Comunicaciones

Trabajo Práctico nº1

Augusto Rabbia,
Manuel Spreutels

1ro de Octubre

Ejercicio 1:

Ejecutamos el comando **ipconfig**:

c)

```
C:\Users\rabbi>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : wifi-abierta.fceia.unr.edu.ar
   Link-local IPv6 Address . . . . . : fe80::a92e:9a64:645a:8e76%14
   IPv4 Address. . . . . . . . . . . : 10.66.91.158
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.66.91.1
```

Vemos que se nos asignó una dirección IPv4, una IPv6, y conocemos la IP de la puerta de enlace predeterminada.

d)

```
C:\Users\rabbi>ping ::1

Pinging ::1 with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Al haber recibido una respuesta en el ping, sabemos que tenemos conectividad.

e) Cuando ejecutamos el comando ping, obtenemos los siguientes resultados:

```
alumno@pelle016:~$ ping6 -I enp1s0 fe80::87b:f9b0:75f0:1ca9
ping6: Warning: source address might be selected on device other than: enp1s0
PING fe80::87b:f9b0:75f0:1ca9(fe80::87b:f9b0:75f0:1ca9) from :: enp1s0: 56 data bytes
64 bytes from fe80::87b:f9b0:75f0:1ca9%enp1s0: icmp_seq=1 ttl=64 time=0.616 ms
64 bytes from fe80::87b:f9b0:75f0:1ca9%enp1s0: icmp_seq=2 ttl=64 time=0.358 ms
64 bytes from fe80::87b:f9b0:75f0:1ca9%enp1s0: icmp_seq=3 ttl=64 time=0.554 ms
64 bytes from fe80::87b:f9b0:75f0:1ca9%enp1s0: icmp_seq=4 ttl=64 time=0.400 ms
64 bytes from fe80::87b:f9b0:75f0:1ca9%enp1s0: icmp_seq=5 ttl=64 time=0.406 ms
64 bytes from fe80::87b:f9b0:75f0:1ca9%enp1s0: icmp_seq=6 ttl=64 time=0.534 ms
64 bytes from fe80::87b:f9b0:75f0:1ca9%enp1s0: icmp_seq=7 ttl=64 time=0.230 ms
64 bytes from fe80::87b:f9b0:75f0:1ca9%enp1s0: icmp_seq=8 ttl=64 time=0.214 ms
64 bytes from fe80::87b:f9b0:75f0:1ca9%enp1s0: icmp_seq=9 ttl=64 time=0.225 ms
64 bytes from fe80::87b:f9b0:75f0:1ca9%enp1s0: icmp_seq=10 ttl=64 time=0.440 ms
64 bytes from fe80::87b:f9b0:75f0:1ca9%enp1s0: icmp_seq=11 ttl=64 time=0.533 ms
64 bytes from fe80::87b:f9b0:75f0:1ca9%enp1s0: icmp_seq=12 ttl=64 time=0.482 ms
^C
--- fe80::87b:f9b0:75f0:1ca9 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11267ms
rtt min/avg/max/mdev = 0.214/0.416/0.616/0.131 ms
```

f) Afortunadamente, Wireshark interpreta los campos de las cabeceras, dandonos el significado de los campos de bits para que podamos entenderlos en lenguaje humano.

Primero que nada, vemos que, como era de esperar, las direcciones en la cabecera están invertidas. Notemos que el paquete no tiene ninguna cabecera de extensión, sino que el Next Header es 58 en ambos casos.

Por otro lado, se puede ver que las direcciones de los paquetes son direcciones Local-Link.

Finalmente, vemos que la solicitud ICMP tiene tipo 128 (echo request) en la solicitud y 129 (echo reply) en la respuesta.

- Cabecera de la solicitud:

```
▾ Internet Protocol Version 6, Src: fe80::8f04:3d9d:e48b:36df, Dst: fe80::87b:f9b0:75f0:1ca9
    0110 .... = Version: 6
  ▶ .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0111 1001 0010 1101 1101 = Flow Label: 0x792dd
    Payload Length: 64
    Next Header: ICMPv6 (58)
    Hop Limit: 64
    Source: fe80::8f04:3d9d:e48b:36df
    Destination: fe80::87b:f9b0:75f0:1ca9
▾ Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0x5989 [correct]
    [Checksum Status: Good]
    Identifier: 0x0003
    Sequence: 14
    [Response In: 2]
```

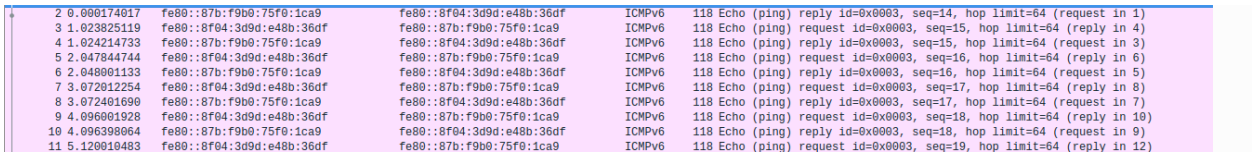
- Cabecera de la respuesta:

```
▾ Internet Protocol Version 6, Src: fe80::87b:f9b0:75f0:1ca9, Dst: fe80::8f04:3d9d:e48b:36df
    0110 .... = Version: 6
  ▶ .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1111 1011 0101 1110 1010 = Flow Label: 0xfb5ea
    Payload Length: 64
    Next Header: ICMPv6 (58)
    Hop Limit: 64
    Source: fe80::87b:f9b0:75f0:1ca9
    Destination: fe80::8f04:3d9d:e48b:36df
▾ Internet Control Message Protocol v6
    Type: Echo (ping) reply (129)
    Code: 0
    Checksum: 0x5889 [correct]
    [Checksum Status: Good]
    Identifier: 0x0003
    Sequence: 14
    [Response To: 1]
    [Response Time: 0,174 ms]
  ▾ Data (56 bytes)
      Data: 6ecd15650000000064110500000000010111213141516 17…
      [Length: 56]

0000  1c 1b 0d 1f c5 c3 1c 1b  0d 31 34 d0 86 dd 60 0f   ·········· ·14···`·
0010  b5 ea 00 40 3a 40 fe 80  00 00 00 00 00 00 08 7b   ···@:@·· ·······{
0020  f9 b0 75 f0 1c a9 fe 80  00 00 00 00 00 00 8f 04   ··u····· ········
0030  3d 9d e4 8b 36 df 81 00  58 89 00 03 00 0e 6e cd   =···6··· X·····n·
0040  15 65 00 00 00 00 64 11  05 00 00 00 00 00 10 11   ·e····d· ········
0050  12 13 14 15 16 17 18 19  1a 1b 1c 1d 1e 1f 20 21   ·------- ------ !
0060  22 23 24 25 26 27 28 29  2a 2b 2c 2d 2e 2f 30 31   "#$%&'() *+,-./01
0070  32 33 34 35 36 37                                 234567
```

g) No encontramos ningún paquete relativo al proceso de Network Discovery. Según nuestro entendimiento, esto probablemente se debe a que la computadora llevaba un tiempo prendida y ya se había realizado.

Por otro lado, los paquetes ICMP, con sus direcciones de origen y destino son los siguientes:



2	0.000174017	fe80::87b:f9b0:75f0:1ca9	fe80::8f04:3d9d:e48b:36df	ICMPv6	118	Echo (ping) reply id=0x0003, seq=14, hop limit=64 (request in 1)
3	1.023825119	fe80::8f04:3d9d:e48b:36df	fe80::87b:f9b0:75f0:1ca9	ICMPv6	118	Echo (ping) request id=0x0003, seq=15, hop limit=64 (reply in 4)
4	1.024214733	fe80::87b:f9b0:75f0:1ca9	fe80::8f04:3d9d:e48b:36df	ICMPv6	118	Echo (ping) reply id=0x0003, seq=15, hop limit=64 (request in 3)
5	2.047844744	fe80::8f04:3d9d:e48b:36df	fe80::87b:f9b0:75f0:1ca9	ICMPv6	118	Echo (ping) request id=0x0003, seq=16, hop limit=64 (reply in 6)
6	2.048001133	fe80::87b:f9b0:75f0:1ca9	fe80::8f04:3d9d:e48b:36df	ICMPv6	118	Echo (ping) reply id=0x0003, seq=16, hop limit=64 (request in 5)
7	3.072012254	fe80::8f04:3d9d:e48b:36df	fe80::87b:f9b0:75f0:1ca9	ICMPv6	118	Echo (ping) request id=0x0003, seq=17, hop limit=64 (reply in 8)
8	3.072401690	fe80::87b:f9b0:75f0:1ca9	fe80::8f04:3d9d:e48b:36df	ICMPv6	118	Echo (ping) reply id=0x0003, seq=17, hop limit=64 (request in 7)
9	4.096001928	fe80::8f04:3d9d:e48b:36df	fe80::87b:f9b0:75f0:1ca9	ICMPv6	118	Echo (ping) request id=0x0003, seq=18, hop limit=64 (reply in 10)
10	4.096398064	fe80::87b:f9b0:75f0:1ca9	fe80::8f04:3d9d:e48b:36df	ICMPv6	118	Echo (ping) reply id=0x0003, seq=18, hop limit=64 (request in 9)
11	5.120010483	fe80::8f04:3d9d:e48b:36df	fe80::87b:f9b0:75f0:1ca9	ICMPv6	118	Echo (ping) request id=0x0003, seq=19, hop limit=64 (reply in 12)

Wireshark nos provee la posibilidad de verificar cuáles paquetes son enviado como respuesta a otros. Los tipos de mensajes fueron discutidos en el anterior punto.

Ejercicio 2:

Tarea 2)

Habiendo ejecutado el comando show ipv6 interface en el modo administrador del CLI de cada Router, obtuvimos la siguiente información:

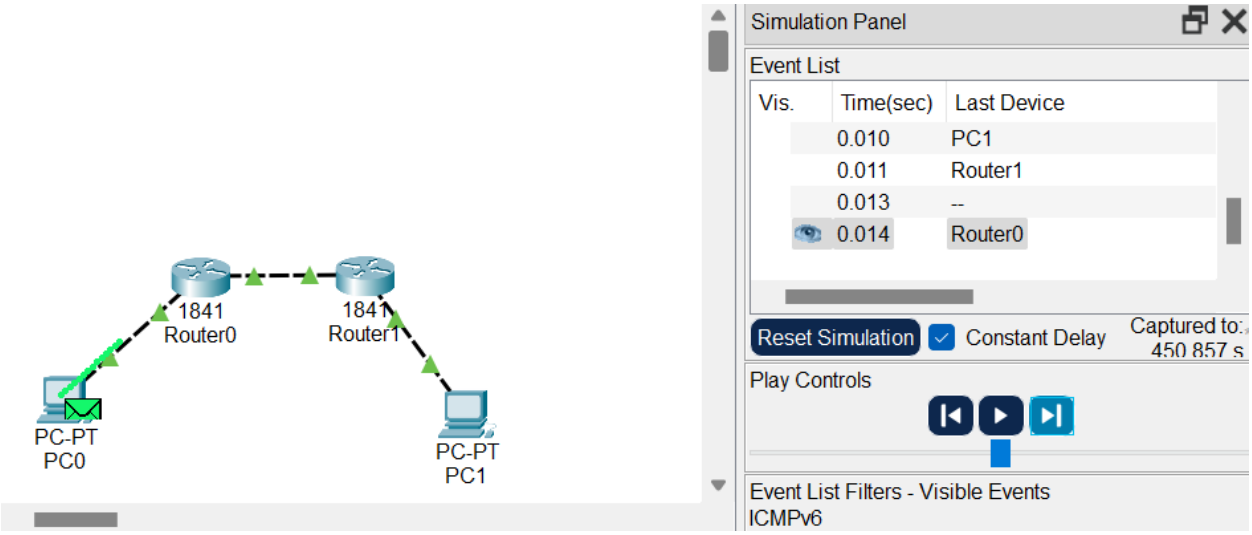
Dispositivo		IPv6 habilitado	Dirección IP Local	Dirección IP Global
Routers0	Fa0/0	SI	FE80::2D0:D3FF:FEB4:1301	2001:DB8:1:0:2D0:D3FF:FEB4:1301
	Fa0/1	SI	FE80::2D0:D3FF:FEB4:1302	2001:DB8:2:0:2D0:D3FF:FEB4:1302
Routers1	Fa0/0	SI	FE80::205:5EFF:FE41:601	2001:DB8:3:0:205:5EFF:FE41:601
	Fa0/1	SI	FE80::205:5EFF:FE41:602	2001:DB8:2:0:205:5EFF:FE41:602

Todas las IPs tenian una máscara de subred de 64 bits.

a. 128
b. No tiene subnet ID, ya que su máscara de subred es de 64 bits. La ID de la interfaz son los últimos 64 bits, es decir, 2D0:D3FF:FEB4:1301.
c. La dirección MAC es: 00D0.D3D4.1301. Se relaciona con la dirección IP ya que la IP fue asignada utilizando el método de EUI. En este, se crea una IPv6 utilizando los primeros 24 bits de la dirección IP con el 7mo bit invertido, llevando el primer hexadecimal de 00 a 02, en el medio, se inserta FF FE, y los últimos 24 bits simplemente se copian de la dirección MAC.

Tarea 3)

d) Utilizar la herramienta del sobre envía un paquete ICMPv6 del tipo Echo. La PC0 envía un paquete a la PC1 de tipo 128, y recibe un paquete de tipo 129 de vuelta desde esta última. Estos son mensajes de tipo Echo Request y Echo Reply. Esta simulación nos permite verificar que existe una conexión entre los dos hosts.



Tarea 4)
Mensaje ICMPv6: Tipo 128
Dirección Fuente: 2001:DB8:1:0:205:5EFF:FE06:A9D2
Dirección Destino: 2001:DB8:3:0:201:C9FF:FE63:5AEB
Dato: El payload no contiene información.

Mensaje ICMPv6: Tipo 129
Dirección Fuente: 2001:DB8:3:0:201:C9FF:FE63:5AEB
Dirección Destino: 2001:DB8:1:0:205:5EFF:FE06:A9D2
Dato: El payload no contiene información.

Mensaje ICMPv6: Tipo 133
Dirección Fuente: FE80::205:5EFF:FE06:A9D2
Dirección Destino: FF02::2 - Esto significa que se envió un mensaje multicast al grupo FF02::2.
Dato: El payload no contiene información.

Mensaje ICMPv6: Tipo 134
Dirección Fuente: FE80::2D0:D3FF:FEB4:1301

Dirección Destino: FF02::1
Dato: El payload no contiene información.

Aquí, podemos ver que se utilizan direcciones multicast para enviar mensajes de tipo 133 (Router Solicitation) a todos los routers del enlace (al ser una dirección de la forma FF02::2), y el router le responde con un mensaje de tipo 134 (Router Advertisement), a todos los equipos en el enlace (FF02::1).

Conclusión

El protocolo IPv6 representa una evolución fundamental en la arquitectura de Internet. IPv6, además de solucionar el problema de las limitadas direcciones IPv4, introduce una estructura de cabecera más eficiente y simplificada, lo que mejora el rendimiento y reduce la sobrecarga de procesamiento en los enrutadores. De esta forma, incrementa la escalabilidad y eficiencia de las redes.

Las diferentes tipos de direcciones IP en IPv6 son de gran utilidad, agregando seguridad y eficiencia en las redes. Las direcciones Unique Global permiten la comunicación global a través del Internet. Las direcciones Unique Local, por otro lado, son ideales para redes privadas o locales, como intranets, ya que no se enrutan en Internet y brindan un mayor control sobre las direcciones IP internas sin el riesgo de conflictos de direcciones globales. Por último, las direcciones Link Local son esenciales para la comunicación dentro de una red local o segmento de red, como en una LAN, y no se enrutan más allá de ese segmento.

Los mensajes ICMPv6, incluyendo los tipos como Echo Request/Reply, son esenciales para la resolución de problemas y el mantenimiento de la red en IPv6, proporcionando información sobre el estado de la red y permitiendo el diagnóstico de problemas.

Por último, herramientas como Wireshark y Cisco Packet Tracer nos permiten analizar redes IPv6 y monitorear el tráfico en una red, y son herramientas útiles para el estudio de las comunicaciones.