TPL 7 - Protocolo IPv6

Fecha de Entrega Comisión 6 (Luján): 08/07/2021 - Comisión 35 (Chivilcoy): 08/07/2021

URL de Entrega: https://tinyurl.com/TyR-2021-TP7

Objetivo: Familiarizarse con la sintaxis y semántica del protocolo IPv6. Conocer las estrategias de configuración manual y autoconfiguración de direcciones y analizar intercambios de paquetes.

Consignas

Esta guía sobre IPv6 consta de dos partes. En la primera, se trabaja sobre un laboratorio Netkit (descargar, link alternativo) para reproducir las acciones propuestas (puntos 1 y 2). Es demostrativo para que puedan apreciar algunos cambios entre IPv4 e IPv6.
En la segunda actividad (Análisis de Capturas), se trabaja con tres capturas de tráfico (descargar). A partir de éstas, se propone identificar los mensajes y hosts enunciados a los efectos de comprender de mejor manera los procedimientos.

Trabajando en el hostA

Antes de levantar la interfaz `eth0` del host, verificar las direcciones IPv6 creadas automáticamente, las direcciones MAC y grupos multicast de los cuales el host es miembro.

a. Verificar las direcciones IPv6. Indicar tipo y alcance de la dirección.

```
# ip -6 addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436
    inet6 ::1/128 scope host «--
       valid_lft forever preferred_lft forever
```

b. Verificar cuáles son las direcciones MAC en el hostA.

```
# ip link  show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN mode DEFAULT
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT qlen 1000
    link/ether 02:03:04:05:06:0a brd ff:ff:ff:ff:ff:ff «--
```

c. Verificar a qué grupos multicast se encuentra asociado el hostA al momento de bootear. ¿En qué casos se utiliza dicha dirección?

```
# ip  maddr show
1:  lo
    inet  224.0.0.1
    inet6 ff02::1
2:  eth0
    link  33:33:00:00:00:01
    inet6 ff02::1 «--
```

d. Levantar la interfaz `eth0` . Identificar si hay una nueva dirección IPv6:

```
# ip link set dev eth0 up
# ip -6 addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qlen 1000
    inet6 fe80::3:4ff:fe05:60a/64 scope link «--
       valid_lft forever preferred_lft forever
```

e. Clasificar la nueva dirección según su tipo y alcance. ¿Cuál es el prefijo y el ID de interfaz de la nueva dirección?

Determinar qué método utilizó el host para crear automáticamente el ID de interfaz de la dirección de enlace local.

usa EUI-64 ya que:

MAC = `02:03:04:05:06:0a` , el método especifica que:

1. agregar `fffe` en la mitad de la MAC → **02:03:04 ff:fe 05:06:0a**
2. invertir el séptimo bit de la MAC 02:03:04 ff:fe 05:06:0a → **00:03:04 ff:fe 05:06:0a**
3. agrupar, aplicar reglas de notación y agregar el prefijo link-local `fe80::/64`

   `0003:04ff:fe05:060a  3:4ff:fe05:60a`

IP = `fe80::3:4ff:fe05:60a/64`

f. Verificar nuevamente a que nuevos grupos está asociado el hostA. Identificar si hay algún grupo nuevo y para que se utiliza la nueva dirección.

```
# ip maddr show
1:  lo
    inet  224.0.0.1
    inet6 ff02::1
2:  eth0
    link  33:33:00:00:00:01
    link  01:00:5e:00:00:01
    link  33:33:ff:05:06:0a
    inet  224.0.0.1
    inet6 ff02::1:ff05:60a «--
    inet6 ff02::1
```

Trabajando en el router con radvd

a. Verificar las direcciones IPv6 en el router. ¿Cuál es la diferencia que encuentra con el hostA? Indicar el tipo y alcance (scope) de cada dirección.

```
# ip -6 addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436
```

```
    inet6 ::1/128 scope host «--
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qlen 1000
    inet6 2001:123:aaaa:bbbb::1/64 scope global «--
       valid_lft forever preferred_lft forever
    inet6 fe80::3:4ff:fe05:601/64 scope link «--
       valid_lft forever preferred_lft forever
```

b. Verificar a qué grupos pertenece el router. Explique las diferencias con el hostA

```
# ip maddr show
1:  lo
    inet  224.0.0.1
    inet6 ff02::1
2:  eth0
    link  33:33:00:00:00:01
    link  01:00:5e:00:00:01
    link  33:33:ff:05:06:01
    link  33:33:ff:00:00:01
    link  33:33:00:00:00:02
    link  33:33:ff:00:00:00
    inet  224.0.0.1
    inet6 ff02::1:ff00:0 users 2
    inet6 ff02::2 «--
    inet6 ff02::1:ff00:1
    inet6 ff02::1:ff05:601 «--
    inet6 ff02::1
```

c. Iniciar el demonio radvd: `/etc/init.d/radvd start`

d. Levantar nuevamente la interfaz `eth0` **del hostA. Verificar nuevamente las direcciones IPv6 en el host. ¿Cuál es el prefijo y el ID de interfaz de la nueva dirección en el hostA? Clasificar tipo y alcance de la dirección.**

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qlen 1000
    inet6 2001:123:aaaa:bbbb:3:4ff:fe05:60a/64 scope global dynamic «--
       valid_lft 86395sec preferred_lft 14395sec
    inet6 fe80::3:4ff:fe05:60a/64 scope link
       valid_lft forever preferred_lft forever
```

Análisis de capturas

1. La captura del archivo *link-up.pcap* corresponde al intercambio de mensajes ocurrido en el laboratorio de netkit al ejecutar el comando `ip link set eth0 up` en uno de los hosts. Analice el tráfico generado e indique:

   a. para el mensaje *Neighbor Solicitation*:

- Que host lo envía.
- Cuál es la IP origen y IP destino.
- Cuál es el objetivo del mensaje para este caso particular.
- Qué característica en el encabezado IP sugiere el objetivo
- Cuál es la diferencia entre la IP que aparece como destino en el encabezado IP y la que aparece como destino (target) en el Mensaje ICMP. Justifique

b. para el mensaje *Router Solicitation*:

- Cuál es la IP origen y destino
- Cuál considera que es el objetivo del mensaje.

2. La captura del archivo *global-up.pcap* corresponde al intercambio de mensajes ocurrido al ejecutar el comando `ip link set eth0 up` en uno de los hosts, pero en este caso en el router de la red el demonio radvd se encuentra iniciado:

a. Para los mensajes de RA (Router Advertisement) y RS (Router Solicitation) indique:

- Qué host envía cada mensaje.
- IP origen y IP destino en cada caso. Justifique.
- Objetivo del mensaje en cada caso
- ¿Cuál es el objetivo del último mensaje NS que aparece en la captura? ¿Por qué es necesario este último mensaje?

3. La captura del archivo *captura_ejemplo_ping6.pcap* corresponde al intercambio de mensajes generados luego de la ejecución del comando `ping6` en uno de los host del laboratorio. Analice el tráfico y responda:

a. Para los mensajes Echo Request y Echo Reply indique:

- ¿Cuál es la dirección IP origen y destino del Echo Request?
- ¿Qué diferencia encuentra entre los mensajes Neighbor Solicitation de esta captura y los que aparecen en las capturas anteriores? Justifique.
- ¿Qué hosts contestan el Echo Request?

4. Haga una tabla con las distintas direcciones IPv6 que aparecen en las capturas indicando Prefijo de la dirección, ID de interfaz, y a cual de los siguientes grupos pertenece: Solicited-node address, all-IPv6-devices, all-IPv6-routers, Unicast link-local, Unicast Global.

Bibliografía

- DEERING, S., HINDEN, R. 2017. *Internet Protocol, Version 6 (IPv6) Specification*, RFC 8200. https://tools.ietf.org/html/rfc8200
- HINDEN, R., DEERING, S. 2006. *IP Version 6 Addressing Architecture*, RFC 4291 https://tools.ietf.org/html/rfc4291
- STALLINGS, W. 2007. Capítulo 18. Sección 1. IPv6. en *Data and Computer Communications (8th ed)*. pp. 586-595. Prentice Hall.
- O'FLAHERTY, C. et al. 2009. *IPv6 para Todos: Guía de uso y aplicación para diversos entornos.* ISOC.Ar Asociación Civil de Argentinos en Internet. http://www.ipv6tf.org/pdf/ipv6paratodos.pdf
- NARTEN, T., et al. 2007. *Neighbor Discovery for IPv6*, RFC 4861 https://tools.ietf.org/html/rfc4861

- BIERINGER, P. 2017. *Linux IPv6 HOWTO*
  http://tldp.org/HOWTO/Linux+IPv6-HOWTO/