

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**.

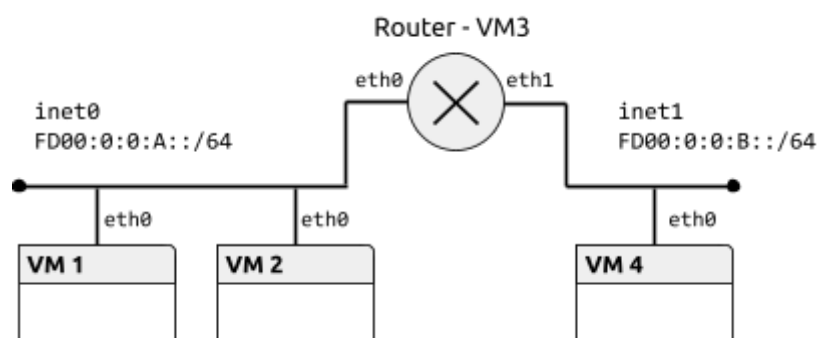
La **contraseña** del usuario cursoredes es cursoredes.

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.

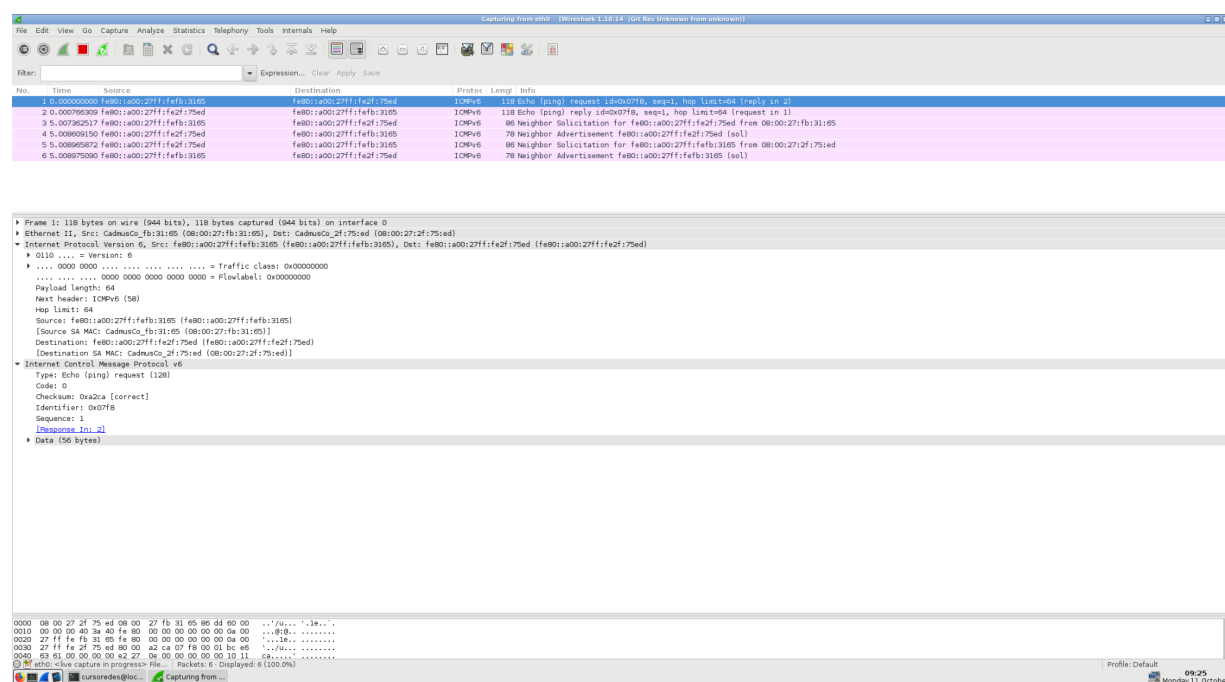
Ejercicio 1 [VM1, VM2]. Activar el interfaz eth0 en VM1 y VM2. Comprobar las direcciones de enlace local que tienen asignadas con el comando ip.

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.

Copiar el comando utilizados y su salida. Copiar una captura de pantalla de Wireshark donde se vean los campos de la cabecera IPv6.

```
VM1: [cursoredes@localhost ~]$ ping6 fe80::a00:27ff:fe2f:75ed%eth0 -c 1
PING fe80::a00:27ff:fe2f:75ed%eth0(fe80::a00:27ff:fe2f:75ed%eth0) 56 data bytes
64 bytes from fe80::a00:27ff:fe2f:75ed%eth0: icmp_seq=1 ttl=64 time=0.779 ms

--- fe80::a00:27ff:fe2f:75ed%eth0 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.779/0.779/0.779/0.000 ms
```



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.

Copiar los comandos utilizados y su salida.

Router:

```
[cursoredes@localhost ~]$ ping6 -c 1 fe80::a00:27ff:fe2f:3165%eth0
PING fe80::a00:27ff:fe2f:3165%eth0(fe80::a00:27ff:fe2f:3165%eth0) 56 data bytes
64 bytes from fe80::a00:27ff:fe2f:3165%eth0: icmp_seq=1 ttl=64 time=1.60 ms
```

```
--- fe80::a00:27ff:fe2f:3165%eth0 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.603/1.603/1.603/0.000 ms
```

```
[cursoredes@localhost ~]$ ping6 -c 1 fe80::a00:27ff:fec0:825d%eth1
PING fe80::a00:27ff:fec0:825d%eth1(fe80::a00:27ff:fec0:825d%eth1) 56 data bytes
64 bytes from fe80::a00:27ff:fec0:825d%eth1: icmp_seq=1 ttl=64 time=1.37 ms

--- fe80::a00:27ff:fec0:825d%eth1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.376/1.376/1.376/0.000 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.

Copiar los comandos utilizados.

```
VM1: [cursoredes@localhost ~]$ sudo ip -6 address add fd00:0:0:A::0001/64 dev eth0
```

```
VM2: [cursoredes@localhost ~]$ sudo ip -6 address add fd00:0:0:a::0002/64 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.

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.

Copiar los comandos utilizados.

Router:

```
[cursoredes@localhost ~]$ sudo ip -6 address add fd00:0:0:a::0003/64 dev eth0
```

```
[cursoredes@localhost ~]$ sudo ip -6 address add fd00:0:0:b::0003/64 dev eth1
```

VM4:

```
[cursoredes@localhost ~]$ sudo ip addr add fd00:0:0:b::0004/64 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.

Copiar los comandos utilizados.

Router:

```
[cursoredes@localhost ~]$ ping6 -c 1 fd00:0:0:a::0001
```

```
PING fd00:0:0:a::0001(fd00:0:0:a::1) 56 data bytes
```

```
64 bytes from fd00:0:0:a::1: icmp_seq=1 ttl=64 time=1.90 ms
```

```
--- fd00:0:0:a::0001 ping statistics ---
```

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

```
rtt min/avg/max/mdev = 1.907/1.907/1.907/0.000 ms
```

```
[cursoredes@localhost ~]$ ping6 -c 1 fd00:0:0:b::0004
PING fd00:0:0:b::0004(fd00:0:0:b::4) 56 data bytes
64 bytes from fd00:0:0:b::4: icmp_seq=1 ttl=64 time=0.877 ms

--- fd00:0:0:b::0004 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.877/0.877/0.877/0.000 ms

VM1:
[cursoredes@localhost ~]$ ping6 -c 1 fd00:0:0:b::0004
connect: Network is unreachable
```

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.

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`.

Copiar los comandos utilizados y su salida.

VM1 y VM2: `[cursoredes@localhost ~]$ sudo ip route add default via fd00:0:0:a::0003`

VM4: `[cursoredes@localhost ~]$ sudo ip route add default via fd00:0:0:b::0003`

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:fb:31:65	33:33:ff:00:00:03	fd00:0:0:a::1	ff02::1:ff00:3	Neighbor Solicitation
08:00:27:79:50:08	08:00:27:fb:31:65	fd00:0:0:a::3	fd00:0:0:a::1	Neighbor Advertisement
08:00:27:fb:31:65	33:33:ff:00:00:03	fe80::a00:27ff:fefb:3165	ff02::1:ff00:3	Neighbor Solicitation
08:00:27:79:50:08	08:00:27:fb:31:65	fd00:0:0:a::3	fe80::a00:27ff:fefb:3165	Neighbor Advertisement

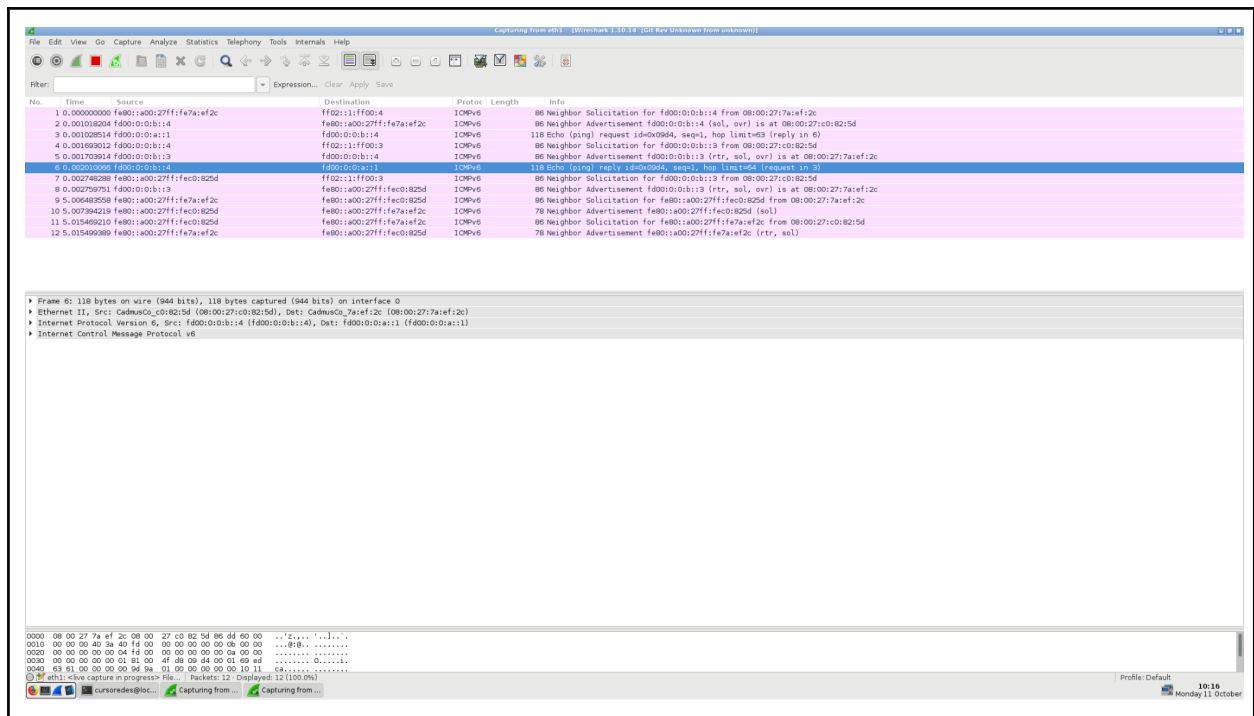
08:00:27:fb:31:65	08:00:27:79:50:08	fd00:0:0:a::1	fd00:0:0:b::4	Echo request
08:00:27:fb:31:65	33:33:ff:00:00:03	fe80::a00:27ff:fefb:3165	ff02::1:ff00:3	Neighbor Solicitation
08:00:27:79:50:08	08:00:27:fb:31:65	fd00:0:0:a::3	fe80::a00:27ff:fefb:3165	Neighbor Advertisement
08:00:27:79:50:08	08:00:27:fb:31:65	fd00:0:0:b::4	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
08:00:27:7a:ef:2c	33:33:ff:00:00:04	fe80::a00:27ff:fe7a:ef2c	ff02::1:ff00:4	Neighbor solicitation
08:00:27:c0:82:5d	08:00:27:7a:ef:2c	fd00:0:0:b::0004	fe80::a00:27ff:fe7a:ef2c	Neighbor advertisement
08:00:27:7a:ef:2c	08:00:27:c0:82:5d	fd00:0:0:a::0001	fd00:0:0:b::0004	Echo request
08:00:27:c0:82:5d	33:33:ff:00:00:04	fd00:0:0:b::0004	ff02::1:ff00:3	Neighbor solicitation
08:00:27:7a:ef:2c	08:00:27:c0:82:5d	fd00:0:0:b::0003	fd00:0:0:b::0004	Neighbor advertisement
08:00:27:c0:82:5d	08:00:27:7a:ef:2c	fd00:0:0:b::0004	fd00:0:0:a::0001	Echo reply

Copiar dos capturas de pantalla de Wireshark.

The screenshot shows the Wireshark network protocol analyzer interface. The top pane, 'Packet List', shows a series of IPv6 Neighbor Solicitation and Advertisement messages between fd00:0:0:a::1 and fd00:0:0:b::4, along with an Echo (ping) request. The bottom pane, 'Packet Details', provides a detailed view of the selected packet (Frame 8), which is an ICMPv6 Echo (ping) reply. It shows the packet structure including Ethernet II, Internet Protocol Version 6, and ICMPv6 fields, with a response time of 2.055 ms.



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>
```

Copiar el contenido de los ficheros.

```
[cursoredes@localhost ~]$ cat /etc/sysconfig/network-scripts/ifcfg-eth0
```

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

```
[cursoredes@localhost ~]$ cat /etc/sysconfig/network-scripts/ifcfg-eth1
```

```
TYPE=Ethernet
BOOTPROTO=none
IPV6ADDR=fd00:0:0:b::3/64
DEVICE=eth1
```

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

Copiar los comandos utilizados y su salida.

```
[cursoredes@localhost ~]$ sudo ifdown eth0
[cursoredes@localhost ~]$ sudo ifdown eth1
[cursoredes@localhost ~]$ sudo ifup eth0
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'
INFO : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the 'tentative'
state
INFO : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the 'tentative'
state
[cursoredes@localhost ~]$ sudo ifup eth1
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'
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`.

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
```

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.

Copiar la dirección asignada.

```
[cursoredes@localhost ~]$ ip a
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
```

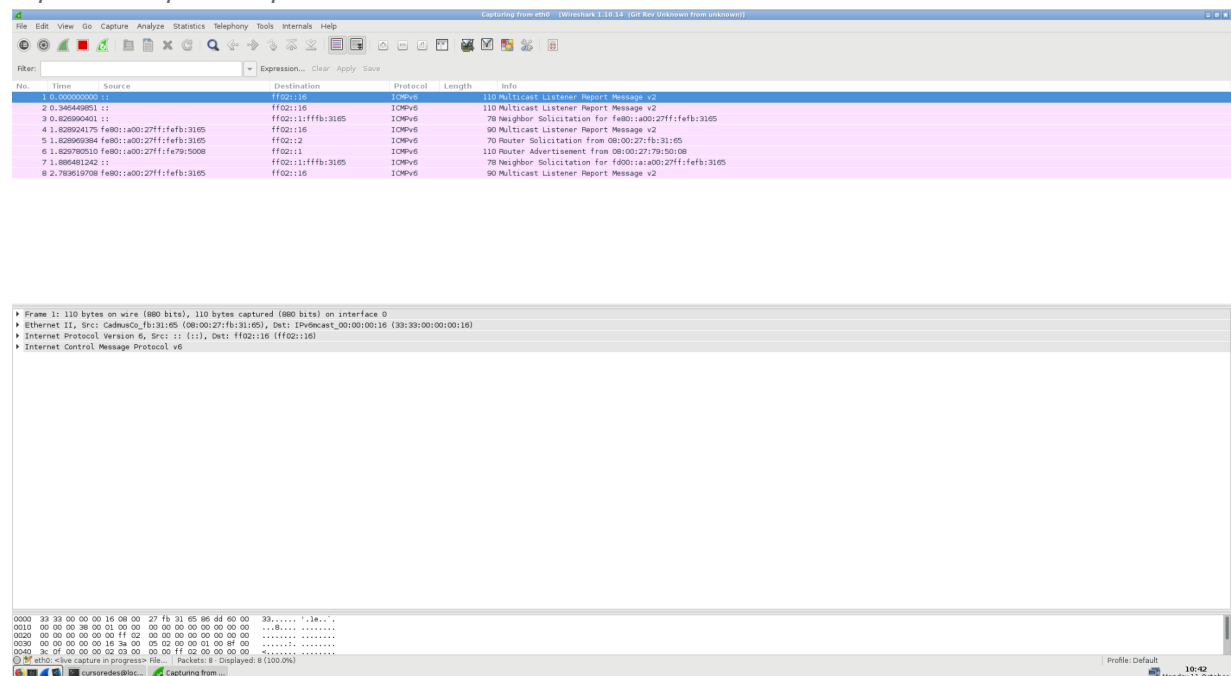
qlen 1000

```
link/ether 08:00:27:c0:82:5d brd ff:ff:ff:ff:ff:ff
inet6 fd00::b:a00:27ff:fec0:825d/64 scope global tentative mngtmpaddr dynamic
valid_lft 2592000sec preferred_lft 604800sec
inet6 fe80::a00:27ff:fec0:825d/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`.

Copiar una captura de pantalla de Wireshark.



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`.

Copiar la dirección asignada.

```
[cursoredes@localhost ~]$ ip a
```

```
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:fb:31:65 brd ff:ff:ff:ff:ff:ff
```

```
    inet6 fd00::a:4089:c35d:ef98:e8fe/64 scope global temporary tentative dynamic
```

```
        valid_lft 604799sec preferred_lft 85799sec
```

```
    inet6 fd00::a:a00:27ff:febf:3165/64 scope global tentative mngtmpaddr dynamic
```

```
        valid_lft 2591999sec preferred_lft 604799sec
```

```
    inet6 fe80::a00:27ff:febf:3165/64 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)

Copiar capturas de pantalla de Wireshark con los tres últimos mensajes.

Sin ruta al destino:

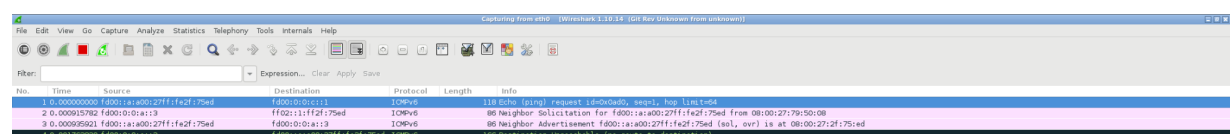
```
[cursoredes@localhost ~]$ ping6 -c 1 fd00:0:0:c::1
```

```
PING fd00:0:0:c::1 (fd00:0:0:c::1) 56 data bytes
```

```
From fd00:0:0:a::3 icmp_seq=1 Destination unreachable: No route
```

```
--- fd00:0:0:c::1 ping statistics ---
```

```
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fd00:0:0:27ff:fe2f:75ed	fd00:0:0:c::1	ICMPv6	112	80 Echo (ping) request: fd00:0:0:27ff:fe2f:75ed to fd00:0:0:c::1
2	0.000015782	fd00:0:0:a::3	ff02::1:ff2f:75ed	ICMPv6	80	80 Neighbor Solicitation for fd00:0:0:27ff:fe2f:75ed from 08:00:27:79:50:08
3	0.000059921	fd00:0:0:a::3	fd00:0:0:a::3	ICMPv6	80	80 Neighbor Advertisement: fd00:0:0:27ff:fe2f:75ed (sol, ov) is at 08:00:27:2f:75:ed
4	0.000169823	fd00:0:0:a::3	fd00:0:0:27ff:fe2f:75ed	ICMPv6	112	00 Destination Unreachable: No route to destination

Dirección inalcanzable:

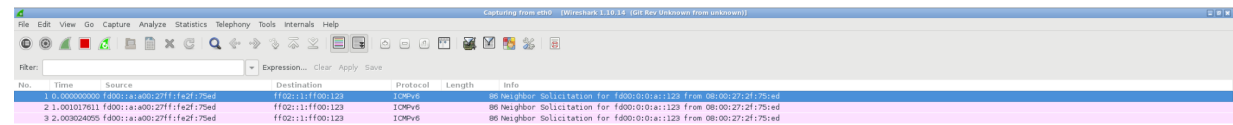
```
[cursoredes@localhost ~]$ ping6 -c 1 fd00:0:0:a::123
```

```
PING fd00:0:0:a::123(fd00:0:0:a::123) 56 data bytes
```

```
From fd00::a:a00:27ff:fe2f:75ed icmp_seq=1 Destination unreachable: Address unreachable
```

--- fd00:0:0:a::123 ping statistics ---

1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms



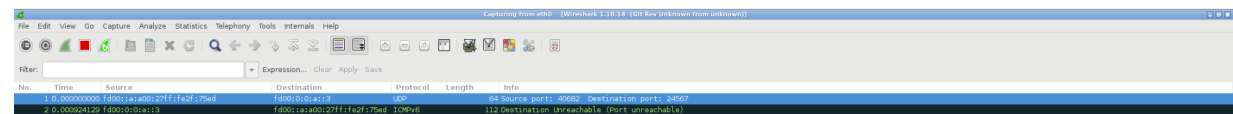
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fd00::a:a00:27ff:fe2f:75ed	ff02::1:ff00:123	ICMPv6	86	Neighbor Solicitation for fd00:0:0:a::123 from 08:00:27:2f:75:ed
2	1.001017611	fd00::a:a00:27ff:fe2f:75ed	ff02::1:ff00:123	ICMPv6	86	Neighbor Solicitation for fd00:0:0:a::123 from 08:00:27:2f:75:ed
3	2.003024055	fd00::a:a00:27ff:fe2f:75ed	ff02::1:ff00:123	ICMPv6	86	Neighbor Solicitation for fd00:0:0:a::123 from 08:00:27:2f:75:ed

Puerto inalcanzable:

```
[cursoredes@localhost ~]$ nc fd00:0:0:a::3 -u 24567
```

```
s
```

```
Ncat: Connection refused.
```



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fd00::a:a00:27ff:fe2f:75ed	fd00:0:0:a::3	TCP	64	Source port: 40862 Destination port: 24567
2	0.000004129	fd00:0:0:a::3	fd00::a:a00:27ff:fe2f:75ed	ICMPv6	112	Destination unreachable (port unreachable)