El protocolo IPv6

Integrantes:

Martín Moloeznik, Nicolás Paz Reyes

martinmoloeznik@gmail.com, rubenpaz2105@gmail.com

Repositorio: `https://github.com/N1C0-P4Z/Protocolo-IPv6`

27 de marzo de 2025

Índice

Introducción

El protocolo IPv6 fue desarrollado para reemplazar a IPv4 debido a la necesidad de una mayor cantidad de direcciones IP en el mundo. Dentro de IPv6 existen mecanismos esenciales para la configuración de direcciones y la comunicación entre dispositivos, entre los cuales se destacan SLAAC, EUI-64 y el protocolo Neighbor Discovery (NDP).

1. IPv6 SLAAC and EUI-64 Basics

1.1. Configuración del Router en IPv6

Mediante los siguientes comandos configuramos la Link Local Address del router a fe80::1 y la GUA a 2001:db8:acad:1::1/64.

```
Router#enable
Router#configure terminal
Router(config)#ipv6 unicast-routing
Router(config)#interface g0/0
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 address fe80::1 link-local
Router(config-if)#ipv6 address 2001:db8:acad:1::1/64
Router(config-if)#no shutdown
```

1.2. Explicacion algoritmo EUI-64

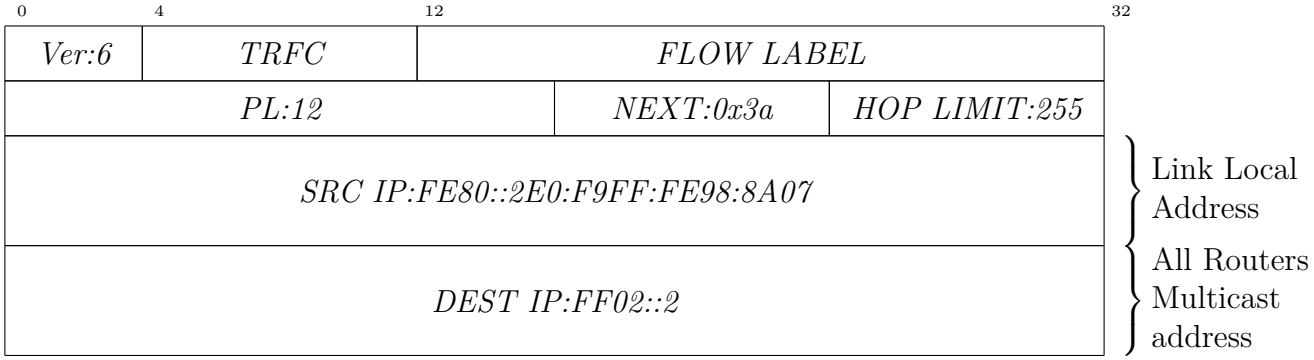
La PC se autoconfigura su Link Local Addres siguiendo los pasos a continuacion:

48 bit MAC	*00-E0-F9-98-8A-07*
Separa al medio	*00-E0-F9 / 98-8A-07*
Insertar FF-FE	*00-E0-F9* ***FF-FE*** *98-8A-07*
Primeros dos hexa a binario	*0000-0000-E0-F9* ***FF-FE*** *98-8A-07*
Se invierte el septimo bit	*0000-001**0**-E0-F9* ***FF-FE*** *98-8A-07*
64 bits host interface ID	***02****-E0-F9-****FF-FE****-98-8A-07*
Link Local Address	*FE80::****2E0:F9FF:FE98:8A07***

Algoritmo EUI-64

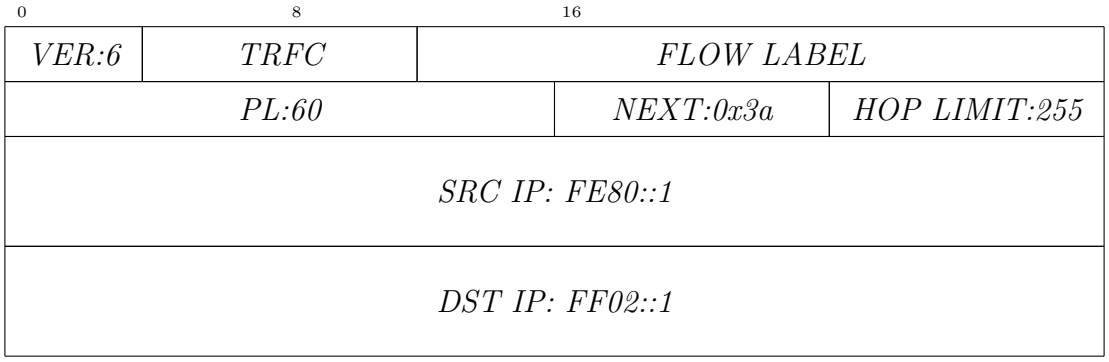
1.3. Router Solicitation

Luego entramos al modo simulación y cambiamos la configuración ipv6 de la pc de static a auto-config, inmediatamente, la pc envía un mensaje de router solicitation. Donde la ip de origen es la LLA de la pc que se autoconfiguró mediante EUI-64 y la ip destino es la ALL routers multicast address.

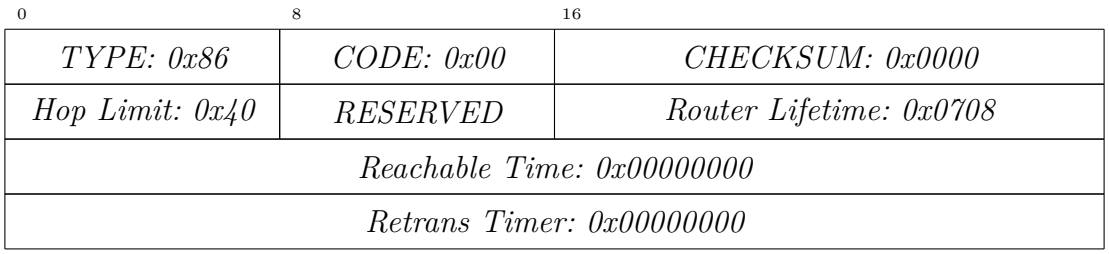


1.4. Router Advertisement

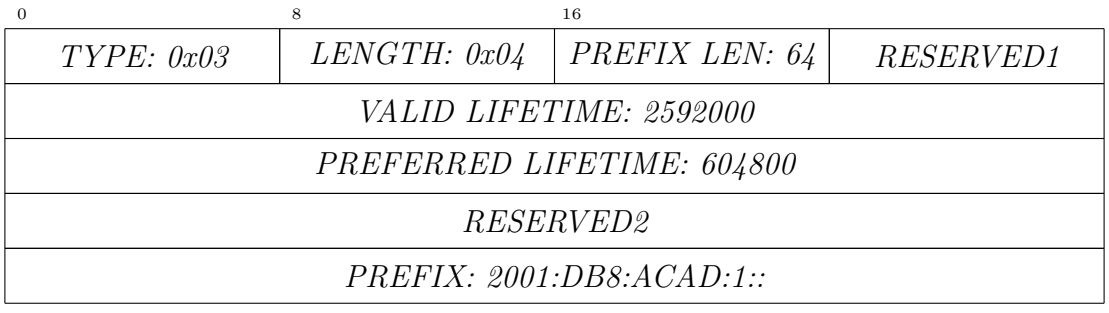
La PC aprende que se esta usando IPv6 y a la LLA del router que usará como gateway.



El router responde con el siguiente mensaje de Router Advertisement:



Prefix Option



Aquí la PC aprende el prefijo de red, su tamaño, el tipo y por cuanto tiempo es valida esta informacion. De esta forma, la PC se autoconfigura su IPv6 Global Unicast Address,

ya que tiene todos los elementos necesarios. Usará como interface ID lo que ya aprendio usando el algoritmo EUI-64.

0	8	16
TYPE: 0x01	*LENGTH: 0x01*	
LINK LAYER ADDRESS: 0060.3E5A.5801		

En este mensaje, la PC aprende la Link Layer Address del Router.

2. Neighbor Discovery

Configuramos las IPs de las PCs y el Router con los comandos que vimos en el apartado anterior. Luego nos aseguramos que el R0 no tenga información de sus vecinos con

R0#show ipv6 neighbors

2.1. Local Delivery

Realizaremos un ping desde la consola de P0 a P1 en el modo simulación, filtrando los mensajes ICMPv6 y NDP para visualizarlos en la *Event List*

2.1.1. Mensaje NDP

En el tercer evento vemos que la PC0 envia un PDU NDP al Switch0. Este PDU va a ser de tipo 135 Neighbor Solicitation, con el objetivo de descubrir la dirección MAC de los otros dispositivos en la misma red local. El mensaje de Neighbor Solicitation se ve representado de la siguiente manera:

0			8	16
TYPE: 0x87			*CODE: 0x00*	*CHECKSUM*
R	*S*	*O*	*Reserved*	
Target Address: 2001:DB8:ACAD:1::B				

En TYPE se muestra en hexadecimal 0x87, que en decimal es 135, confirmando que el mensaje es de tipo Neighbor Solicitation. En el 4to y 5to evento vemos que el Switch hizo forward del NDP a la PC1 y al Router.

La respuesta va a ser una PDU NDP de tipo Neighbor Advertisement, es decir Type 136(0x87 en hexadecimal).

0			8	16
TYPE: 0x88			*CODE: 0x00*	*CHECKSUM*
R	*S*	*O*	*Reserved*	
Target Address: 2001:DB8:ACAD:1::B				

Esta respuesta llega al Switch, el cual nuevamente fordwardea por todas sus interfaces, menos por la que recibió el mensaje. La PC1 lo descarta y la PC0 lo acepta.

De esta manera mostramos cómo funcionan los mensajes de Neighbor Solicitation y Neighbor Advertisement.

2.1.2. Mensaje ICMPv6

En el primer evento, seleccionamos el mensaje ICMPv6 en la PC0, para analizar la PDU.

Observamos que es un mensaje ICMPv6 de TYPE 0x80, es decir 128 en decimal, lo que corresponde a un mensaje ECHO REQUEST, que cuenta con la siguiente estructura:

0	8	16
TYPE: 0x80	*CODE: 0x00*	*CHECKSUM: 0x0000*
IDENTIFIER: 2		*SEQUENCE NUMBER: 1*

También podemos observar que la sección Out Layers del OSI Model se resuelve en la layer 3.

Luego presionamos en Next Layer y nos aparece una salida con lo sucedido en la Layer 2.

Nos explica que el next hop es una dirección unicast, por lo que el proceso de Neighbor Discovery la busca en la neighbor table. Luego ve que el next hop no se encuentra en la tabla, por lo que el protocolo NDP envía una neighbor solicitation, comenzando el proceso visto en el apartado anterior.

2.1.3. Cómo recibe el Router los mensajes del protocolo NPD?

Seleccionamos el próximo evento, el mensaje NDP en la PC0 y observamos que la dirección de destino cambió por una dirección multicast de enlace local (FF02::) que utiliza el proceso de Neighbor Discovery.

En la layer 2 vemos que tenemos la dirección MAC de origen de la PC0 y la dirección MAC de destino que es 3333.FF00.000B, que es una dirección de multidifusión. Lo que tiene de particular esta dirección es que pertenece al rango de direcciones de multidifusión de la layer 2, asignadas a IPv6. Los ultimo 32 bits de la dirección MAC coinciden con los últimos 32 bits de la dirección IPv6 de multidifusión.

Esto permite que el descubrimientos de vecinos sea mucho mas eficiente en redes IPv6.

2.1.4. Próximo evento en el Switch 0

Seleccionamos el próximo evento que ocurre en el Switch 0, y observamos que no ocurren cambios en la entrada y salida en la capa 2. Esto ocurre ya que el switch no altera o cambia nada en las tramas, solo las reenvía por todos sus puertos, excepto por el de entrada.

2.1.5. Información sobre el primer evento en PC1

- Ethernet Destination Address: *3333.FF00.000B*
- Ethernet Source Address: *0090.0C5B.E7DC*
- IPv6 Source Address: *2001:DB8:ACAD:1::B*
- IPv6 Destination Address: *FF02::1:FF00:B*

2.1.6. Falta de Información en Out Layers

Al seleccionar el primer evento en el Router 0, en el que el router recibe el mensaje NDP forwardeado desde el Switch, observamos que en las Out Layers no hay información porque la dirección IP destino del mensaje NDP es la de la PC1, y no la del Router. El Router entiende que el mensaje no es para él y la descarta.

2.1.7. Proximo paquete ICMPv6

Seleccionamos el próximo evento ICMPv6 de la PC0 y observamos que efectivamente tiene toda la información para comunicarse con la PC1.

Efectivamente la PC0 tiene la dirección de IP destino y la dirección MAC de destino de la PC1, por lo que ahora la comunicación entre PCs debería ser exitosa.

2.1.8. Ultimo evento de la lista

En el último evento de la lista, que es un mensaje ICMPv6 de PC0, vemos que es un ECHO MESSAGE TYPE 129, es decir, *Echo Reply*.

2.1.9. Resetear la simulación

Reseteamos la simulación y volvemos a hacer un ping entre la PC0 y la PC1 mediante comandos, y observamos la ausencia del proceso Neighbor Discovery, ya que la PC0 ya conoce la MAC de la PC1 gracias al proceso realizado anteriormente.

Con esta información, la PC0 puede hacer pings a la PC1 cuantas veces quiera. Por esto sólo observamos los eventos ICMPv6 que van del PC0 al Switch, del Switch a la PC1 y las respuestas correspondientes.

2.2. Non Local Delivery

2.2.1. Configuracion el escenario

Para analizar el proceso en redes remotas, primero borraremos la informacion sobre neighbors en el Router 0 mediante el comando clear ipv6 neighbors y reseteamos la información.

2.2.2. Comienzo del escenario

Realizaremos un ping desde la PC0 a la PC2 que tiene la IP 2001:DB8:ACAD:2: :A/64, en el modo simulación para poder ver y analizar la lista de eventos.

2.2.3. Primer Evento en PC0

Al observar el primer evento en la PC0, que se trata de un mensaje ICMPv6, vemos que no hay información en la capa 2, ya que la PC0 todavía no sabe la MAC address de la PC2.

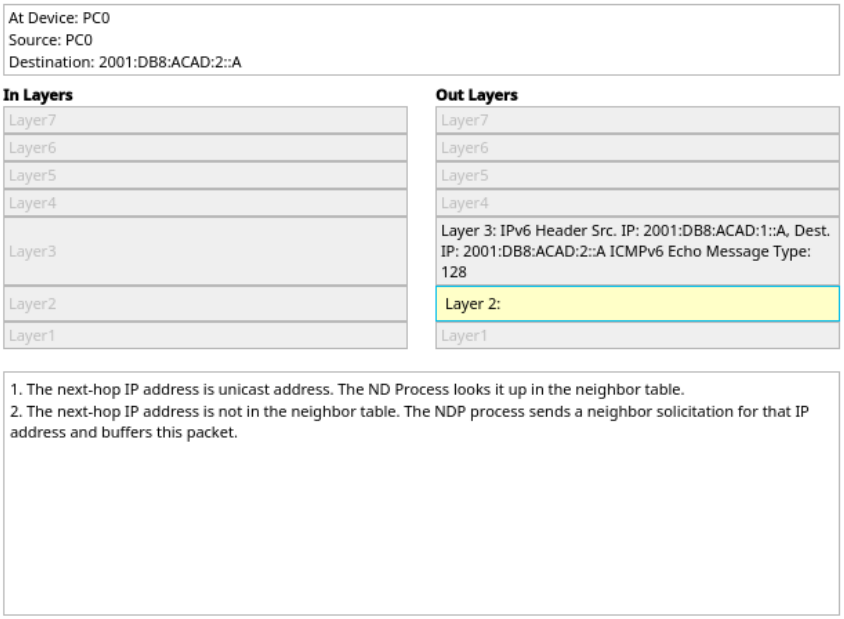


Figura 1: Primer ICMPv6 Pc0

2.2.4. Segundo Evento en la PC0

Al observar el primer mensaje NDP en la PC0, vemos que es un Neighbor Solicitation, ya que es de tipo 0x87(135 en decimal) al igual que anteriormente en el Local Delivery. La dirección IPv6 de origen es la Link Local Address de la PC0, la cual es FE80::290:2BFF:FE89:2D86.

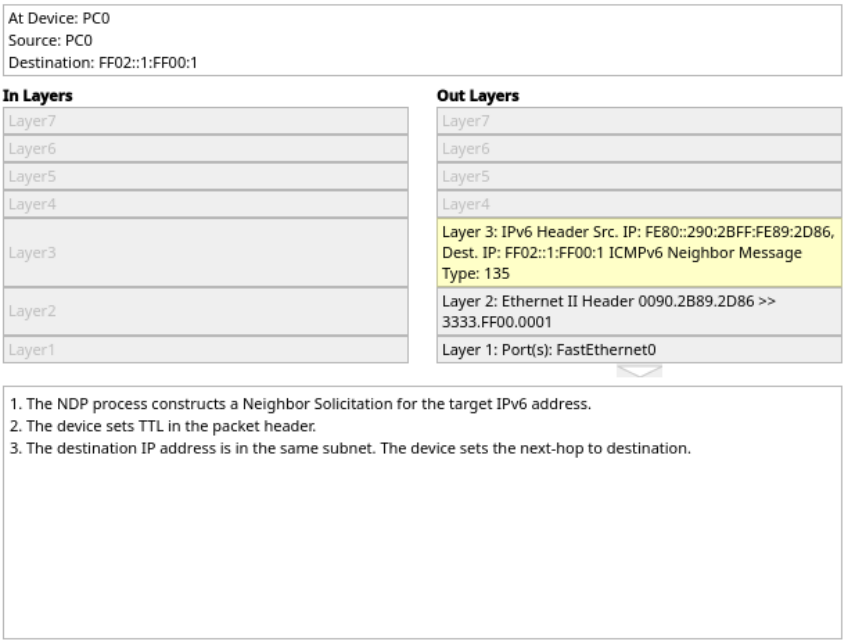


Figura 2: Primer NDP Pc0

2.2.5. Próximo Evento ICMPv6 en la PC0

Buscamos el siguiente mensaje ICMPv6 que sale de la PC0. Comprobamos que ahora si tiene información en la capa 2. La MAC de origen es la MAC address de la PC0 y se utiliza la MAC address de la interfaz g0/0 del router como MAC de destino. Esto se debe a que la única forma de acceder a la PC2, desde la PC0, es utilizando el Router.

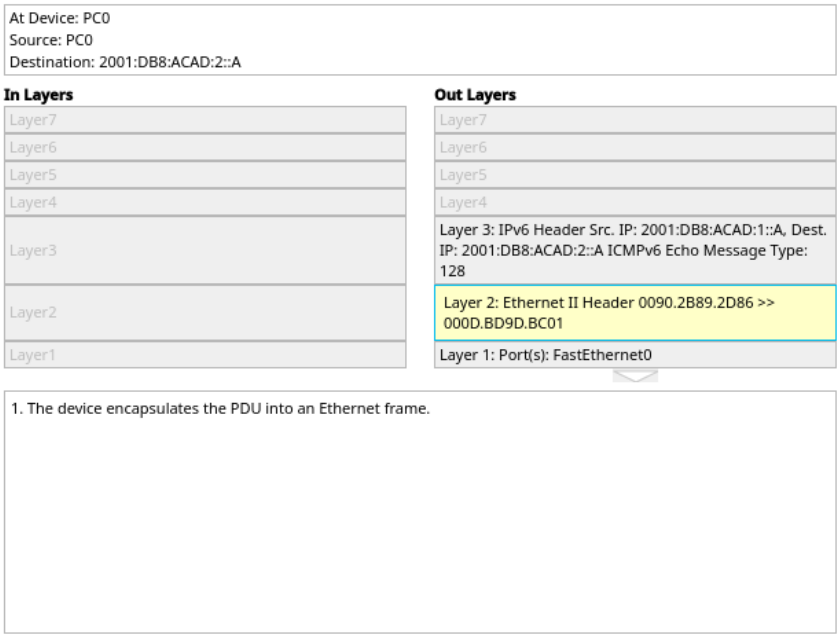


Figura 3: Siguiente ICMPv6 Pc0

2.2.6. Primer evento ICMPv6 en R0

Observamos el primer evento ICMPv6 en el Router 0 y comprobamos que la información de la capa 2 está vacía. Esto se debe a que el Router no conoce la MAC address de la PC2, ya que borramos la información de vecinos del Router, por lo que comenzará otro proceso NDP para descubrir la direccion desconocida.

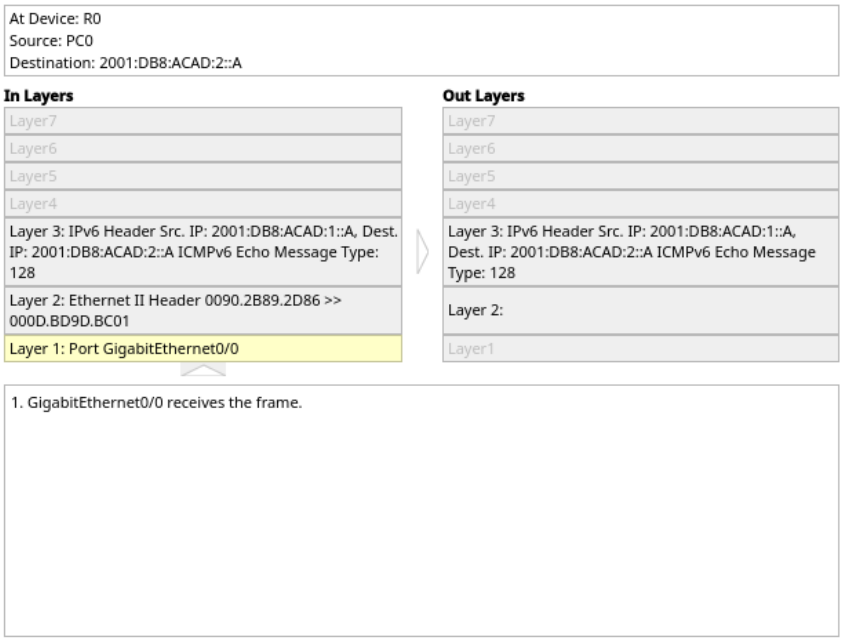


Figura 4: ICMPv6 R0

2.2.7. Evento ICMPv6 en la PC2

Observamos el próximo evento ICMPv6 en la PC2 y volvemos a ver que la capa 2 está vacía. Esto se debe a que la PC2 no conoce la MAC address para comunicarse con la PC0, por lo que comienza un proceso de NDP.

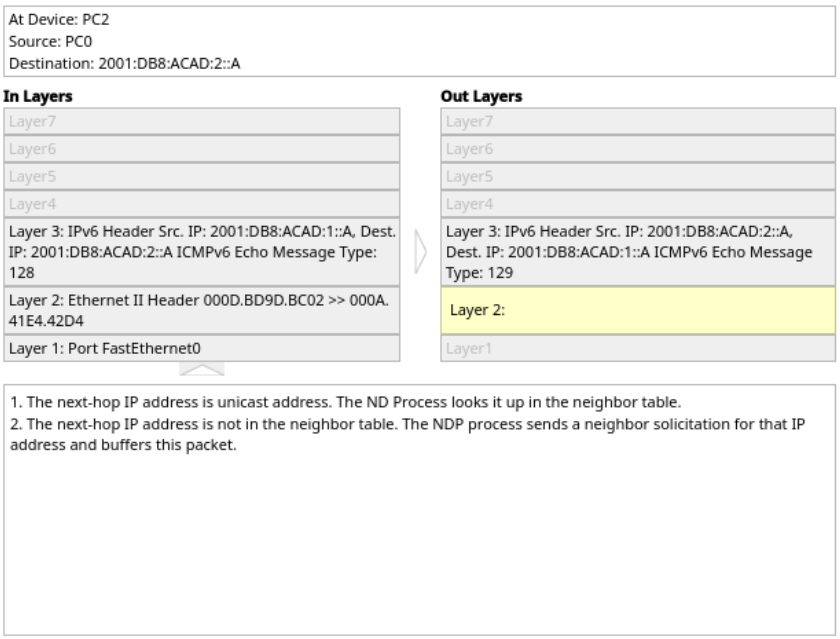


Figura 5: ICMPv6 Pc2

2.2.8. Ultimos eventos ICMPv6

Al ir al ultimo conjunto de eventos ICMPv6, luego de haber finalizado todos los procesos de NDP, la PC2 ya conoce la MAC address del Router y a su vez, el Router conoce la MAC address de la PC0, por lo que la PC2 puede enviar mensajes de respuesta a la PC0 sin necesidad de ningun mensaje NDP.

2.2.9. Reinicio de simulación

Esto lo podemos confirmar al reiniciar la simulación volver a hacer ping de la Pc0 a la Pc2 y notamos que no hubo ningún evento NDP.

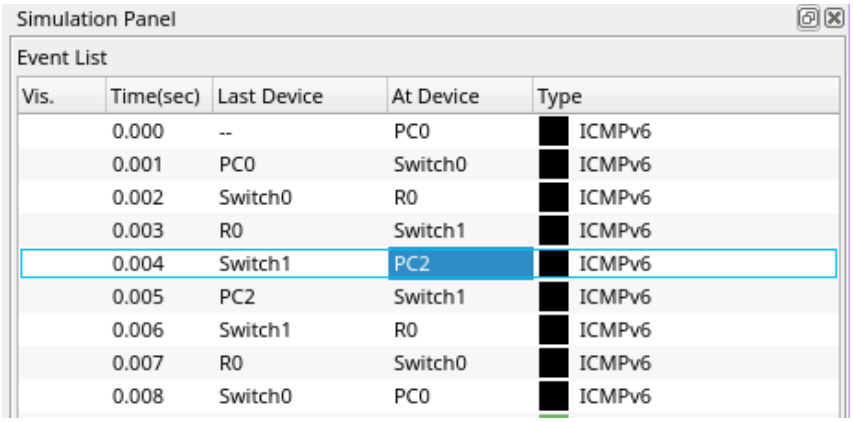


Figura 6: Ningun NDP

Al observar el mensaje seleccionado, vemos que en la capa 2 la direccion MAC de destino es la dirección MAC de la interface G0/1 del Router, ya que este es el encargado de relacionar la red de la PC2 con la PC0.

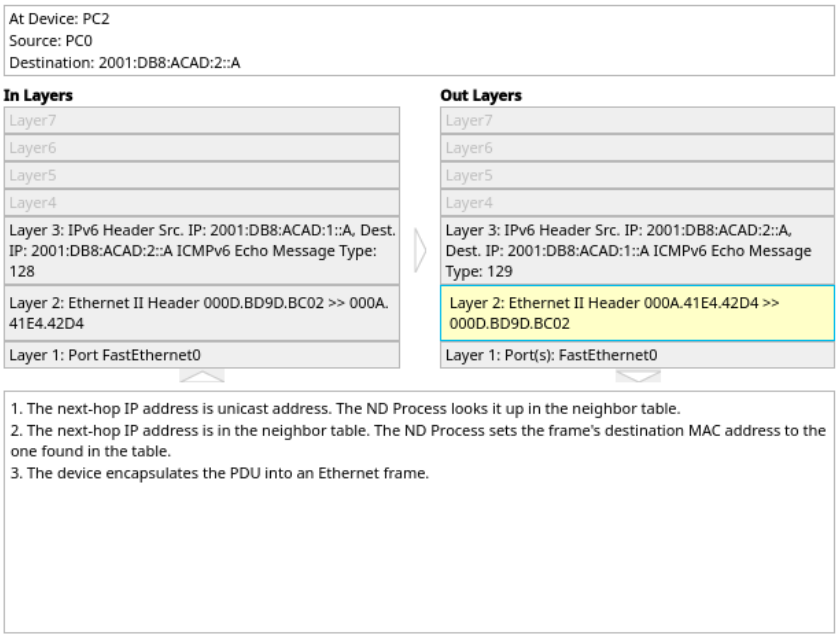


Figura 7: ICMPv6 Pc2

2.2.10. Modo Realtime

Ingresamos al modo realtime ejecutamos el comando show ipv6 neighbors y vemos la siguiente tabla:

0 8 16

IPv6 Address	*Age*	*Link-layer Addr*	*State*	*Interface*
2001:DB8:ACAD:1::A	*0*	*0090.2B89.2D86*	*REACH*	*Gig0/0*
2001:DB8:ACAD:2::A	*0*	*000A.41E4.42D4*	*REACH*	*Gig0/1*
FE80::20A:41FF:FEE4:42D4	*0*	*000A.41E4.42D4*	*REACH*	*Gig0/1*
FE80::290:2BFF:FE89:2D86	*0*	*0090.2B89.2D86*	*REACH*	*Gig0/0*

Aquí vemos 4 direcciones, 2 Global Unicast Address (GUA) y 2 Link - Local Address(LLA) que corresponden a las PC0 y PC2. No vemos ninguna entrada que corresponda a la PC1 ya que no la utilizamos hasta este punto.

2.2.11. Ping de R0 a la Pc1

Realizamos un ping a la PC1 desde el Router y volvemos a ejecutar el comando show ipv6 neighbors:

IPv6 Address	*Age*	*Link-layer Addr*	*State*	*Interface*
2001:DB8:ACAD:1::A	*28*	*0090.2B89.2D86*	*REACH*	*Gig0/0*
2001:DB8:ACAD:2::B	*0*	*000A.41E4.42D4*	*REACH*	*Gig0/1*
2001:DB8:ACAD:2::A	*28*	*000A.41E4.42D4*	*REACH*	*Gig0/1*
FE80::20A:41FF:FEE4:42D4	*28*	*000A.41E4.42D4*	*REACH*	*Gig0/1*
FE80::290:2BFF:FE89:2D86	*28*	*0090.2B89.2D86*	*REACH*	*Gig0/0*

Vemos una nueva dirección correspondiente a la GUA de la PC1, ya que luego del ping hubo interacción con el router y este aprendió su dirección. IPv6.

3. Conclusiones

Aquí se sintetizan los resultados obtenidos y se discuten las ventajas y desventajas de la autoconfiguración en IPv6, así como el impacto del proceso de Neighbor Discovery en el rendimiento de la red.

4. Referencias

Para la elaboracion de este informe utilizamos el contenido de los siguientes videos.

- **Video 1:** "IPv6 SLAAC and EUI-64 Basics in Packet Tracer", Dan Alberghetti, 2019, at `https://www.youtube.com/watch?v=yMK1NVHksDE`.
- **Video 2:** "IPv6 NDP and ICMPv6 using Packet Tracer", Dan Alberghetti, 2020, at `https://www.youtube.com/watch?v=y2GpG9aOIFI`
- **Video 3:** "Detección de vecinos IPv6 (Packet Tracer Lab 9.3.4)", RedesNetw channel, 2022, at `https://www.youtube.com/watch?v=ZBVXbgF39gw` +