

Trabajo práctico - Comunicaciones

Delfina Martín - Francisco Alcacer

22 de noviembre de 2020

1. Análisis de aspectos de IPv6 sobre PCs y sus enlaces

Se capturaron paquetes en Wireshark. Una de las capturas obtenidas se muestra en (1)

The image shows the Wireshark network protocol analyzer interface. The title bar reads "Capture00000002.pcapng". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like opening files, saving, zooming, and navigating through the packet list. The packet list pane on the left shows a single packet selected, with the filter "ipvs" applied. The packet details pane on the right shows the structure of the selected packet, which is an ICMPv6 message. The packet list pane contains the following data:

No.	Time	Source	Destination	Protocol	Length	Info
761	67.103948487	fe80::cad7:19ff:fe9...ff02::1		ICMPv6	118	Router Advertisement from c8:07:19:9c:bb:3e
762	67.114255218	fe80::640e:a8f0:4ac...ff02::1		ICMPv6	130	Multicast Listener Report Message v2
763	67.966254662	fe80::640e:a8f0:4ac...ff02::1		ICMPv6	130	Multicast Listener Report Message v2

Figura 1: Captura de paquetes - Wireshark

Se verificó la conectividad con el propio equipo.

```

PING :: (::1) 56 data bytes
64 bytes from ::1: icmp_seq=1 ttl=64 time=0.099 ms
64 bytes from ::1: icmp_seq=2 ttl=64 time=0.028 ms
64 bytes from ::1: icmp_seq=3 ttl=64 time=0.028 ms
64 bytes from ::1: icmp_seq=4 ttl=64 time=0.039 ms
64 bytes from ::1: icmp_seq=5 ttl=64 time=0.039 ms
64 bytes from ::1: icmp_seq=6 ttl=64 time=0.058 ms
64 bytes from ::1: icmp_seq=7 ttl=64 time=0.044 ms
64 bytes from ::1: icmp_seq=8 ttl=64 time=0.029 ms
64 bytes from ::1: icmp_seq=9 ttl=64 time=0.044 ms
64 bytes from ::1: icmp_seq=10 ttl=64 time=0.052 ms
64 bytes from ::1: icmp_seq=11 ttl=64 time=0.043 ms
64 bytes from ::1: icmp_seq=12 ttl=64 time=0.044 ms
64 bytes from ::1: icmp_seq=13 ttl=64 time=0.041 ms
64 bytes from ::1: icmp_seq=14 ttl=64 time=0.044 ms
64 bytes from ::1: icmp_seq=15 ttl=64 time=0.044 ms
64 bytes from ::1: icmp_seq=16 ttl=64 time=0.039 ms
64 bytes from ::1: icmp_seq=17 ttl=64 time=0.044 ms
64 bytes from ::1: icmp_seq=18 ttl=64 time=0.044 ms
64 bytes from ::1: icmp_seq=19 ttl=64 time=0.059 ms
64 bytes from ::1: icmp_seq=20 ttl=64 time=0.071 ms
64 bytes from ::1: icmp_seq=21 ttl=64 time=0.071 ms
64 bytes from ::1: icmp_seq=22 ttl=64 time=0.059 ms
64 bytes from ::1: icmp_seq=23 ttl=64 time=0.062 ms
[Ctrl]+C: Stopped
[Ctrl]+C: -s -i ping ::1

```

Figura 2: Conectividad - Loopback

2. Análisis sobre red simulada

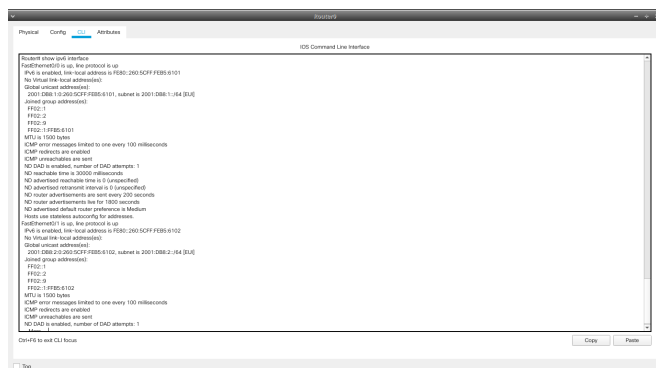
2.1. Tarea 1

Se siguió el paso a paso para reproducir la red.

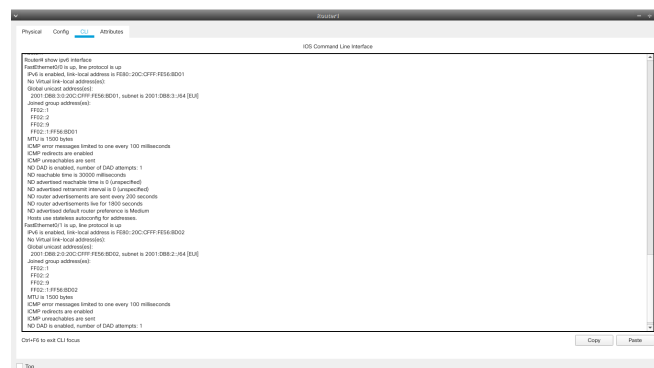
2.2. Tarea 2

2.2.1. Inciso a

Se verificó que las interfaces sobre cada router hayan sido configuradas para soportar IPv6.



(a) Interfaces IPv6 en Router0



(b) Interfaces IPv6 en Router1

Figura 3: Interfaces IPv6 en routers

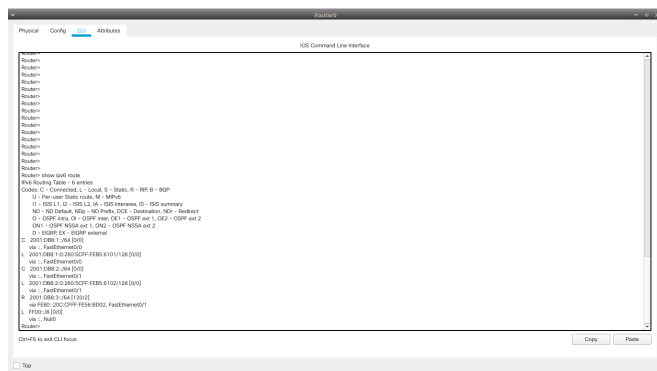
2.2.2. Inciso b

Dispositivo		IPv6 habilitado	Dirección IP Local	Dirección IP Global
Router0	Fa0/0	Si	FE80::260:5CFF:FEB5:6101	2001:DB8:1:0:260:5CFF:FEB5:6101
	Fa0/1	Si	FE80::260:5CFF:FEB5:6102	2001:DB8:2:0:260:5CFF:FEB5:6102
Router1	Fa0/0	Si	FE80::20C:CFFF:FE56:BD01	2001:DB8:3:0:20C:CFFF:FE56:BD01
	Fa0/1	Si	FE80::20C:CFFF:FE56:BD02	2001:DB8:2:0:20C:CFFF:FE56:BD02

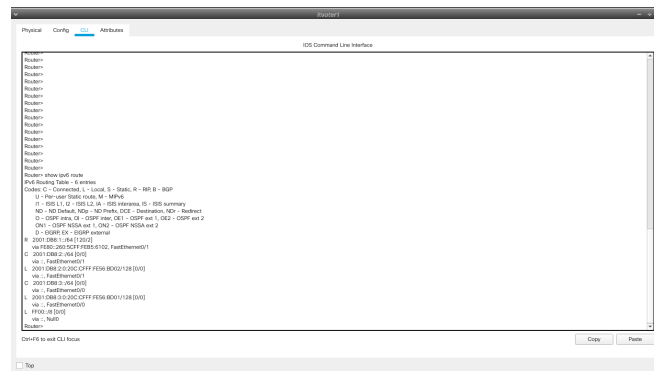
- Todas las direcciones IP versión 6 tienen 128 bits divididos en 8 nibbles (16 bits).
- El prefijo de la subred para la interface Fa0/0 del Router0 es 2001:DB8:1:0:/64 - dirección de la red (3 primeros nibbles) + dirección de la subred (4to nibble) + agregado de ceros. El ID de la interface es 260:5CFF:FEB5:6101 (últimos 4 nibbles)
- La dirección MAC de la interface Fa0/0 del Router0 es 00:60:5C:B5:61:01 y se obtiene de la dirección IP con el algoritmo EUI64 que se describe a continuación:
 - tomamos los primeros 8 bits de la interface e invertimos el 6to bit (contando desde 0)
 - agregamos los nuevos 8 bits en la posición de donde los extrajimos
 - eliminamos el fragmento "FFEE" del centro de la dirección
 - escribimos los bits con la notación de direcciones MAC

2.2.3. Inciso c

Se verificaron las tablas de ruteo para cada router.



(a) Tabla de ruteo en Router0

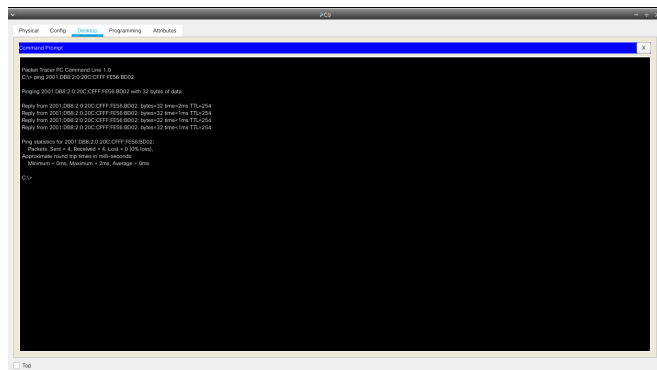


(b) Tabla de ruteo en Router1

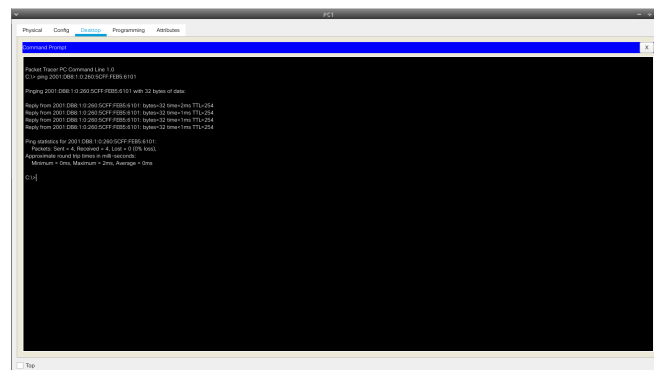
Figura 4: Tablas de ruteo

2.2.4. Inciso d

Se verificó la conectividad extremo a extremo entre PCs.



(a) Verificación extremo a extremo desde PC0



(b) Verificación extremo a extremo desde PC1

Figura 5: Conexión extremo a extremo

2.3. Tarea 3

Se realizó la simulación paso a paso habiendo hecho un ping desde la PC0 a la PC1.

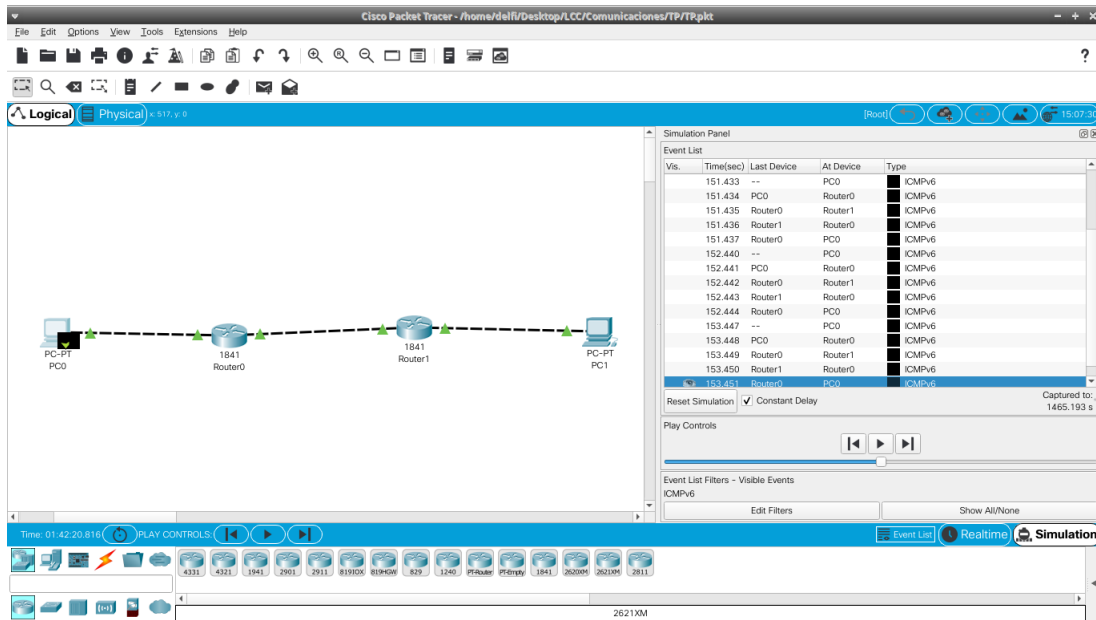


Figura 6: Resultado de la simulación

El flujo de datos observados es el siguiente:

- se envía un mensaje de la PC0 al Router0
- se envía un mensaje del Router0 al Router1
- se envía un mensaje del Router1 al Router0
- se envía un mensaje del Router0 a la PC0
- se repite el ciclo a-d dos veces más

El encabezado del primer mensaje se ve como sigue:

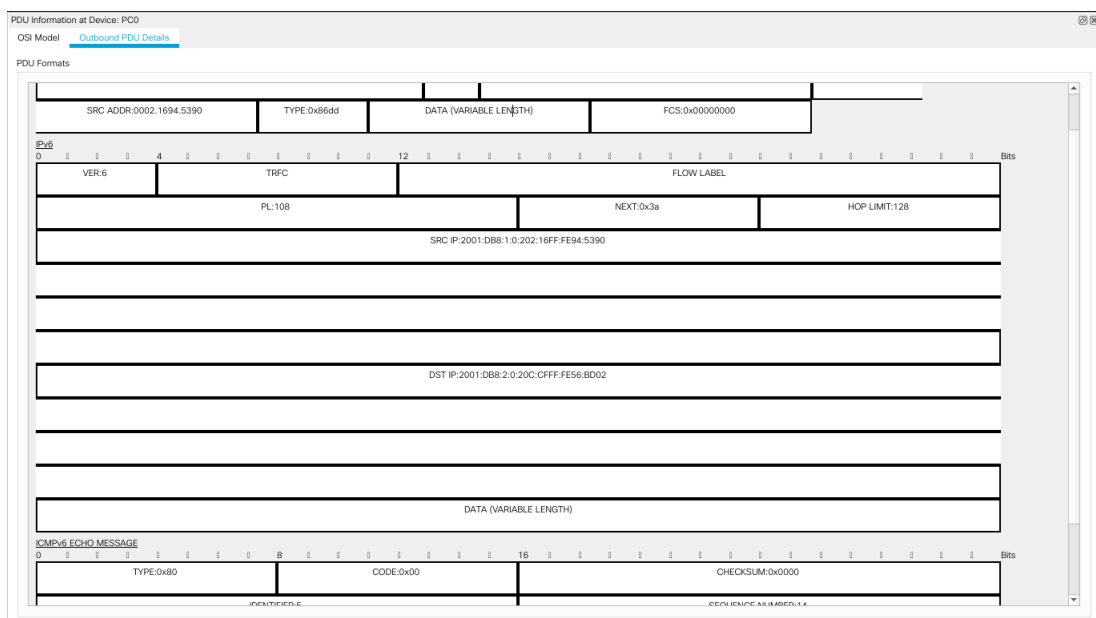


Figura 7: Cabecera de un mensaje ICMP

2.3.1. Inciso d

Mensaje ICMPv6 de Router 0 a Router 1:

Tipo:0x86dd

Dirección fuente:0060.6CB5.6102

Dirección destino:000C.CF56.BD0

Dato:-

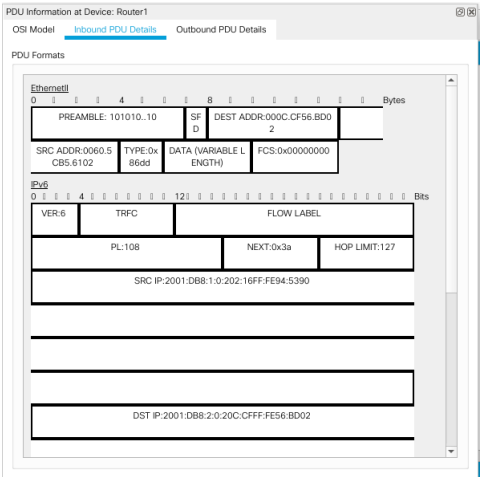


Figura 8: Mensaje ICMPv6 de Router 0 a Router 1

Mensaje ICMPv6 de Router 1 a Router 2:

Tipo:0x86dd

Dirección fuente:000C.CF56.BD0

Dirección destino:0060.6CB5.6102

Dato:-

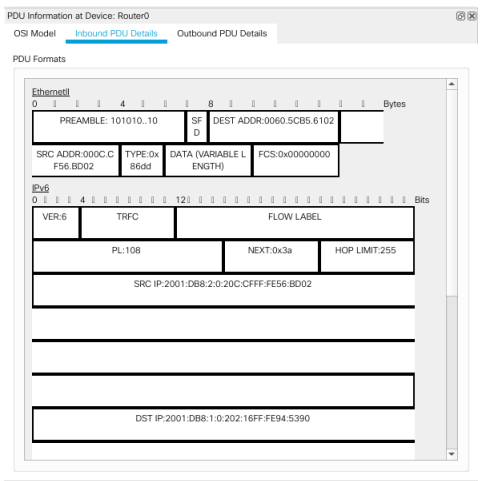


Figura 9: Mensaje ICMPv6 de Router 1 a Router 0