ALBERTO LEÓN LUENGO

MEMORIA PRÁCTICA 1: IPv6

ÍNDICE DE CONTENIDOS

[] 1. FUNCIONAMIENTO BÁSICO DE IPv6

} 1.1 AUTOCONFIGURACIÓN DE DIRECCIONES IPv6 (LINK-LOCAL)

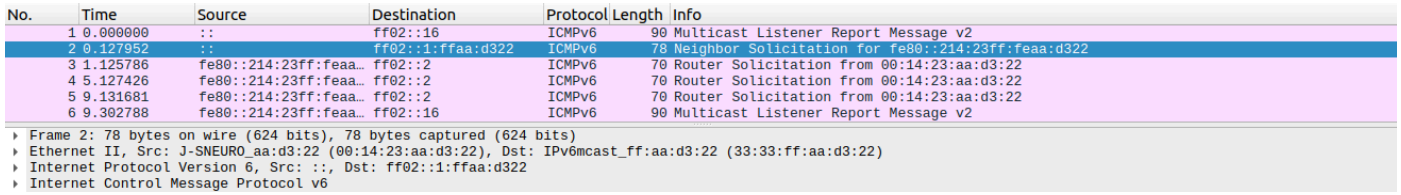
PREGUNTA 1
COMANDO: pc1:~# ip -6 addr show (mostrar dirección IPv6)
COMANDO: pc1:~# ifconfig (mostrar dirección Ethernet)
La dirección IPv6 link-local configurada en pc1 es fe80::214:23ff:feaa:d311(/64) y su dirección Ethernet es 00:14:23:aa:d3:11.
La principal relación que existe entre la dirección IPv6 link-local y la dirección Ethernet establece que se puede construir la dirección IPv6 a partir de la dirección Ethernet, donde la dirección Ethernet se expande hasta tener una longitud de 64 bits añadiendo ff:fe, además de invertir el segundo bit por 0 si es local o 1 si es global.

PREGUNTA 2
COMANDO: pc1:~# ip -6 maddr show dev eth0 (mostrar dirección IPv6 multicast de nodo solicitado en eth0)
La dirección IPv6 multicast de nodo solicitado a la que pertenece pc1 es ff02::1:ffaa:d311.

PREGUNTA 3
COMANDO: pc2:~# ip -6 addr show (mostrar dirección IPv6)
COMANDO: pc2:~# ifconfig (mostrar dirección Ethernet)
La dirección IPv6 link-local configurada en pc2 es fe80::214:23ff:feaa:d322(/64) y su dirección Ethernet es 00:14:23:aa:d3:22.
La principal relación que existe entre la dirección IPv6 link-local y la dirección Ethernet establece que se puede construir la dirección IPv6 a partir de la dirección Ethernet, donde la dirección Ethernet se expande hasta tener una longitud de 64 bits añadiendo ff:fe, además de invertir el segundo bit por 0 si es local o 1 si es global.
COMANDO: pc1:~# tcpdump -i eth0 -s 0 -w /hosthome/ipv6-01.cap (arrancar una captura de tráfico)

PREGUNTA 4
COMANDO: pc2:~# ip -6 maddr show dev eth0 (mostrar dirección IPv6 multicast de nodo solicitado en eth0)
La dirección IPv6 multicast de nodo solicitado a la que pertenece pc2 es ff02::1:ffaa:d322.

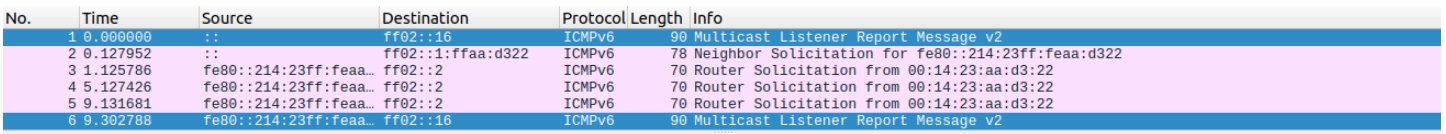
PREGUNTA 5
COMANDO: pc1:~# ctrl+c (interrumpir una captura de tráfico)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-01.cap (abrir una captura de tráfico en wireshark)



El paquete 2 es el que indica si pc2 está detectando si existen direcciones IPv6 duplicadas con su dirección link-local.

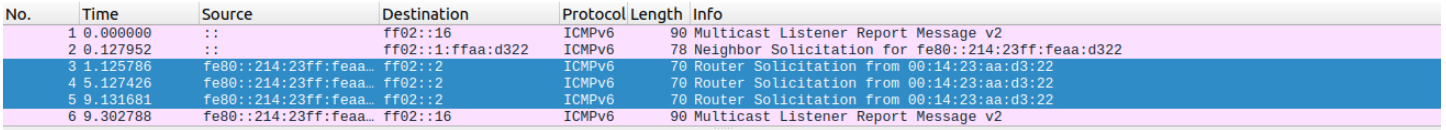
PREGUNTA 6
La máquina pc1 no recibe/procesa este mensaje, ya que la dirección destino del mismo es la dirección IPv6 multicast de nodo solicitado de pc2.

PREGUNTA 7



Los paquetes 1 y 6 son mensajes ICMPv6 Multicast Listener Report, cuyo propósito consiste en un datagrama dirigido a una dirección de multicast que será entregado en todas las máquinas que tengan esa IP (o dicho de otra forma, que pertenezcan a ese grupo de multicast).

PREGUNTA 8



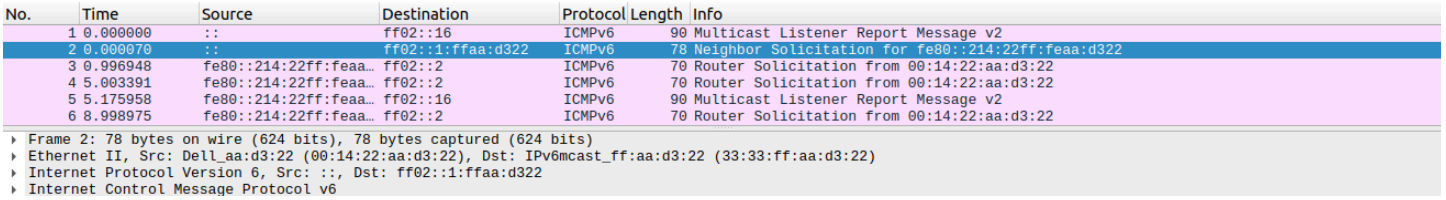
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
2	0.127952	::	ff02::1:ffaa:d322	ICMPv6	78	Neighbor Solicitation for fe80::214:23ff:feaa:d322
3	1.125786	fe80::214:23ff:feaa…	ff02::2	ICMPv6	70	Router Solicitation from 00:14:23:aa:d3:22
4	5.127426	fe80::214:23ff:feaa…	ff02::2	ICMPv6	70	Router Solicitation from 00:14:23:aa:d3:22
5	9.131681	fe80::214:23ff:feaa…	ff02::2	ICMPv6	70	Router Solicitation from 00:14:23:aa:d3:22
6	9.302788	fe80::214:23ff:feaa…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2

Los paquetes 3, 4 y 5 son mensajes ICMPv6 Router Solicitation, cuyo propósito de la máquina, en caso de que el periodo sea grande, es el de enviar uno o más mensajes de este tipo al grupo de multicast de todos los routers que estén conectados al mismo nivel de enlace (ff02::2).
COMANDO: pc1:~# tcpdump -i eth0 -s 0 -w /hosthome/ipv6-02.cap (arrancar una captura de tráfico)

PREGUNTA 8
COMANDO: pc3:~# ip -6 addr show (mostrar dirección IPv6)
COMANDO: pc3:~# ifconfig (mostrar dirección Ethernet)
La dirección IPv6 link-local configurada en pc3 es fe80::214:22ff:feaa:d322(/64) y su dirección Ethernet es 00:14:22:aa:d3:22.
La principal relación que existe entre la dirección IPv6 link-local y la dirección Ethernet establece que se puede construir la dirección IPv6 a partir de la dirección Ethernet, donde la dirección Ethernet se expande hasta tener una longitud de 64 bits añadiendo ff:fe, además de invertir el segundo bit por 0 si es local o 1 si es global.

PREGUNTA 9
COMANDO: pc3:~# ip -6 maddr show dev eth0 (mostrar dirección IPv6 multicast de nodo solicitado en eth0)
La dirección IPv6 multicast de nodo solicitado a la que pertenece pc2 es ff02::1:ffaa:d322.

PREGUNTA 10
COMANDO: pc1:~# ctrl+c (interrumpir una captura de tráfico)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-02.cap (abrir una captura de tráfico en wireshark)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
2	0.000070	::	ff02::1:ffaa:d322	ICMPv6	78	Neighbor Solicitation for fe80::214:22ff:feaa:d322
3	0.996948	fe80::214:22ff:feaa…	ff02::2	ICMPv6	70	Router Solicitation from 00:14:22:aa:d3:22
4	5.003391	fe80::214:22ff:feaa…	ff02::2	ICMPv6	70	Router Solicitation from 00:14:22:aa:d3:22
5	5.175958	fe80::214:22ff:feaa…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
6	8.998975	fe80::214:22ff:feaa…	ff02::2	ICMPv6	70	Router Solicitation from 00:14:22:aa:d3:22


```
▸ Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▸ Ethernet II, Src: Dell_aa:d3:22 (00:14:22:aa:d3:22), Dst: IPv6mcast_ff:aa:d3:22 (33:33:ff:aa:d3:22)
▸ Internet Protocol Version 6, Src: ::, Dst: ff02::1:ffaa:d322
▸ Internet Control Message Protocol v6
```

El paquete 2 es el que indica si pc2 está detectando si existen direcciones IPv6 duplicadas con su dirección link-local.

PREGUNTA 11
La máquina pc1 no recibe/procesa este mensaje, ya que la dirección destino del mismo es la dirección IPv6 multicast de nodo solicitado de pc2. Y en el caso de pc2, aunque la dirección IPv6 multicast de nodo solicitado coincida con la de pc3, tampoco recibirá/procesará el mensaje, ya que en el target del mensaje aparece la dirección IPv6 de pc3.

PREGUNTA 12
Ni pc1 ni pc2 responden al mensaje enviado por pc3, ya que, en el caso de pc1, la dirección destino es la dirección IPv6 multicast de nodo solicitado de pc2, mientras que en el caso de pc2, aunque su dirección IPv6 multicast de nodo solicitado coincida con la de pc3, aparece la dirección IPv6 de pc3 en el target del mensaje.

} 1.2 TRÁFICO IPv6 ENTRE 2 MÁQUINAS DIRECTAMENTE CONECTADAS

PREGUNTA 1
COMANDO: pc1:~# ip -6 route (mostrar las rutas IPv6 configuradas en pc1)
fe80::/64 dev eth0 metric 256 expires -2280sec mtu 1500 advmss 1440 hoplimit 4294967295
ff00::/8 dev eth0 metric 256 expires -2280sec mtu 1500 advmss 1440 hoplimit 4294967295
COMANDO: pc2:~# ip -6 route (mostrar las rutas IPv6 configuradas en pc2)
fe80::/64 dev eth0 metric 256 expires -10sec mtu 1500 advmss 1440 hoplimit 4294967295
ff00::/8 dev eth0 metric 256 expires -10sec mtu 1500 advmss 1440 hoplimit 4294967295
COMANDO: pc3:~# ip -6 route (mostrar las rutas IPv6 configuradas en pc3)
fe80::/64 dev eth0 metric 256 expires -2591sec mtu 1500 advmss 1440 hoplimit 4294967295
ff00::/8 dev eth0 metric 256 expires -2591sec mtu 1500 advmss 1440 hoplimit 4294967295
Como se puede ver, las rutas IPv6 configuradas en pc1, pc2 y pc3 son iguales, lo que significa que las máquinas pueden comunicarse con todas las máquinas vecinas cuyas direcciones empiecen por fe80:: por la interfaz eth0, y con todos los multicast vecinos cuyas direcciones empiecen por ff00:: por la interfaz eth0.

PREGUNTA 2
COMANDO: pc3:~# tcpdump -i eth0 -s 0 -w /hosthome/ipv6-03.cap (arrancar una captura de tráfico)
COMANDO: pc1:~# ping6 -I eth0 fe80::214:23ff:feaa:d322 (realizar ping6 de pc1 a pc2)

PREGUNTA 3
COMANDO: pc2:~# ping6 -I eth0 ff02::1:ffaa:d311 (realizar ping6 de pc2 a pc1)

```
pc2:~# ping6 -I eth0 ff02::1:ffaa:d311
PING ff02::1:ffaa:d311(ff02::1:ffaa:d311) from fe80::214:23ff:feaa:d322 eth0: 56 data bytes
64 bytes from fe80::214:23ff:feaa:d311: icmp_seq=1 ttl=64 time=0.115 ms
64 bytes from fe80::214:23ff:feaa:d311: icmp_seq=2 ttl=64 time=0.322 ms
64 bytes from fe80::214:23ff:feaa:d311: icmp_seq=3 ttl=64 time=0.360 ms
64 bytes from fe80::214:23ff:feaa:d311: icmp_seq=4 ttl=64 time=0.161 ms
64 bytes from fe80::214:23ff:feaa:d311: icmp_seq=5 ttl=64 time=0.322 ms
64 bytes from fe80::214:23ff:feaa:d311: icmp_seq=6 ttl=64 time=0.272 ms
```

El ping6 realizado desde pc2 a la dirección IPv6 multicast de nodo solicitado de pc1 funciona correctamente, donde se envían mensajes desde pc2 y se obtiene respuesta por parte de pc1.

PREGUNTA 4
COMANDO: pc1:~# ping6 -I eth0 ff02::1:ffaa:d322 (realizar ping6 de pc1 a pc2)

```
pc1:~# ping6 -I eth0 ff02::1:ffaa:d322
PING ff02::1:ffaa:d322(ff02::1:ffaa:d322) from fe80::214:23ff:feaa:d311 eth0: 56 data bytes
64 bytes from fe80::214:23ff:feaa:d322: icmp_seq=1 ttl=64 time=0.154 ms
64 bytes from fe80::214:22ff:feaa:d322: icmp_seq=1 ttl=64 time=10.7 ms (DUP!)
64 bytes from fe80::214:23ff:feaa:d322: icmp_seq=2 ttl=64 time=0.196 ms
64 bytes from fe80::214:22ff:feaa:d322: icmp_seq=2 ttl=64 time=0.198 ms (DUP!)
64 bytes from fe80::214:22ff:feaa:d322: icmp_seq=3 ttl=64 time=0.202 ms
64 bytes from fe80::214:23ff:feaa:d322: icmp_seq=3 ttl=64 time=0.203 ms (DUP!)
```

El ping6 realizado desde pc1 a la dirección IPv6 multicast de nodo solicitado de pc2 funciona correctamente, con la única diferencia de que en este ping6 aparece el mensaje DUP!. Esto se debe a que las direcciones IPv6 multicast de nodo solicitado de pc2 y pc3 coinciden.

PREGUNTA 5
COMANDO: pc1:~# ping6 -I eth0 ff02::1 (realizar ping6 de pc1 a todos los nodos del enlace)

```
pc1:~# ping6 -I eth0 ff02::1
PING ff02::1(ff02::1) from fe80::214:23ff:feaa:d311 eth0: 56 data bytes
64 bytes from fe80::214:23ff:feaa:d311: icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from fe80::214:23ff:feaa:d322: icmp_seq=1 ttl=64 time=0.160 ms (DUP!)
64 bytes from fe80::214:22ff:feaa:d322: icmp_seq=1 ttl=64 time=0.212 ms (DUP!)
64 bytes from fe80::214:23ff:feaa:d311: icmp_seq=2 ttl=64 time=0.096 ms
64 bytes from fe80::214:23ff:feaa:d322: icmp_seq=2 ttl=64 time=0.305 ms (DUP!)
64 bytes from fe80::214:22ff:feaa:d322: icmp_seq=2 ttl=64 time=0.307 ms (DUP!)
```

El ping6 realizado desde pc1 a la dirección IPv6 multicast de todos los nodos del enlace funciona correctamente, donde se envían mensajes desde pc1 y se obtiene respuesta por parte de todos los nodos del enlace.

PREGUNTA 6
COMANDO: pc3:~# ctrl+c (interrumpir una captura de tráfico)

PREGUNTA 7
COMANDO: user@f-IX-pcX:~$ wireshark ipv6-03.cap (abrir una captura en wireshark)
Los paquetes 1 (envía desde pc1 a todos los nodos del enlace), 15 (envía desde pc2 a pc1), 87 (envía desde pc2 a pc1), 181 (envía desde pc3 a todos los nodos del enlace), 209 (envía desde pc1 a pc3), 218 (envía desde pc2 a pc1), 311 (envía desde pc1 a pc2) y 364 (envía desde pc2 a pc1) son mensajes de Neighbor Solicitation.
Estos mensajes son enviados por pc1, pc2 y pc3 a direcciones Ethernet específicas de cada máquina para solicitar la dirección IPv6 del nivel de enlace asociada a la dirección IPv6 que posee el mensaje, los cuales serán procesados si la dirección IPv6 multicast de nodo solicitado coincide.

PREGUNTA 8
COMANDO: pc1:~# ip neigh show (mostrar la caché de vecinos de pc1)
fe80::214:23ff:feaa:d322 dev eth0 lladdr 00:14:23:aa:d3:22 REACHABLE
fe80::214:22ff:feaa:d322 dev eth0 lladdr 00:14:22:aa:d3:22 STALE
COMANDO: pc2:~# ip neigh show (mostrar la caché de vecinos de pc2)
fe80::214:23ff:feaa:d311 dev eth0 lladdr 00:14:23:aa:d3:11 REACHABLE

PREGUNTA 9
COMANDO: pc3:~# ip neigh show (mostrar la caché de vecinos de pc3)
fe80::214:23ff:feaa:d311 dev eth0 lladdr 00:14:23:aa:d3:11 STALE

} 1.3 AUTOCONFIGURACIÓN DE DIRECCIONES IPv6 GLOBALES

PREGUNTA 1
COMANDO: pc4:~# tcpdump -i eth0 -s 0 -w /hosthome/ipv6-04.cap & (arrancar una captura de tráfico en &)
COMANDO: pc4:~# ip -6 addr show (mostrar dirección IPv6)
COMANDO: pc4:~# ip -6 maddr show dev eth0 (mostrar dirección IPv6 multicast de nodo solicitado en eth0)
La dirección IPv6 link-local configurada en pc4 es fe80::214:23ff:feaa:d388(/64).
Las direcciones IPv6 multicast de nodo solicitado configuradas son ff02::1:ffaa:d388 y ff02::1.
COMANDO: pc4:~# ip -6 route (mostrar las rutas IPv6 configuradas en pc4)
fe80::/64 dev eth0 metric 256 expires -1169sec mtu 1500 advmss 1440 hoplimit 4294967295
ff00::/8 dev eth0 metric 256 expires -1169sec mtu 1500 advmss 1440 hoplimit 4294967295

PREGUNTA 2
COMANDO: pc4:~# ip -6 addr show (mostrar dirección IPv6)
COMANDO: pc4:~# ip -6 maddr show dev eth0 (mostrar dirección IPv6 multicast de nodo solicitado en eth0)
Las direcciones IPv6 configuradas tras arrancar r2 son fe80::214:23ff:feaa:d388(/64) (link-local) y 2001:db8:300:300:214:23ff:feaa:d388(/64) (link-global).
Las direcciones IPv6 multicast de nodo solicitado configuradas por pc4 tras arrancar r2 son ff02::1:ffaa:d388 users 2 (indica que hay 2 usuarios) y ff02::1.
COMANDO: pc4:~# ip -6 route (mostrar las rutas IPv6 configuradas en pc4)
2001:db8:300:300::/64 dev eth0 proto kernel metric 256 expires 55sec mtu 1500 advmss 1440 hoplimit 4294967295
fe80::/64 dev eth0 metric 256 expires -1252sec mtu 1500 advmss 1440 hoplimit 4294967295
ff00::/8 dev eth0 metric 256 expires -1252sec mtu 1500 advmss 1440 hoplimit 4294967295
default via fe80::214:23ff:feaa:d377 dev eth0 proto kernel metric 1024 expires 25sec mtu 1500 advmss 1440 hoplimit 64

PREGUNTA 3
COMANDO: pc4:~# kill -SIGINT <PID captura> (matar el proceso que tiene abierto la captura en &)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-04.cap (abrir una captura en wireshark)
En la captura se pueden observar mensajes del tipo Neighbor Solicitation enviados a r2, a la dirección link-local y a la dirección link-global (paquetes 1, 4 y 8), Multicast Listener Report enviados a todos los nodos (paquetes 2, 3, 5 y 6) y Router Advertisement enviados por r2 a la dirección IPv6 multicast de nodo solicitado de todos los nodos del enlace (paquete 7, y del 9 al 24).
El último paquete de la captura que no es un Router Advertisement es el paquete 8 (Neighbor Solicitation), el cual se envía a la dirección link-global 2001:db8:300:300::/64.

PREGUNTA 4
COMANDO: pc4:~# ip neigh show (mostrar la caché de vecinos de pc4)
fe80::214:23ff:feaa:d377 dev eth0 lladdr 00:14:23:aa:d3:77 router STALE
COMANDO: r2:~# ip neigh show (mostrar la caché de vecinos de r2)
En el caso de la caché de vecinos de pc4, aparece la dirección IPv6 link-local de r2, ya que, como se ha visto en la captura, r2 está enviando contínuamente mensajes de Router Advertisement a pc4, lo que hace que pc4 se guarde en su caché de vecinos su dirección IPv6 link-local.
En el caso de r2, su caché de vecinos está vacía, ya que no recibe respuesta por parte de ningún otro router/máquina.

PREGUNTA 5
La dirección IPv6 global configurada en pc4 (2001:db8:300:300:214:23ff:feaa:d388(/64)) tiene configurados los valores de valid_lft = 54sec y preferred_lft = 24sec ejecutando el comando ip -6 addr show en pc4. Estos valores se ajustan a los que aparecen en los paquetes de Router Advertisement, que son valid_lft = 60sec y preferred_lft = 30sec.

PREGUNTA 6
COMANDO: r2:~# /etc/init.d/radvd stop (interrumpir el demonio radvd en r2)
COMANDO: r2:~# ip -6 addr show (mostrar dirección IPv6)
COMANDO: r2:~# ip neigh show (mostrar la caché de vecinos de r2)
Los valores de valid lft y preferred lft comienzan a decrecer conforme pasa el tiempo, ya que no reciben ningún mensaje de Router Advertisement con el cual actualizar esas variables. Una vez el valor de la variable Valid Lifetime llega a cero, la dirección IPv6 global de enlace de pc4 desaparece, y la caché de vecinos de pc4 se vacía, desapareciendo la dirección IPv6 de r2 que tenía guardada.

PREGUNTA 7
COMANDO: pc1:~# ip -6 addr show (mostrar dirección IPv6)
La dirección IPv6 global de pc1 es 2001:db8:100:100:214:23ff:feaa:d311(/64).
COMANDO: pc2:~# ip -6 addr show (mostrar dirección IPv6)
La dirección IPv6 global de pc2 es 2001:db8:100:100:214:23ff:feaa:d322(/64).
COMANDO: pc3:~# ip -6 addr show (mostrar dirección IPv6)
La dirección IPv6 global de pc3 es 2001:db8:100:100:214:22ff:feaa:d322(/64).

PREGUNTA 8
COMANDO: pc1:~# ip -6 addr show (mostrar dirección IPv6)
2001:db8:100:100::/64 dev eth0 proto kernel metric 256 expires 55sec mtu 1500 advmss 1440 hoplimit 4294967295
fe80::/64 dev eth0 metric 256 expires -5886sec mtu 1500 advmss 1440 hoplimit 4294967295
ff00::/8 dev eth0 metric 256 expires -5886sec mtu 1500 advmss 1440 hoplimit 4294967295
default via fe80::214:23ff:feaa:d344 dev eth0 proto kernel metric 1024 expires 25sec mtu 1500 advmss 1440 hoplimit 64
COMANDO: pc2:~# ip -6 addr show (mostrar dirección IPv6)
2001:db8:100:100::/64 dev eth0 proto kernel metric 256 expires 59sec mtu 1500 advmss 1440 hoplimit 4294967295
fe80::/64 dev eth0 metric 256 expires -5883sec mtu 1500 advmss 1440 hoplimit 4294967295
ff00::/8 dev eth0 metric 256 expires -5883sec mtu 1500 advmss 1440 hoplimit 4294967295
default via fe80::214:23ff:feaa:d344 dev eth0 proto kernel metric 1024 expires 29sec mtu 1500 advmss 1440 hoplimit 64
COMANDO: pc3:~# ip -6 addr show (mostrar dirección IPv6)
2001:db8:100:100::/64 dev eth0 proto kernel metric 256 expires 58sec mtu 1500 advmss 1440 hoplimit 4294967295
fe80::/64 dev eth0 metric 256 expires -13sec mtu 1500 advmss 1440 hoplimit 4294967295
ff00::/8 dev eth0 metric 256 expires -13sec mtu 1500 advmss 1440 hoplimit 4294967295
default via fe80::214:23ff:feaa:d344 dev eth0 proto kernel metric 1024 expires 28sec mtu 1500 advmss 1440 hoplimit 64
El campo expires es tomado por las máquinas de uno de los campos que posee los mensajes de Router Advertisement enviados por r1, el cual se refiere al número de segundos que las máquinas deben usar a r1 como router por defecto.

PREGUNTA 9
COMANDO: pc4:~# ping6 -I eth0 fe80::214:23ff:feaa:d311 (realizar ping6 de pc4 a pc1)

```
pc4:~# ping6 -I eth0 fe80::214:23ff:feaa:d311
PING fe80::214:23ff:feaa:d311(fe80::214:23ff:feaa:d311) from fe80::214:23ff:feaa:d388 eth0: 56 data bytes
From fe80::214:23ff:feaa:d388 icmp_seq=2 Destination unreachable: Address unreachable
From fe80::214:23ff:feaa:d388 icmp_seq=3 Destination unreachable: Address unreachable
From fe80::214:23ff:feaa:d388 icmp_seq=4 Destination unreachable: Address unreachable
```

COMANDO: pc4:~# ping6 -I eth0 2001:db8:100:100:214:23ff:feaa:d311 (realizar ping6 de pc4 a pc1)

```
pc4:~# ping6 -I eth0 2001:db8:100:100:214:23ff:feaa:d311
PING 2001:db8:100:100:214:23ff:feaa:d311(2001:db8:100:100:214:23ff:feaa:d311) from 2001:db8:300:300:214:23ff:feaa:d388 eth0: 56 data bytes
From 2001:db8:300:300:214:23ff:feaa:d377 icmp_seq=1 Destination unreachable: No route
From 2001:db8:300:300:214:23ff:feaa:d377 icmp_seq=2 Destination unreachable: No route
From 2001:db8:300:300:214:23ff:feaa:d377 icmp_seq=3 Destination unreachable: No route
From 2001:db8:300:300:214:23ff:feaa:d377 icmp_seq=4 Destination unreachable: No route
```

En este caso, he realizado un ping6 de pc4 a pc1, utilizando tanto la dirección local como la dirección global de pc1, y en ambos casos el ping6 no funciona, mostrando un mensaje de ‘Destino inalcanzable. No hay ruta en el caso de la dirección global, y un mensaje de ‘Dirección inalcanzable’ en el caso de la dirección local.

PREGUNTA 10

COMANDO: pc1:~# ping6 -I eth0 ff02::2 (realizar ping6 de pc1 a ff02::2)

```
PING ff02::2(ff02::2) from fe80::214:23ff:feaa:d311 eth0: 56 data bytes
64 bytes from fe80::214:23ff:feaa:d344: icmp_seq=1 ttl=64 time=6.28 ms
64 bytes from fe80::214:23ff:feaa:d344: icmp_seq=2 ttl=64 time=0.364 ms
64 bytes from fe80::214:23ff:feaa:d344: icmp_seq=3 ttl=64 time=0.622 ms
64 bytes from fe80::214:23ff:feaa:d344: icmp_seq=4 ttl=64 time=0.239 ms
```

Como se puede ver, solamente responde r1, ya que, aunque el ping se haya realizado desde pc1 a la dirección IPv6 destino ff02::2 que engloba a todos los routers, ya que r1 es el único router que se encuentra en el mismo nivel de enlace que pc1.

} 1.4 IPv6 ENTRE 2 MÁQUINAS DE SUBREDES DIFERENTES

PREGUNTA 1

Tanto en r1 como en r2 he configurado las siguientes rutas por defecto:

COMANDO: r1:~# ip route add default via fe80::214:23ff:feaa:d366 dev eth1 (añadir una ruta por defecto)

COMANDO: r2:~# ip route add default via fe80::214:23ff:feaa:d355 dev eth0 (añadir una ruta por defecto)

PREGUNTA 2

COMANDO: pc2:~# tcpdump -i eth0 -s 0 -w /hosthome/ipv6-05.cap (arrancar una captura de tráfico)

COMANDO: pc1:~# ping6 2001:db8:300:300:214:23ff:feaa:d388 (realizar ping6 de pc1 a pc4)

COMANDO: pc1:~# ping6 2001:db8:200:200:214:23ff:feaa:d366 (realizar ping6 de pc1 a r2)

COMANDO: pc2:~# ctrl+c (interrumpir una captura de tráfico)

COMANDO: user@f-lX-pcX:~$ wireshark ipv6-05.cap (abrir una captura en wireshark)

En el caso del ping6 de pc1 a pc4, el valor del hop limit de la respuesta es 62, ya que tiene que atravesar tanto r1 como r2. Por otro lado, en el caso del ping6 de pc1 a r2, el valor del hop limit de la respuesta es 63, ya que solo tiene que atravesar r1 para llegar a la máquina destino.

[] 2. FRAGMENTACIÓN EN IPv6

PREGUNTA 1
COMANDO: r1:~# tcpdump -i eth0 -s 0 -w /hosthome/ipv6-06.cap (arrancar una captura de tráfico)
COMANDO: r2:~# tcpdump -i eth0 -s 0 -w /hosthome/ipv6-07.cap (arrancar una captura de tráfico)
COMANDO: pc1:~# ping6 -s 2000 2001:db8:300:300:214:23ff:feaa:d388 (realizar ping6 de pc1 a pc4)
COMANDO: r1:~# ctrl+c (interrumpir una captura de tráfico)
COMANDO: r2:~# ctrl+c (interrumpir una captura de tráfico)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-06.cap (abrir una captura en wireshark)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-07.cap (abrir una captura en wireshark)
pc1 fragmenta el paquete antes de enviarlo a pc4, al igual que pc4 fragmenta el paquete antes de responder a pc1. Ambos saben cuál es su tamaño máximo de fragmentación, ya que el tamaño máximo del MTU en Ethernet es de 1500, además de estar así configurado en la interfaz eth0 de las máquinas. Por lo tanto, teniendo en cuenta el tamaño de la cabecera IPv6, la parte fragmentada debe de ser múltiplo de 8, excepto el último.

PREGUNTA 2
COMANDO: r1:~# ip link set eth1 mtu 1304 (modificar el valor de la MTU entre r1 y r2)
COMANDO: r2:~# ip link set eth0 mtu 1304 (modificar el valor de la MTU entre r1 y r2)
COMANDO: r1:~# tcpdump -i eth0 -s 0 -w /hosthome/ipv6-08.cap (arrancar una captura de tráfico)
COMANDO: r2:~# tcpdump -i eth0 -s 0 -w /hosthome/ipv6-09.cap (arrancar una captura de tráfico)
COMANDO: pc1:~# ping6 -s 1400 2001:db8:300:300:214:23ff:feaa:d388 (realizar ping6 de pc1 a pc4)
COMANDO: r1:~# ctrl+c (interrumpir una captura de tráfico)
COMANDO: r2:~# ctrl+c (interrumpir una captura de tráfico)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-08.cap (abrir una captura en wireshark)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-09.cap (abrir una captura en wireshark)
El valor de Next Header en las cabeceras de los paquetes es 58, indicando que la siguiente cabecera es del tipo ICMPv6.
Por lo tanto, teniendo en cuenta el tamaño de la cabecera IPv6, la parte fragmentada debe de ser múltiplo de 8, excepto el último.

PREGUNTA 3
Las máquinas pc1 y pc4 fragmentan sus propios paquetes antes de realizar el envío. Además, saben a qué tamaño máximo se deben fragmentar, ya que, al realizar el primer envío de pc1, recibe una respuesta de r1 indicando que el paquete enviado es demasiado grande para él y que debe fragmentarlo según el MTU que tenga configurado.

PREGUNTA 4
En la captura ipv6-08.cap aparece el mensaje “Packet Too Big” de r1 a pc1, mientras que en la captura ipv6-09.cap únicamente aparecen los mensajes de request y reply, sin tener en cuenta los mensajes de Router Advertisement.

[] 3. TÚNEL IPv6 IN IPv4

PREGUNTA 1
Los routers que deberían ser los extremos del túnel IPv6 dentro de IPv4 son r2 y r6, ya que son routers frontera que tienen la doble pila instalada, tanto IPv4 como IPv6, por lo que son capaces de comunicarse por IPv4 en una de sus interfaces y por IPv6 en la otra.

PREGUNTA 2
COMANDO: r2:~# ip tunnel add sit1 mode sit ttl 32 remote 14.211.0.6 local 11.211.0.2
COMANDO: r2:~# ip link set sit1 up
COMANDO: r2:~# ip -6 route add 2001:db8:400:400::/64 dev sit1 metric 1

PREGUNTA 3
COMANDO: r1:~# tcpdump -i eth1 -s 0 -w /hosthome/ipv6-tun-01.cap (arrancar una captura de tráfico)
COMANDO: r4:~# tcpdump -i eth1 -s 0 -w /hosthome/ipv6-tun-02.cap (arrancar una captura de tráfico)
COMANDO: r7:~# tcpdump -i eth1 -s 0 -w /hosthome/ipv6-tun-03.cap (arrancar una captura de tráfico)
COMANDO: pc1:~# ping6 2001:db8:400:400:214:22ff:fecc:d303 (realizar ping6 de pc1 a pc3)
Con la configuración actual, los ICMPv6 request pueden viajar por el túnel, sin embargo, al no estar configurado el otro extremo del túnel en r6 devolviendo un mensaje en el que indica que no se reconoce el protocolo.
COMANDO: r1:~# ctrl+c (interrumpir una captura de tráfico)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-tun-01.cap (abrir una captura de tráfico en wireshark)
COMANDO: r4:~# ctrl+c (interrumpir una captura de tráfico)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-tun-02.cap (abrir una captura de tráfico en wireshark)
COMANDO: r7:~# ctrl+c (interrumpir una captura de tráfico)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-tun-03.cap (abrir una captura de tráfico en wireshark)

PREGUNTA 4
COMANDO: r6:~# ip tunnel add sit1 mode sit ttl 32 remote 11.211.0.2 local 14.211.0.6
COMANDO: r6:~# ip link set sit1 up
COMANDO: r6:~# ip -6 route add 2001:db8:100:100::/64 dev sit1 metric 1

PREGUNTA 5
COMANDO: r1:~# tcpdump -i eth1 -s 0 -w /hosthome/ipv6-tun-04.cap (arrancar una captura de tráfico)
COMANDO: r4:~# tcpdump -i eth1 -s 0 -w /hosthome/ipv6-tun-05.cap (arrancar una captura de tráfico)
COMANDO: r7:~# tcpdump -i eth1 -s 0 -w /hosthome/ipv6-tun-06.cap (arrancar una captura de tráfico)
COMANDO: pc1:~# ping6 2001:db8:400:400:214:22ff:fecc:d303 (realizar ping6 de pc1 a pc3)

a)
COMANDO: r1:~# ctrl+c (interrumpir una captura de tráfico)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-tun-04.cap (abrir una captura de tráfico en wireshark)
COMANDO: r4:~# ctrl+c (interrumpir una captura de tráfico)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-tun-05.cap (abrir una captura de tráfico en wireshark)
COMANDO: r7:~# ctrl+c (interrumpir una captura de tráfico)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-tun-06.cap (abrir una captura de tráfico en wireshark)
En la captura realizada en r1, la versión del protocolo IP que hay en la cabecera IP que va detrás de la cabecera Ethernet es IPv6. En la captura realizada en r4, la versión del protocolo IP que hay en la cabecera IP que va detrás de la cabecera Ethernet es IPv4. En la captura realizada en r7, la versión del protocolo IP que hay en la cabecera IP que va detrás de la cabecera Ethernet es IPv6.

b)
En la captura realizada en r1, las direcciones IP origen y destino de esa cabecera son 2001:db8:100:100:214:22ff:feaa:d301 y 2001:db8:400:400:214:22ff:fecc:d303 para los request y 2001:db8:400:400:214:22ff:fecc:d303 y 2001:db8:100:100:214:22ff:feaa:d301 para los reply.
En la captura realizada en r4, las direcciones IP origen y destino de esa cabecera son 11.211.0.2 y 14.211.0.6 para los request y 14.211.0.6 y 11.211.0.2 para los reply. En este caso, las direcciones IP origen y destino se encuentran en IPv4 ya que el paquete IPv6 se ha encapsulado en una cabecera IPv4 para atravesar la zona de routers configurados con IPv4.
En la captura realizada en r7, las direcciones IP origen y destino de esa cabecera son 2001:db8:100:100:214:22ff:feaa:d301 y 2001:db8:400:400:214:22ff:fecc:d303 para los request y 2001:db8:400:400:214:22ff:fecc:d303 y 2001:db8:100:100:214:22ff:feaa:d301 para los reply.

c)
El Next Header en IPv6 en las capturas realizadas en r1 y r7 es ICMPv6 debido al mensaje que se envía.
El Protocol en IPv4 en la captura realizada en r4 es IPv6, ya que debe entregarse a IPv6, que es la capa de transporte TCP/IP.
El Hop Limit en IPv6 en la captura realizada en r1 es 64 en los request y 60 en los replies.
El TTL en IPv4 en la captura realizada en r4 es 30 en los request y 31 en los replies.
El Hop Limit en IPv6 en la captura realizada en r7 es 60 en los request y 64 en los replies.

d)
El Next Header en IPv6 en las capturas realizadas en r1 y r7 es ICMPv6 debido al mensaje que se envía.
El Protocol en IPv4 en la captura realizada en r4 es IPv6, ya que debe entregarse a IPv6, que es la capa de transporte TCP/IP.

e)
En IPv4 el contenido del datagrama es la cabecera IPv4 más la cabecera IPv6 y los datos en IPv6, por otro lado, en IPv6, encontramos únicamente su cabecera y los datos.

PREGUNTA 6
En r1 (eth1) se capturan todos los paquetes que envía pc2 a pc4, ya que es necesario que atraviesen ese router si se quiere llegar a pc4.
En r4 (eth1) se capturan todos los paquetes menos los 6 primeros, ya que los 3 primeros llegan a r1, posteriormente a r2 y de ahí llegan a r6 habiendo pasado previamente por r4.
En r7 (eth1) se capturan los 6 últimos paquetes, ya que sería la última y penúltima secuencia de paquetes que envía pc2 antes de que llegue a su destino (pc4).

PREGUNTA 7
COMANDO: r1:~# tcpdump -i eth1 -s 0 -w /hosthome/ipv6-tun-07.cap (arrancar una captura de tráfico)
COMANDO: r4:~# tcpdump -i eth1 -s 0 -w /hosthome/ipv6-tun-08.cap (arrancar una captura de tráfico)
COMANDO: r7:~# tcpdump -i eth1 -s 0 -w /hosthome/ipv6-tun-09.cap (arrancar una captura de tráfico)
COMANDO: pc1:~# traceroute6 -z 200 2001:db8:400:400:214:22ff:fecc:d303 (traza la ruta de pc2 a pc4)

PREGUNTA 8
COMANDO: r1:~# ctrl+c (interrumpir una captura de tráfico)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-tun-07.cap (abrir una captura de tráfico en wireshark)
COMANDO: r4:~# ctrl+c (interrumpir una captura de tráfico)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-tun-08.cap (abrir una captura de tráfico en wireshark)
COMANDO: r7:~# ctrl+c (interrumpir una captura de tráfico)
COMANDO: user@f-lX-pcX:~$ wireshark ipv6-tun-09.cap (abrir una captura de tráfico en wireshark)
En la captura en r1, el Hop Limit incrementa de 1 a 5, conforme van llegando a las distintas máquinas intermedias hasta llegar a la máquina final pc4.
En la captura en r4, el TTL disminuye debido al paso del paquete por máquinas intermedias, y el Hop Limit, al igual que en la anterior captura, incrementa de 1 a 5, sin embargo su valor no aumenta a pesar de pasar por más máquinas intermedias debido a que el protocolo que se maneja en esa zona es IPv4 y no IPv6.
En la captura en r7, el Hop Limit incrementa de 1 a 3, conforme van llegando a las distintas máquinas intermedias hasta llegar a la máquina final pc4.

PREGUNTA 9
Los valores de Hop Limit únicamente aumentan cuando el protocolo que se maneja en la zona donde se encuentra el paquete es IPv6, por ello, no aumenta al atravesar la zona en la que las máquinas se encuentran configuradas en IPv4, en ese caso, disminuye el TTL.

PREGUNTA 10
No es posible que conozca que se ha atravesado un túnel para llegar a pc4, ya que el tráfico que envía y recibe de pc2, se realiza en IPv6, donde pc2 únicamente envía el mensaje y espera una respuesta en el mismo tipo de protocolo empleado en su envío.