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**.

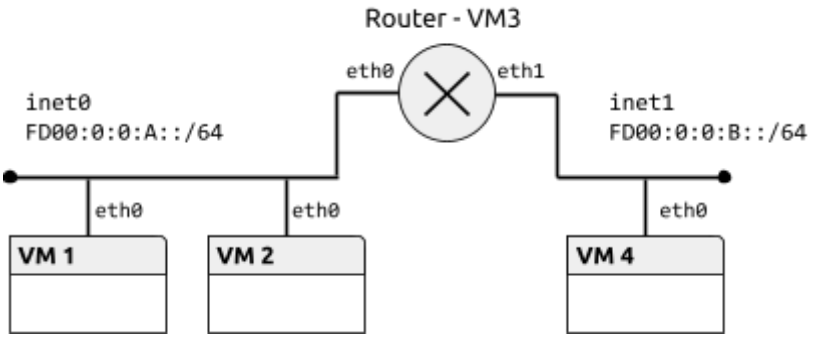
La **contraseña** del usuario `cursoredes` es `cursoredes`.

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`.

ip link set dev eth0 up (VM1 y VM2)

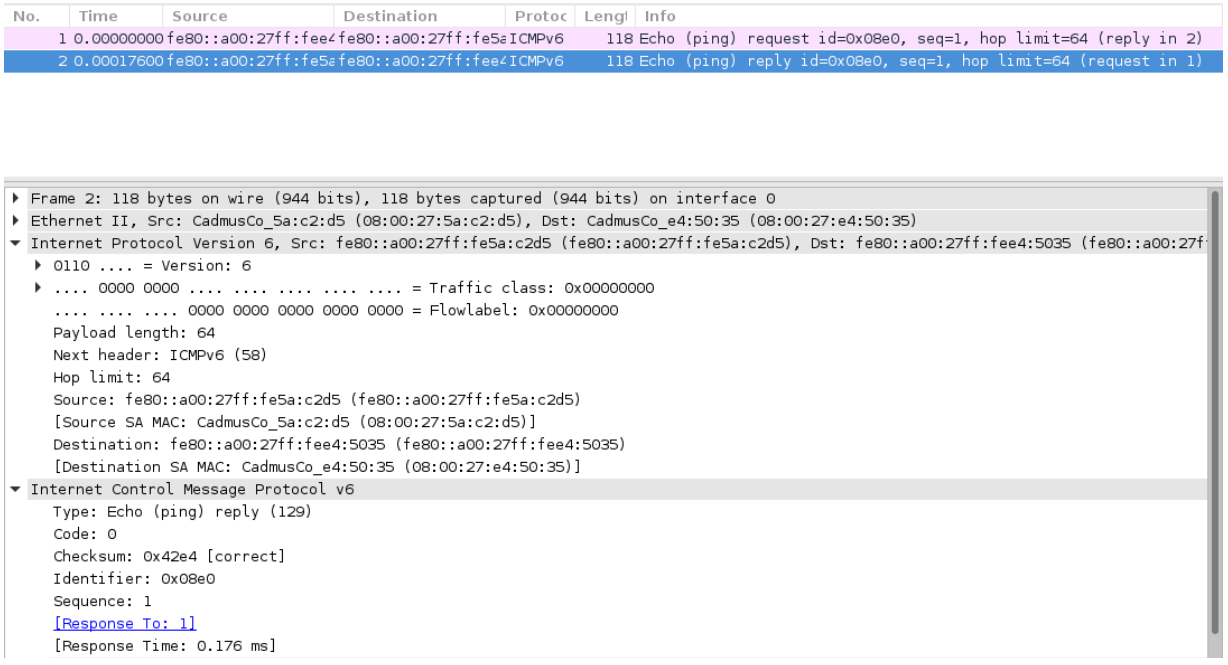
VM1:
ip address
inet6 fe80::a00:27ff:fee4:5035/64 scope link

VM2:
ip address
inet6 fe80::a00:27ff:fe5a:c2d5/64 scope link

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.

VM1:
[cursoredes@localhost ~]$ ping6 fe80::a00:27ff:fe5a:c2d5%eth0 -c 1
PING fe80::a00:27ff:fe5a:c2d5%eth0(fe80::a00:27ff:fe5a:c2d5%eth0) 56 data bytes
64 bytes from fe80::a00:27ff:fe5a:c2d5%eth0: icmp_seq=1 ttl=64 time=0.333 ms

--- fe80::a00:27ff:fe5a:c2d5%eth0 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.333/0.333/0.333/0.000 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.

ip link set dev eth0 up (Router y VM4)
ip link set dev eth1 up (Router)

Router:
ip address
eth0: inet6 fe80::a00:27ff:feac:57e4/64 scope link
eth1: inet6 fe80::a00:27ff:fed9:eb70/64 scope link

VM4:
ip address
inet6 fe80::a00:27ff:fe0c:e735/64 scope link

Router:
-Para VM1
[cursoredes@localhost ~]$ ping6 fe80::a00:27ff:fee4:5035%eth0 -c 1
PING fe80::a00:27ff:fee4:5035%eth0(fe80::a00:27ff:fee4:5035%eth0) 56 data bytes
64 bytes from fe80::a00:27ff:fee4:5035%eth0: icmp_seq=1 ttl=64 time=0.313 ms

--- fe80::a00:27ff:fee4:5035%eth0 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.313/0.313/0.313/0.000 ms

-Para VM4
[cursoredes@localhost ~]$ ping6 fe80::a00:27ff:fe0c:e735%eth1 -c 1
PING fe80::a00:27ff:fe0c:e735%eth1(fe80::a00:27ff:fe0c:e735%eth1) 56 data bytes
64 bytes from fe80::a00:27ff:fe0c:e735%eth1: icmp_seq=1 ttl=64 time=0.281 ms

--- fe80::a00:27ff:fe0c:e735%eth1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.281/0.281/0.281/0.000 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.

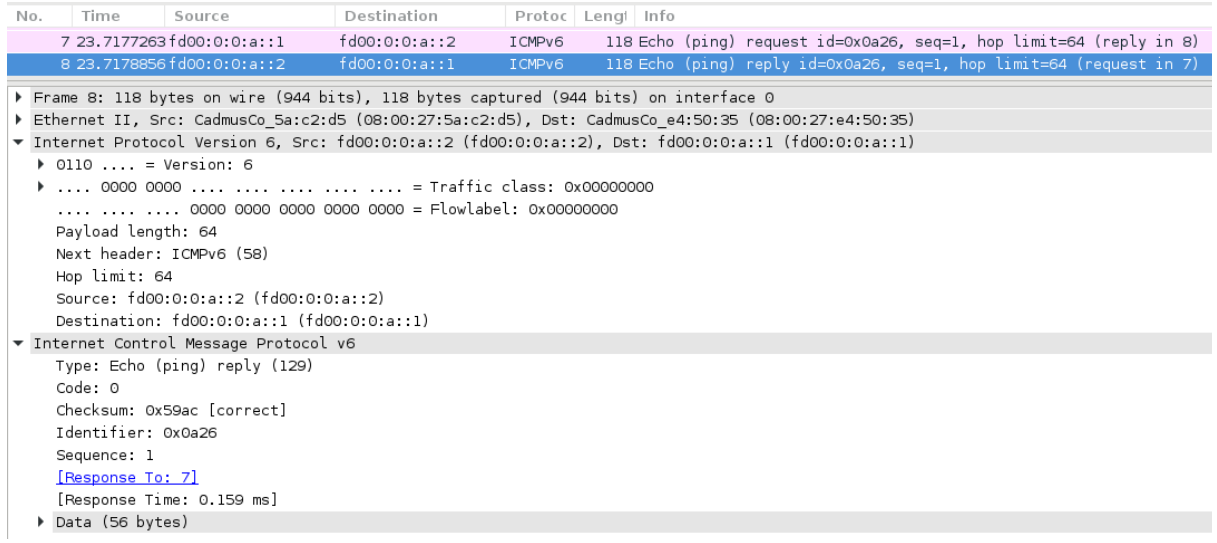
ip link set dev eth0 up (VM1 y VM2)
ip address add fd00:0:0:a::1/64 dev eth0 (VM1)
ip address add fd00:0:0:a::2/64 dev eth0 (VM2)

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.

[cursoredes@localhost ~]$ ping6 fd00:0:0:a::2 -I eth0 -c 1
PING fd00:0:0:a::2(fd00:0:0:a::2) from fd00:0:0:a::1 eth0: 56 data bytes
64 bytes from fd00:0:0:a::2: icmp_seq=1 ttl=64 time=0.168 ms

--- fd00:0:0:a::2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 0.168/0.168/0.168/0.000 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.

ip link set dev eth0 up (Router y VM4)
ip link set dev eth1 up (Router)
ip address add fd00:0:0:a::3/64 dev eth0 (Router)
ip address add fd00:0:0:b::2/64 dev eth1 (Router)
ip address add fd00:0:0:b::1/64 dev eth0 (VM4)

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.

Router:
-Para VM1
[cursoredes@localhost ~]$ ping6 fd00:0:0:a::1 -I eth0 -c 1
PING fd00:0:0:a::1(fd00:0:0:a::1) from fd00:0:0:a::3 eth0: 56 data bytes
64 bytes from fd00:0:0:a::1: icmp_seq=1 ttl=64 time=0.323 ms

--- fd00:0:0:a::1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.323/0.323/0.323/0.000 ms

-Para VM4
[cursoredes@localhost ~]$ ping6 fd00:0:0:b::1 -I eth1 -c 1
PING fd00:0:0:b::1(fd00:0:0:b::1) from fd00:0:0:b::2 eth1: 56 data bytes
64 bytes from fd00:0:0:b::1: icmp_seq=1 ttl=64 time=0.249 ms

--- fd00:0:0:b::1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.249/0.249/0.249/0.000 ms

VM1:
-Para VM4
[cursoredes@localhost ~]$ ping6 fd00:0:0:b::1 -I eth0 -c 1
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.

VM1:
[cursoredes@localhost ~]$ ip -6 route
unreachable ::/96 dev lo metric 1024 error -113 pref medium
unreachable ::ffff:0.0.0.0/96 dev lo metric 1024 error -113 pref medium
unreachable 2002:a00::/24 dev lo metric 1024 error -113 pref medium
unreachable 2002:7f00::/24 dev lo metric 1024 error -113 pref medium
unreachable 2002:a9fe::/32 dev lo metric 1024 error -113 pref medium
unreachable 2002:ac10::/28 dev lo metric 1024 error -113 pref medium
unreachable 2002:c0a8::/32 dev lo metric 1024 error -113 pref medium
unreachable 2002:e000::/19 dev lo metric 1024 error -113 pref medium
unreachable 3ffe:ffff::/32 dev lo metric 1024 error -113 pref medium
fd00:0:0:a::/64 dev eth0 proto kernel metric 256 pref medium
fe80::/64 dev eth0 proto kernel metric 256 pref medium

Router:
[cursoredes@localhost ~]$ ip -6 route
unreachable ::/96 dev lo metric 1024 error -113 pref medium
unreachable ::ffff:0.0.0.0/96 dev lo metric 1024 error -113 pref medium
unreachable 2002:a00::/24 dev lo metric 1024 error -113 pref medium
unreachable 2002:7f00::/24 dev lo metric 1024 error -113 pref medium
unreachable 2002:a9fe::/32 dev lo metric 1024 error -113 pref medium
unreachable 2002:ac10::/28 dev lo metric 1024 error -113 pref medium
unreachable 2002:c0a8::/32 dev lo metric 1024 error -113 pref medium
unreachable 2002:e000::/19 dev lo metric 1024 error -113 pref medium
unreachable 3ffe:ffff::/32 dev lo metric 1024 error -113 pref medium
fd00:0:0:a::/64 dev eth0 proto kernel metric 256 pref medium
fd00:0:0:b::/64 dev eth1 proto kernel metric 256 pref medium
fe80::/64 dev eth0 proto kernel metric 256 pref medium
fe80::/64 dev eth1 proto kernel metric 256 pref medium

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`.

[cursoredes@localhost ~]$ sudo sysctl -w net.ipv6.conf.all.forwarding=1
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`.

sudo ip route add default via fd00:0:0:a::3 (VM1 y VM2)
sudo ip route add default via fd00:0:0:b::2 (VM4)
Copiar los comandos utilizados y su salida.

VM1:

-Para VM4
[cursoredes@localhost ~]$ ping6 fd00:0:0:b::1 -I eth0 -c 1
PING fd00:0:0:b::1(fd00:0:0:b::1) from fd00:0:0:a::1 eth0: 56 data bytes
64 bytes from fd00:0:0:b::1: icmp_seq=1 ttl=63 time=0.327 ms

--- fd00:0:0:b::1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.327/0.327/0.327/0.000 ms

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:

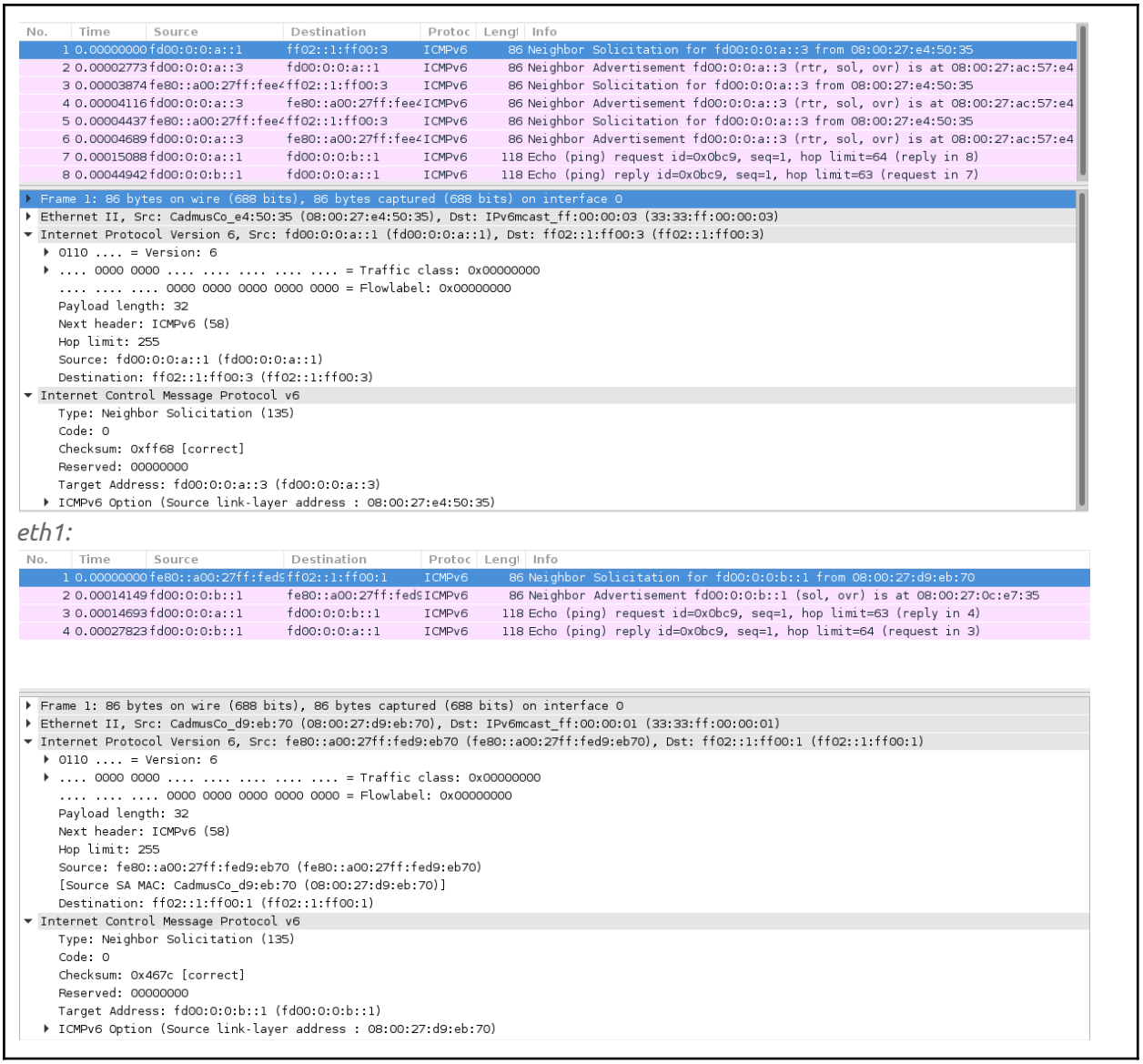
Red `fd00:0:0:a::/64` - Router (eth0)

MAC Origen	**MAC Destino**	**IPv6 Origen**	**IPv6 Destino**	**ICMPv6 Tipo**
MAC VM1	BROADCAST	IP VM1	Solicited-node multicast	Neighbor solicitation (135)
MAC Router	MAC VM1	IP Router	IP VM1	Neighbor advertisement (136)
MAC VM1	MAC Router	IP VM1	IP VM4	Echo request (128)
MAC Router	MAC VM1	IP VM4	IP VM1	Echo reply (129)

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

MAC Origen	**MAC Destino**	**IPv6 Origen**	**IPv6 Destino**	**ICMPv6 Tipo**
MAC VM4	BROADCAST	IP Router	Solicited-node multicast	Neighbor solicitation (135)
MAC Router	MAC VM4	IP VM4	IP Router	Neighbor advertisement (136)
MAC VM4	MAC Router	IP VM1	IP VM4	Echo request (128)
MAC Router	MAC VM4	IP VM4	IP VM1	Echo reply (129)

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>
```

ifcfg-eth0:

```
TYPE=Ethernet
BOOTPROTO=none
IP6ADDR=fd00:0:0:a::3
DEVICE=eth0

ifcfg-eth1:
TYPE=Ethernet
BOOTPROTO=none
IP6ADDR=fd00:0:0:b::2
DEVICE=eth1
```

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

```
[cursoredes@localhost ~]$ sudo ifdown eth0

[cursoredes@localhost ~]$ sudo ifup eth0
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 ifdown eth1

[cursoredes@localhost ~]$ sudo ifup eth1
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
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

[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:ac:57:e4 brd ff:ff:ff:ff:ff:ff
   inet6 fd00:0:0:a::3/64 scope global
      valid_lft forever preferred_lft forever
   inet6 fe80::a00:27ff:feac:57e4/64 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:d9:eb:70 brd ff:ff:ff:ff:ff:ff
   inet6 fd00:0:0:b::2/64 scope global
      valid_lft forever preferred_lft forever
   inet6 fe80::a00:27ff:fed9:eb70/64 scope link
      valid_lft forever preferred_lft forever
```

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.

```
ip link set dev eth0 down (VM1, VM2 y VM4)
```

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`.

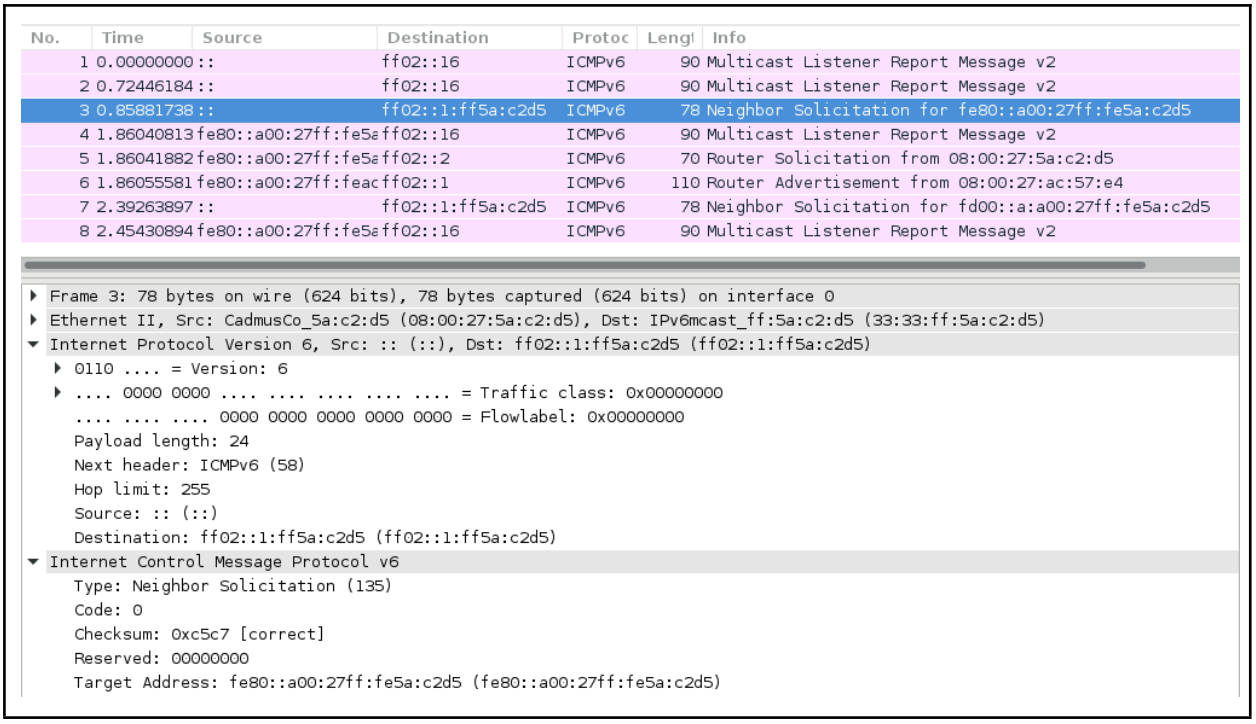
Ejercicio 16 [VM4]. Comprobar la autoconfiguración del interfaz de red en VM4, volviendo a activar el interfaz y consultando la dirección asignada.

```
inet6 fd00::b:a00:27ff:fe0c:e735/64 scope global mngtmpaddr dynamic
    valid_lft 2591977sec preferred_lft 604777sec
```

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`.

```
[cursoredes@localhost ~]$ ip maddr
1:      lo
        inet  224.0.0.1
        inet6 ff02::1
        inet6 ff01::1
2:      eth0
        link  33:33:00:00:00:01
        link  01:00:5e:00:00:01
        link  33:33:ff:e4:50:35
        inet  224.0.0.1
        inet6 ff02::1:ffe4:5035 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 08:00:27:5a:c2:d5 brd ff:ff:ff:ff:ff:ff
    inet6 fd00::a:2d0e:66c3:ae3:833a/64 scope global temporary dynamic
       valid_lft 604799sec preferred_lft 85799sec
    inet6 fd00::a:a00:27ff:fe5a:c2d5/64 scope global tentative mngtmpaddr dynamic
       valid_lft 2591999sec preferred_lft 604799sec
    inet6 fe80::a00:27ff:fe5a:c2d5/64 scope link
       valid_lft forever preferred_lft forever
```

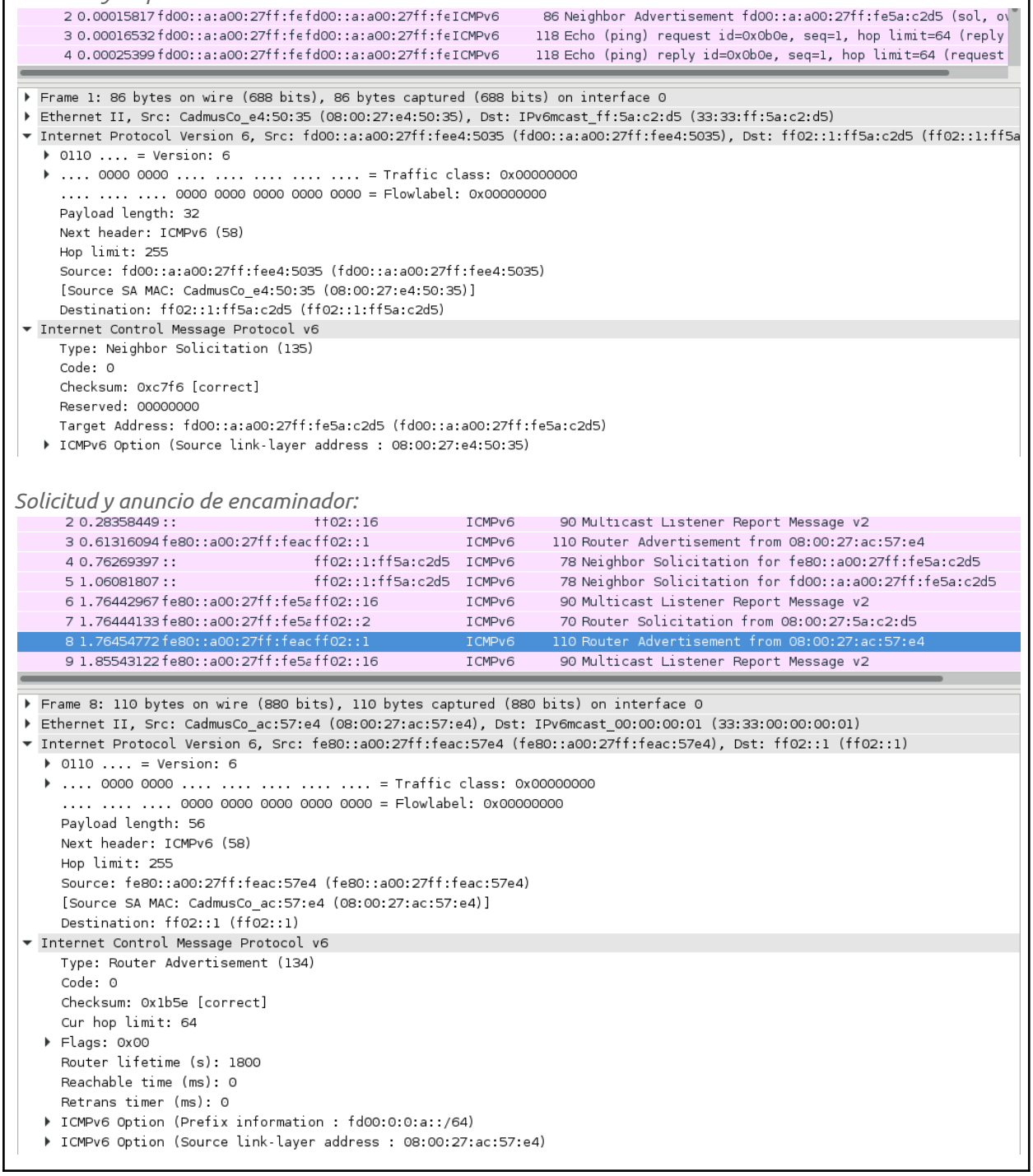
ICMPv6

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:

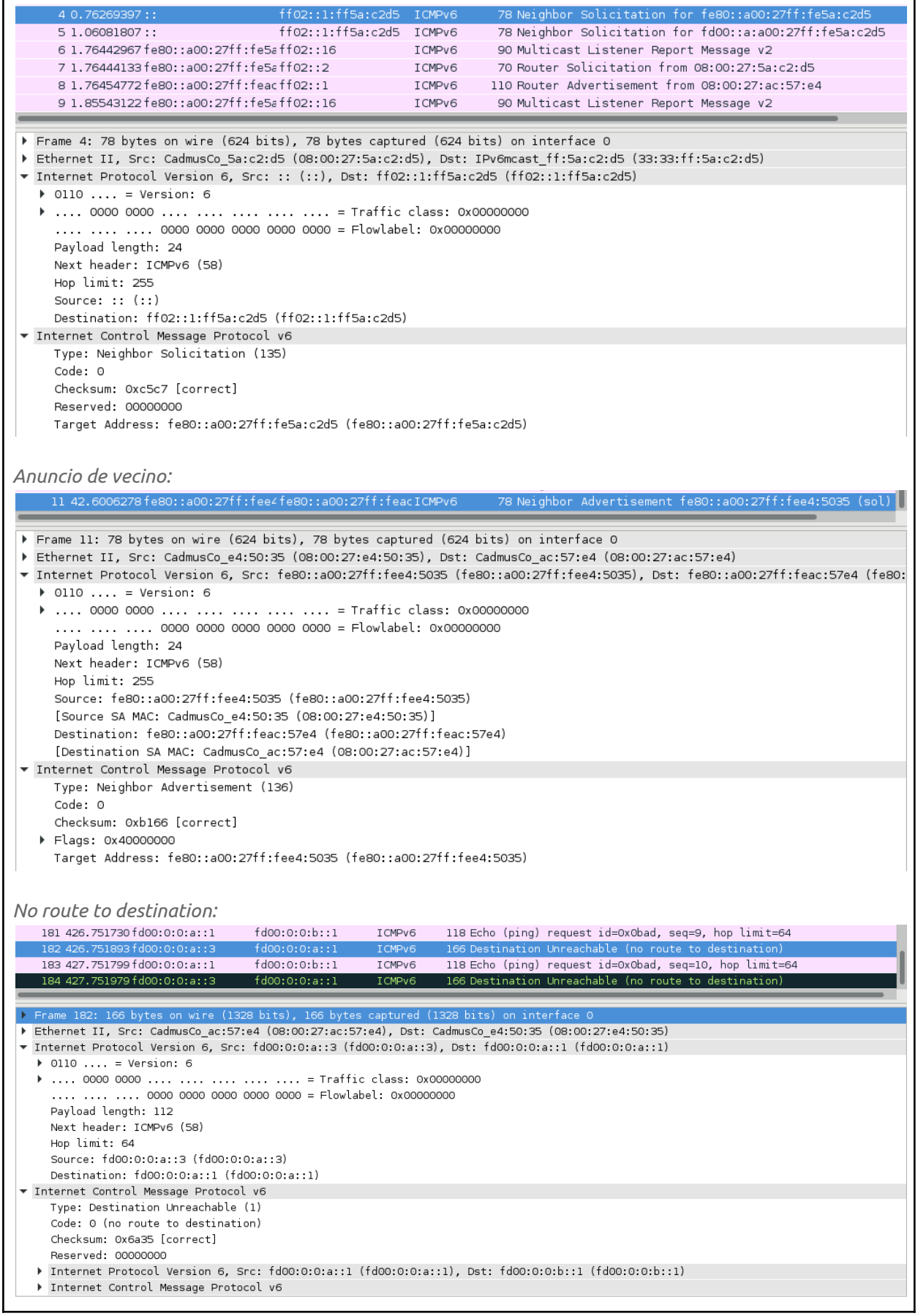
- Solicitud y respuesta de eco.
- Solicitud y anuncio de encaminador.
- Solicitud y anuncio de vecino.
- Destino inalcanzable - Sin ruta al destino (Code: 0).
- Destino inalcanzable - Dirección inalcanzable (Code: 3)
- Destino inalcanzable - Puerto inalcanzable (Code: 4)

Solicitud y respuesta de eco:



Solicitud y anuncio de encaminador:

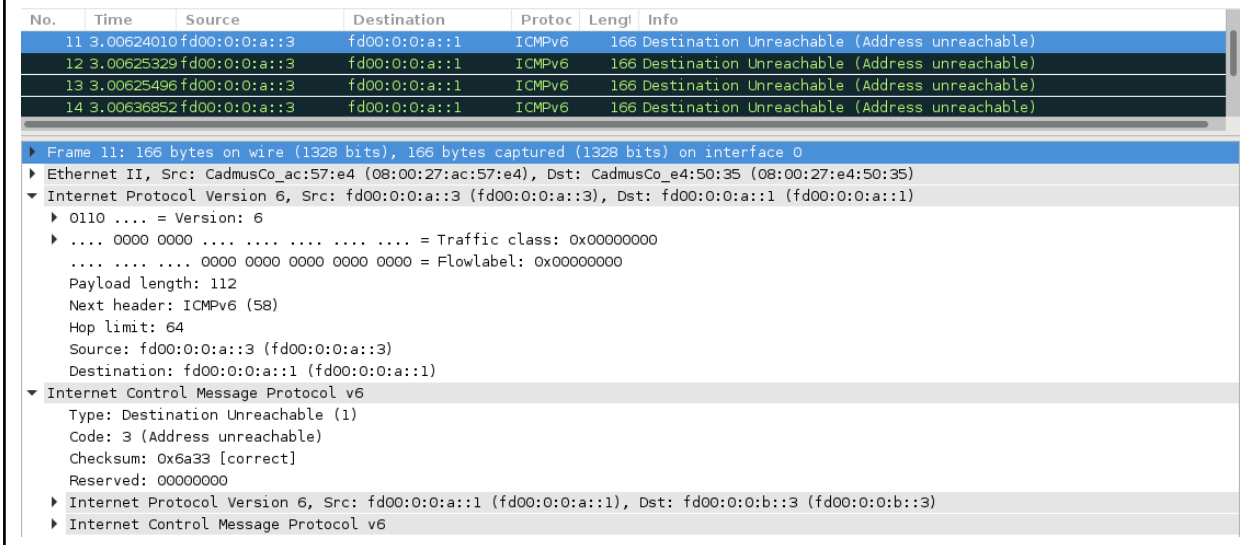
Solicitud de vecino:



Anuncio de vecino:

No route to destination:

Address unreachable:



Port unreachable: