff02::1:ff00:3	Neighbour solicitation
08:00:27:0f:bf:73	08:00:27:b7:a7:54	fd00:0:0:a::3	fe80::a00:27ff:feb7:a754	Neighbour advertisement
08:00:27:b7:a7:54	08:00:27:0f:bf:73	fd00:0:0:a::1	fd00:0:0:b::2	Echo request
08:00:27:0f:bf:73	08:00:27:b7:a7:54	fd00:0:0:b::2	fd00:0:0:a::1	Echo reply

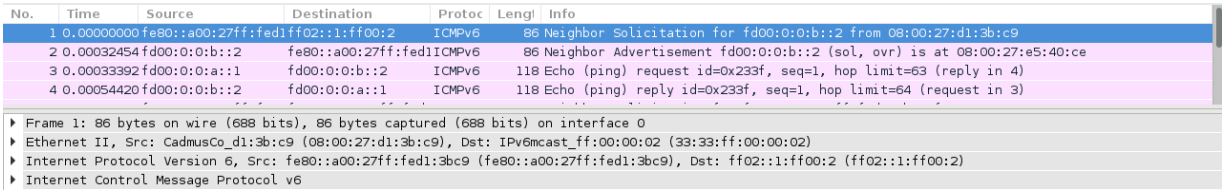
Red `fd00:0:0:b::/64` - Router (eth1)

MAC Origen	MAC Destino	IPv6 Origen	IPv6 Destino	ICMPv6 Tipo
08:00:27:d1:3b:c9	33:33:ff:00:00:02	fe80::a00:27ff:fed1:3bc9	ff02::1:ff00:2	Neighbour solicitation
08:00:27:e5:40:ce	08:00:27:d1:3b:c9	fd00:0:0:b::2	fe80::a00:27ff:fed1:3bc9	Neighbour advertisement
08:00:27:d1:3b:c9	08:00:27:e5:40:ce	fd00:0:0:a::1	fd00:0:0:b::2	Echo request
08:00:27:e5:40:ce	08:00:27:d1:3b:c9	fd00:0:0:b::2	fd00:0:0:a::1	Echo reply

Eth0:



Eth1:



Configuración persistente

Las configuraciones realizadas en los apartados anteriores son volátiles y desaparecen cuando se reinician las máquinas. Durante el arranque del sistema se pueden configurar automáticamente los interfaces según la información almacenada en el disco.

Ejercicio 12 [Router]. Crear los ficheros `ifcfg-eth0` e `ifcfg-eth1` en el directorio `/etc/sysconfig/network-scripts/` con la configuración de cada interfaz. Usar las siguientes opciones (descritas en `/usr/share/doc/initscripts-*/sysconfig.txt`):

```
TYPE=Ethernet
BOOTPROTO=none
IPV6ADDR=<dirección IP en formato CIDR>
IPV6_DEFAULTGW=<dirección IP del encaminador por defecto (en este caso, no tiene)>
DEVICE=<nombre del interfaz>
```

`/etc/sysconfig/network-scripts/ifcfg-eth0`

```
TYPE=Ethernet
BOOTPROTO=none
IPV6ADDR=fd00:0:0:a::3/64
DEVICE=eth0
```

```
/etc/sysconfig/network-scripts/ifcfg-eth1

TYPE=Ethernet
BOOTPROTO=none
IPV6ADDR=fd00:0:0:b::1/64
DEVICE=eth1
```

Ejercicio 13 [Router]. Comprobar la configuración persistente con las órdenes `ifup` e `ifdown`.

```
[cursoredes@localhost ~]$ sudo ifup eth0
RTNETLINK answers: File exists
ERROR    : [/etc/sysconfig/network-scripts/ifup-ipv6] Global IPv6 forwarding is disabled in
configuration, but not currently disabled in kernel
ERROR    : [/etc/sysconfig/network-scripts/ifup-ipv6] Please restart network with '/sbin/service
network restart'
[cursoredes@localhost ~]$ /sbin/service network restart
Restarting network (via systemctl):  ==== AUTHENTICATING FOR
org.freedesktop.systemd1.manage-units ===
Authentication is required to manage system services or units.
Authenticating as: cursoredes
Password:
==== AUTHENTICATION COMPLETE ===
^[[A^[[A                                   [  OK  ]
[cursoredes@localhost ~]$ sudo ifup eth0
RTNETLINK answers: File exists

[cursoredes@localhost ~]$ sudo ifup eth1
RTNETLINK answers: File exists
INFO     : [ipv6_wait_tentative] Waiting for interface eth1 IPv6 address(es) to leave the 'tentative'
state
INFO     : [ipv6_wait_tentative] Waiting for interface eth1 IPv6 address(es) to leave the 'tentative'
state
```

Autoconfiguración. Anuncio de prefijos

El protocolo de descubrimiento de vecinos se usa también para la autoconfiguración de los interfaces de red. Cuando se activa un interfaz, se envía un mensaje de descubrimiento de encaminadores. Los encaminadores presentes responden con un anuncio que contiene, entre otros, el prefijo de la red.

Ejercicio 14 [VM1, VM2, VM4]. Eliminar las direcciones ULA de los interfaces desactivándolos con `ip link`.

En VM1:

[cursoredes@localhost ~]$ sudo ip a del fd00:0:0:a::1/64 dev eth0

[cursoredes@localhost ~]$ sudo ip link set dev eth0 down

En VM2:

[cursoredes@localhost ~]$ sudo ip a del fd00:0:0:a::2/64 dev eth0

[cursoredes@localhost ~]$ sudo ip link set dev eth0 down

En VM4:

[cursoredes@localhost ~]$ sudo ip a del fd00:0:0:b::2/64 dev eth0

[cursoredes@localhost ~]$ sudo ip link set dev eth0 down

Ejercicio 15 [Router]. Configurar el servicio `zebra` para que el encaminador anuncie prefijos. Para ello, crear el archivo `/etc/quagga/zebra.conf` e incluir la información de los prefijos para las dos redes. Cada entrada será de la forma:

```
interface eth0
  no ipv6 nd suppress-ra
  ipv6 nd prefix fd00:0:0:a::/64

interface eth1
  no ipv6 nd suppress-ra
  ipv6 nd prefix fd00:0:0:b::/64
```

Finalmente, arrancar el servicio con el comando `service zebra start`.

Ejercicio 16 [VM4]. Comprobar la autoconfiguración del interfaz de red en VM4, volviendo a activar el interfaz y consultando la dirección asignada.

```
[cursoredes@localhost ~]$ sudo ip link set dev eth0 up
[cursoredes@localhost ~]$ 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
qlen 1000
    link/ether 08:00:27:e5:40:ce brd ff:ff:ff:ff:ff:ff
    inet6 fd00::b:a00:27ff:fee5:40ce/64 scope global mngtmpaddr dynamic
       valid_lft 2591997sec preferred_lft 604797sec
    inet6 fe80::a00:27ff:fee5:40ce/64 scope link
       valid_lft forever preferred_lft forever
```

Ejercicio 17 [VM1, VM2]. Estudiar los mensajes del protocolo de descubrimiento de vecinos:

- Activar el interfaz en VM2, comprobar que está configurado correctamente e iniciar una captura de paquetes con Wireshark.
- Activar el interfaz en VM1 y estudiar los mensajes ICMP de tipo Router Solicitation y Router Advertisement.
- Comprobar las direcciones destino y origen de los datagramas, así como las direcciones destino y origen de la trama Ethernet. Especialmente la relación entre las direcciones IP y MAC. Estudiar la salida del comando `ip maddr`.

Al activar el interfaz eth0 en VM1…

No.	Time	Source	Destination	Protoc	Lengt	Info
1	0.00000000	::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
2	0.54670397	::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
3	0.90299464	::	ff02::1:ffb7:a754	ICMPv6	78	Neighbor Solicitation for fe80::a00:27ff:feb7:a754
4	1.90524029	fe80::a00:27ff:feb7	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
5	1.90525610	fe80::a00:27ff:feb7	ff02::2	ICMPv6	70	Router Solicitation from 08:00:27:b7:a7:54
6	1.90551938	fe80::a00:27ff:fe0f	ff02::1	ICMPv6	110	Router Advertisement from 08:00:27:0f:bf:73
7	2.62258602	fe80::a00:27ff:feb7	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
8	2.72706496	::	ff02::1:ffb7:a754	ICMPv6	78	Neighbor Solicitation for fd00::a:a00:27ff:feb7:a754

Router Solicitation:

```
▾ Ethernet II, Src: CadmusCo_b7:a7:54 (08:00:27:b7:a7:54), Dst: IPv6mcast_00:00:00:02 (33:33:00:00:00:02)
  ▸ Destination: IPv6mcast_00:00:00:02 (33:33:00:00:00:02)
  ▸ Source: CadmusCo_b7:a7:54 (08:00:27:b7:a7:54)
    Type: IPv6 (0x86dd)
▾ Internet Protocol Version 6, Src: fe80::a00:27ff:feb7:a754 (fe80::a00:27ff:feb7:a754), Dst: ff02::2 (ff02::2)
  ▸ 0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 16
    Next header: ICMPv6 (58)
    Hop limit: 255
    Source: fe80::a00:27ff:feb7:a754 (fe80::a00:27ff:feb7:a754)
    [Source SA MAC: CadmusCo_b7:a7:54 (08:00:27:b7:a7:54)]
    Destination: ff02::2 (ff02::2)
```

Router Advertisment:

```
▾ Ethernet II, Src: CadmusCo_0f:bf:73 (08:00:27:0f:bf:73), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
  ▸ Destination: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
  ▸ Source: CadmusCo_0f:bf:73 (08:00:27:0f:bf:73)
    Type: IPv6 (0x86dd)
▾ Internet Protocol Version 6, Src: fe80::a00:27ff:fe0f:bf73 (fe80::a00:27ff:fe0f:bf73), Dst: ff02::1 (ff02::1)
  ▸ 0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 56
    Next header: ICMPv6 (58)
    Hop limit: 255
    Source: fe80::a00:27ff:fe0f:bf73 (fe80::a00:27ff:fe0f:bf73)
    [Source SA MAC: CadmusCo_0f:bf:73 (08:00:27:0f:bf:73)]
    Destination: ff02::1 (ff02::1)
```

En VM2:

```
[cursoredes@localhost ~]$ ip maddr
1:      lo
        inet  224.0.0.1
        inet6 ff02::1
        inet6 ff01::1
2:      eth0
        link  01:00:5e:00:00:01
        link  33:33:00:00:00:01
        link  33:33:ff:cb:5c:ad
        inet  224.0.0.1
        inet6 ff02::1:ffcb:5cad users 2
        inet6 ff02::1
        inet6 ff01::1
```

En VM1:

```
[cursoredes@localhost ~]$ ip maddr
1:      lo
        inet  224.0.0.1
        inet6 ff02::1
        inet6 ff01::1
2:      eth0
        link  01:00:5e:00:00:01
        link  33:33:00:00:00:01
        link  33:33:ff:b7:a7:54
        inet  224.0.0.1
        inet6 ff02::1:ffb7:a754 users 2
        inet6 ff02::1
        inet6 ff01::1
```

Para saber más... En el proceso de autoconfiguración se genera también el identificador de interfaz según el *Extended Unique Identifier* (EUI-64) modificado. La configuración del protocolo de anuncio de encaminadores tiene múltiples opciones que se pueden consultar en la documentación de `zebra` (ej. intervalo entre anuncios no solicitados). Cuando sólo se necesita un servicio que implemente el anuncio de prefijos, y no algoritmos de encaminamiento para el router, se puede usar el proyecto de código libre *Router Advertisement Daemon*, `radvd`.

Ejercicio 18 [VM1]. La generación del identificador de interfaz mediante EUI-64 supone un problema de privacidad para las máquinas clientes, que pueden ser rastreadas por su dirección MAC. En estos casos, es conveniente activar las extensiones de privacidad para generar un identificador de interfaz pseudoaleatorio temporal para las direcciones globales. Activar las extensiones de privacidad en VM1 con `sysctl -w net.ipv6.conf.eth0.use_tempaddr=2`.

```
[cursoredes@localhost ~]$ 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
qlen 1000
    link/ether 08:00:27:b7:a7:54 brd ff:ff:ff:ff:ff:ff
    inet6 fd00::a:a00:27ff:feb7:a754/64 scope global mngtmpaddr dynamic
       valid_lft 2591997sec preferred_lft 604797sec
    inet6 fe80::a00:27ff:feb7:a754/64 scope link
       valid_lft forever preferred_lft forever

[cursoredes@localhost ~]$ sudo sysctl -w net.ipv6.conf.eth0.use_tempaddr=2
net.ipv6.conf.eth0.use_tempaddr = 2

[cursoredes@localhost ~]$ 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
qlen 1000
    link/ether 08:00:27:b7:a7:54 brd ff:ff:ff:ff:ff:ff
    inet6 fd00::a:9dd9:7943:e824:d064/64 scope global temporary dynamic
       valid_lft 604797sec preferred_lft 85797sec
    inet6 fd00::a:a00:27ff:feb7:a754/64 scope global mngtmpaddr dynamic
       valid_lft 2591997sec preferred_lft 604797sec
    inet6 fe80::a00:27ff:feb7:a754/64 scope link
       valid_lft forever preferred_lft forever
```

-ICMPv6

El protocolo ICMPv6 permite el intercambio de mensajes para el control de la red, tanto para la detección de errores como para la consulta de la configuración de ésta. Durante el desarrollo de la práctica hemos visto los más importantes.

Ejercicio 19. Generar mensajes de los siguientes tipos en la red y estudiarlos con ayuda de Wireshark:

- Solicitud y respuesta de eco.
- Solicitud y anuncio de encaminador.
- Solicitud y anuncio de vecino.
- Destino inalcanzable - Sin ruta al destino (Code: 0).
- Destino inalcanzable - Dirección inalcanzable (Code: 3)
- Destino inalcanzable - Puerto inalcanzable (Code: 4)

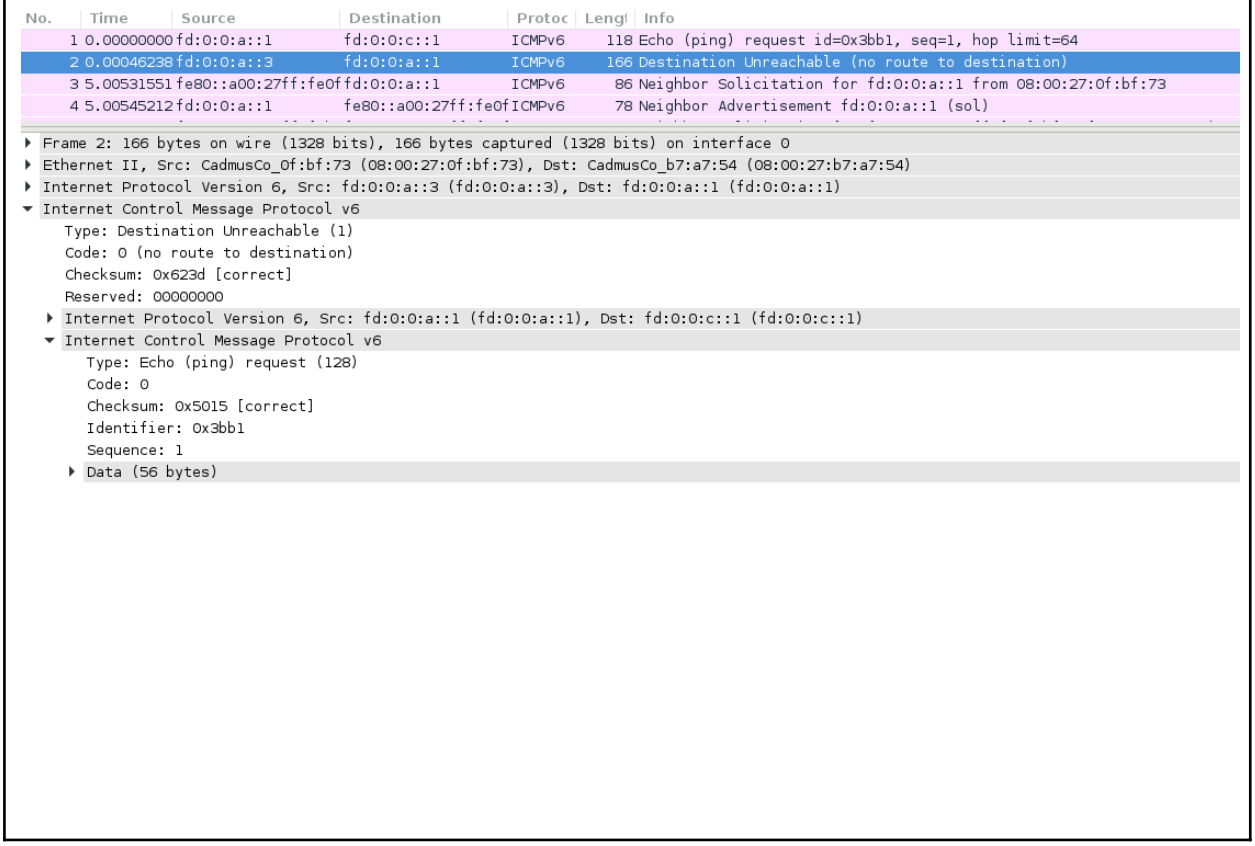
Mantener todas las direcciones IP como antes, el comando *sudo sysctl -w net.ipv6.conf.all.forwarding=1* en VM3 y tener el router como default via en VM1

En VM1:

Code 0:

[cursoredes@localhost ~]$ ping6 -c 1 fd:0:0:c::1 *(esa red no existe)*
PING fd:0:0:c::1(fd:0:0:c::1) 56 data bytes
From fd:0:0:a::3 icmp_seq=1 Destination unreachable: No route

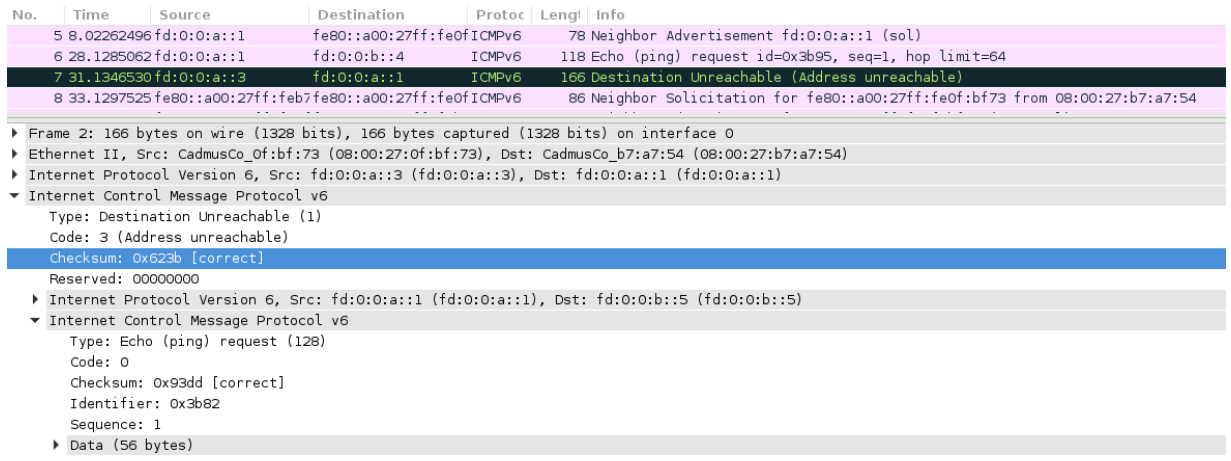
--- fd:0:0:c::1 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms



Code 3:

[cursoredes@localhost ~]$ ping6 -c 1 fd00::0:0:b:4 *(dir. No corresponde con ninguna MV de la red 2)*
PING fd:0:0:b::4(fd:0:0:b::4) 56 data bytes
From fd:0:0:a::3 icmp_seq=1 Destination unreachable: Address unreachable

--- fd:0:0:b::4 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms



Code 4:

[cursoredes@localhost ~]$ nc -6 -u fd00::a:a00:27ff:fecb:5cad 40 *(abrimos una conexion con un puerto (40) de VM2 (dir. fd00::a:a00:27ff:fecb:5cad) que no hemos abierto previamente)*
fg
Ncat: Connection refused.