

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.

Contenidos

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



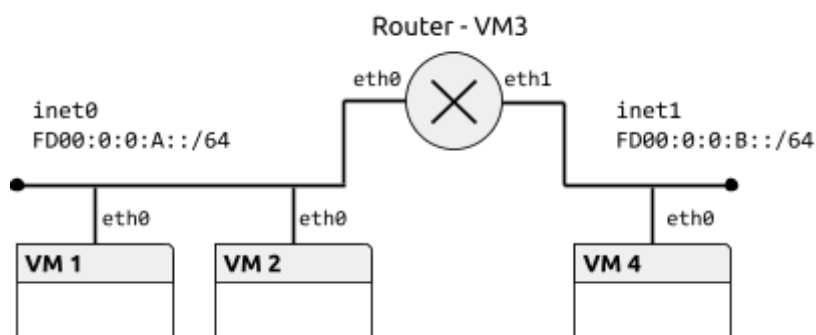
Activar el **portapapeles bidireccional** (menú Dispositivos) en las máquinas virtuales.

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

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

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

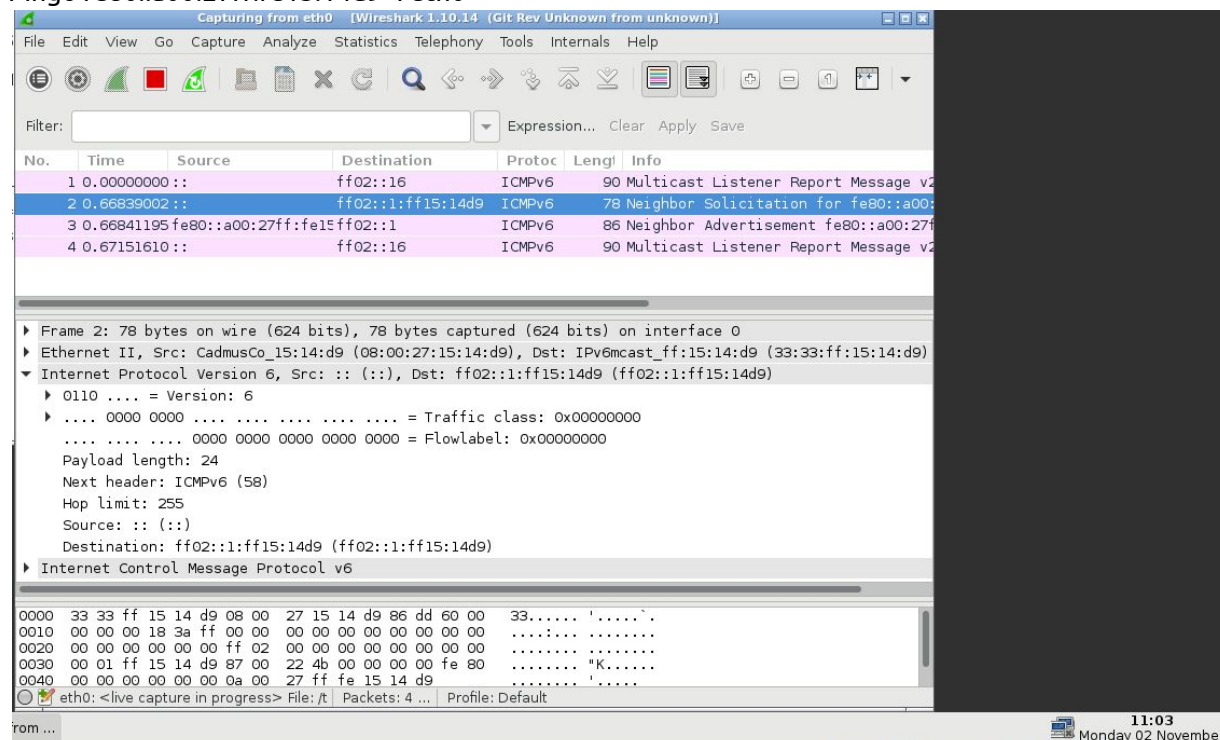
Una dirección de enlace local es únicamente válida en la subred que está definida. Ningún encaminador dará salida a un datagrama con una dirección de enlace local como destino. El prefijo de formato para estas direcciones es fe80::/10.

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. 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

Ping6 fe80::a00:27ff:fe15:14d9 -I 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.

```
V3 a v1
Ping6 fe80::a00:27ff:fe15:14d9 -I eth0
V3 a v4
ping6 fe80::a00:27ff:fe15:14d9 -I eth1
```

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.

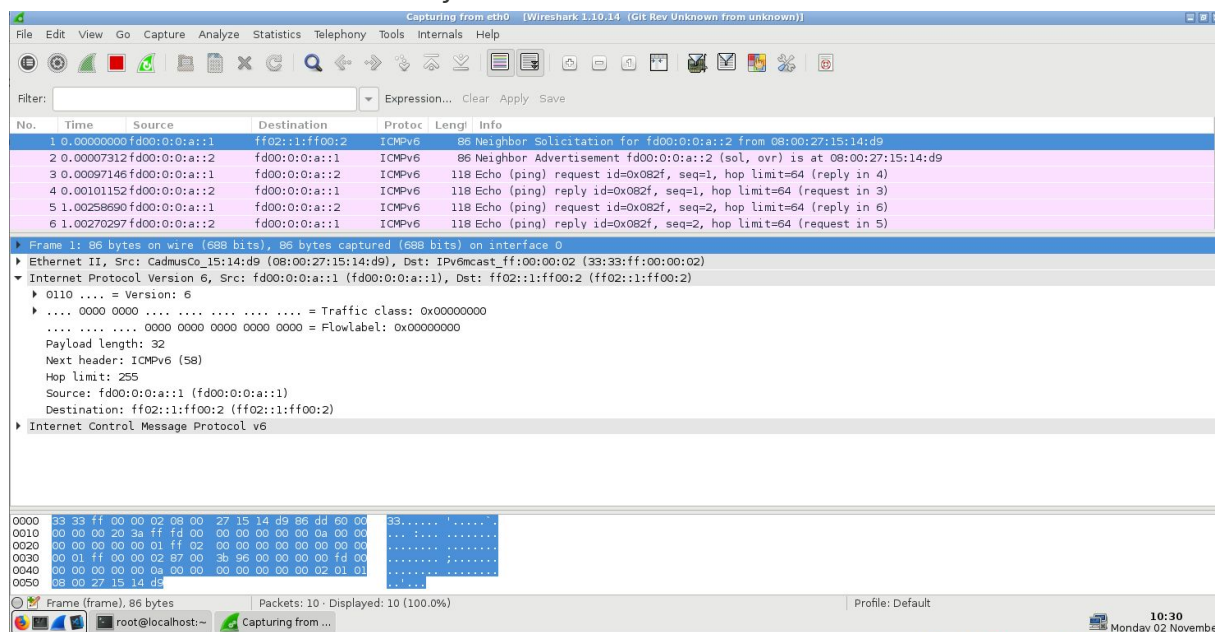
Direcciones ULA

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 eth0
ip -6 a add fd00:0:0:A::1 dev eth0
ip -6 a add fd00:0:0:A::32 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.
V3
ip -6 a add fd00:0:0:B::1 dev eth1
V4
ip -6 a add fd00:0:0:B::2 dev eth0
Desde V3 a V4
Ping6 fd00:0:0:B::2

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.
V3
ip -6 a add fd00:0:0:A::3 dev eth0
Desde V3 a V1
Ping6 fd00:0:0:A::1

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.

En V1 y V2

```
ip -6 route add default via fd00:0:0:A::3
```

En V4

```
ip -6 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
Mac V1	MAC Multicast	fd00:0:0:A::1	Ff02::1:ff00:2	N. Solicitation
ROUTER	V1	IP ROUTER	IP V1	N. Advertismen t
MAC V1	MAC V4	IP V1	IP V4	E. RQ
MAC V4	MAC V1	IP V4	IP V1	E RP

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

MAC Origen	MAC Destino	IPv6 Origen	IPv6 Destino	ICMPv6 Tipo
MAC V4	MAC MULTICAST	V4	Multicast	N. Advertismen t
MAC V1	MAC V4	V1	V4	RQ
MAC R	MAC V4	R	V4	N. Advertismen t
MAC V4	MAC V1	V4	V1	RP

Copiar dos capturas de pantalla de Wireshark.

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/ini-scripts-*/sysconfig.txt):

```

TYPE=Ethernet
BOOTPROTO=none
IPV6ADDR=<dirección IP estática en formato CIDR>
IPV6_DEFAULTGW=<dirección IP estática del encaminador por defecto (si existe)>
DEVICE=<nombre del interfaz>

```

Copiar el contenido de los ficheros.

```
TYPE=Ethernet
BOOTPROTO=none
IPV6ADDR= fd00:0:0:A::/64
IPV6_DEFAULTGW= fd00:0:0:A::3
DEVICE= eth0
```

Error que me sale al hacer ifup eth0 e ifdown eth0

```
/etc/sysconfig/network-scripts/ifcfg-eth0: line 3: fd00:0:0:A::/64: No such file or directory
/etc/sysconfig/network-scripts/ifcfg-eth0: line 4: fd00:0:0:A::3: command not found
/etc/sysconfig/network-scripts/ifcfg-eth0: line 5: eth0: command not found
/etc/sysconfig/network-scripts/ifcfg-eth0: line 3: fd00:0:0:A::/64: No such file or directory
/etc/sysconfig/network-scripts/ifcfg-eth0: line 4: fd00:0:0:A::3: command not found
/etc/sysconfig/network-scripts/ifcfg-eth0: line 5: eth0: command not found
ERROR : [/etc/sysconfig/network-scripts/ifup-eth] Device does not seem to be present, delaying
initialization.
```

```
TYPE=Ethernet
BOOTPROTO=none
IPV6ADDR= fd00:0:0:B::/64
IPV6_DEFAULTGW= fd00:0:0:B::1
DEVICE= eth1
```

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

Copiar los comandos utilizados y su salida.

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.

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default
qlen 1000
link/ether 08:00:27:02:f3:13 brd ff:ff:ff:ff:ff:ff
inet6 fd00::b:a00:27ff:fe02:f313/64 scope global mngtmpaddr dynamic
    valid_lft 2591918sec preferred_lft 604718sec
inet6 fe80::a00:27ff:fe02:f313/64 scope link tentative dadfailed
```

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) que se describe en el RFC 4193. 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.

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 destino inalcanzable (Code: 3)

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