

Diseño y administración de redes

Práctica 2

Diseño y gestión de escenarios IPv6

Informe

Dorian Boleslaw Wozniak - 817570@unizar.es

Marcos Pérez Guillén - 820532@unizar.es

Índice

Índice	1
Cuestión 1	2
Cuestión 2	3
Cuestión 3	3
Cuestión 5	5
Cuestión 6	6
Cuestión 7	7
Cuestión 8	7
Cuestión 9	8

Cuestión 1

Una vez establecido el túnel, conectarse desde el router de salida de la red LAN correspondiente (A o B) a cualquier sitio con conectividad IPv6. Por ejemplo, accede a la siguiente página y apunta la dirección IPv6 (que usaremos más adelante) de la misma: <http://www.consulintel.es>

Capturar en la interfaz eth0 del router (no en la interfaz túnel creada) y verificar que, efectivamente, el tráfico desde el router hacia el exterior es IPv6 sobre IPv4. Muéstralo indicando las direcciones IPv6 e IPv4 que aparecen en los paquetes.

NOTA: Se sustituye esta cuestión por establecer un túnel entre PCA3 y PCB3

El túnel se ha configurado para facilitar la conexión entre las LAN A y B (IPv6) a través de la LAN C (IPv4). En particular, este túnel establece una comunicación IPv6 entre PCA3 y PCB3, encapsulada dentro de una trama IPv4.

Para configurar la entrada del túnel en PCA3, se deben ejecutar los siguientes comandos (ajustando las direcciones IP para PCB3 según sea necesario):

```
ip tunnel add sit1 mode sit remote 192.168.7.20 local 192.168.7.10 ttl 255
ip link set sit1 up
ip addr add 2001::7:10/64 dev sit1
ip route add ::/0 dev sit1
```

Los siguientes comandos establecen una interfaz de túnel SIT que empareja una IPv6 a una interfaz IPv4. De esta manera, al enviar un paquete IPv6 dirigido al exterior, se envía a través de esta interfaz, que la enviará a su destino a través de su dirección IPv4.

Una vez que el túnel esté configurado correctamente en ambas máquinas, se puede probar mediante un ping entre PCA3 y PCB3:

```
ping6 2001::7:20
```

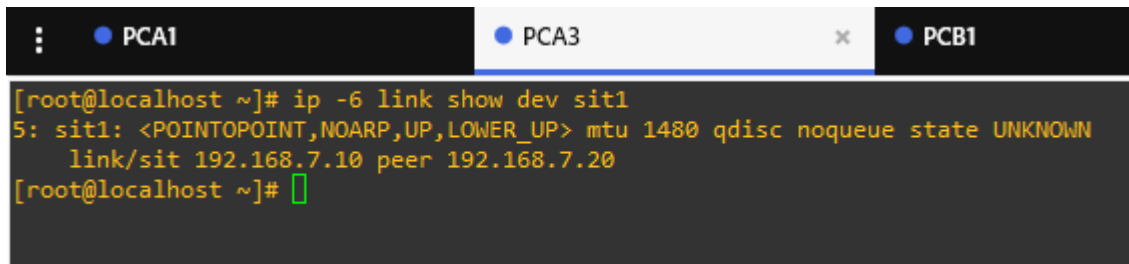
La funcionalidad exitosa del túnel se puede confirmar a través de la captura de Wireshark en las tramas 4 y 5, las cuales corresponden a una *request* y una *reply*, respectivamente. La solicitud de ECHO se envía de 192.168.7.10 (PCA3) a 192.168.7.20 (PCB3). Por debajo, está contenido un paquete IPv6 que indican un envío desde 2001::7:10 (PCA3) a 2001::7:20 (PCB3). El proceso de la respuesta es el inverso.

Un aspecto esencial que se evidencia claramente es el funcionamiento del túnel como un encapsulador de paquetes. En este contexto, el paquete IPv6 que se origina en PCA3 se encapsula dentro de un paquete IPv4 para poder viajar a través de la LAN C. Al llegar al destino (en este caso, PCB3), el paquete se desencapsula y se recupera el paquete IPv6 original.

Cuestión 2

Observa el valor MTU configurado en la interfaz tipo túnel (ip -6 link show dev [nombre_túnel] / ifconfig [nombre_túnel]). Justifica dicho valor teniendo en cuenta la información capturada previamente.

El MTU mínimo para paquetes IPv6 es de 1280 bytes. El tamaño mínimo indicado por el comando ip a sobre la interfaz sit1 es de 1480.



```
[root@localhost ~]# ip -6 link show dev sit1
5: sit1: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1480 qdisc noqueue state UNKNOWN
    link/sit 192.168.7.10 peer 192.168.7.20
[root@localhost ~]#
```

Figura 1: Información sobre la interfaz sit1 de PCA3

Este valor se puede obtener restando la longitud de la cabecera IPv4 (20 bytes) al MTU de la interfaz real (1500 bytes). En este espacio debe caber la totalidad del paquete IPv6 a encapsular, además de acomodar la posibilidad de que se pueda fragmentar el paquete IPv4 en el trayecto.

Cuestión 3

Una vez configurado el escenario completo, se comprobará la conectividad del mismo verificando la comunicación entre los equipos de las redes LAN A y LAN B mediante ping6 (consultar las páginas de ayuda necesarias – Anexo II, apartado 8).

Para el escenario completo, se ha utilizado *radvd* para asignar direcciones IPv6 de forma automática a los hosts 1 y 2 de cada red, editando el fichero `/etc/radvd.conf`:

```
interface eth0
{
    AdvSendAdvert on;
    MinRtrAdvInterval 30;
    MaxRtrAdvInterval 100;
    prefix 2000:A::0/64
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr off;
    };
};
```

En este caso, la interfaz eth0 (LAN A) de PCA3 asigna direcciones globales de la red 2000:A::/64 a sus hosts.

PCA3 además debe tener una dirección global para poder encaminar los paquetes que salen de la red:

```
ip -6 a add 2000:A::3/64 dev eth0
```

Y añadir la ruta que deben tomar los paquetes dirigidos a la red interna, al no aprender el encaminamiento automáticamente:

```
ip -6 route a 2000:b::/64 via 2001::7:10 dev sit1
```

Adicionalmente, hay que modificar en los hosts que no activen el *forwarding* (net.ipv6.conf.all.forwarding) de forma automática al arrancar, o no serán capaces de autoconfigurarse en /etc/sysctl.conf.

Para verificar la correcta configuración de la red, llevaremos a cabo una prueba de ping desde la máquina PCA1 hacia PCB1:

```
ping6 2000:b::e5d:90ff:fe73:0
```

Para evaluar el funcionamiento adecuado del ping, examinaremos las capturas de Wireshark.

La dirección IPv6 PCA1 es 2000:a::ec5:46ff:fefa:0, la de PCB1 es la del comando ping6.

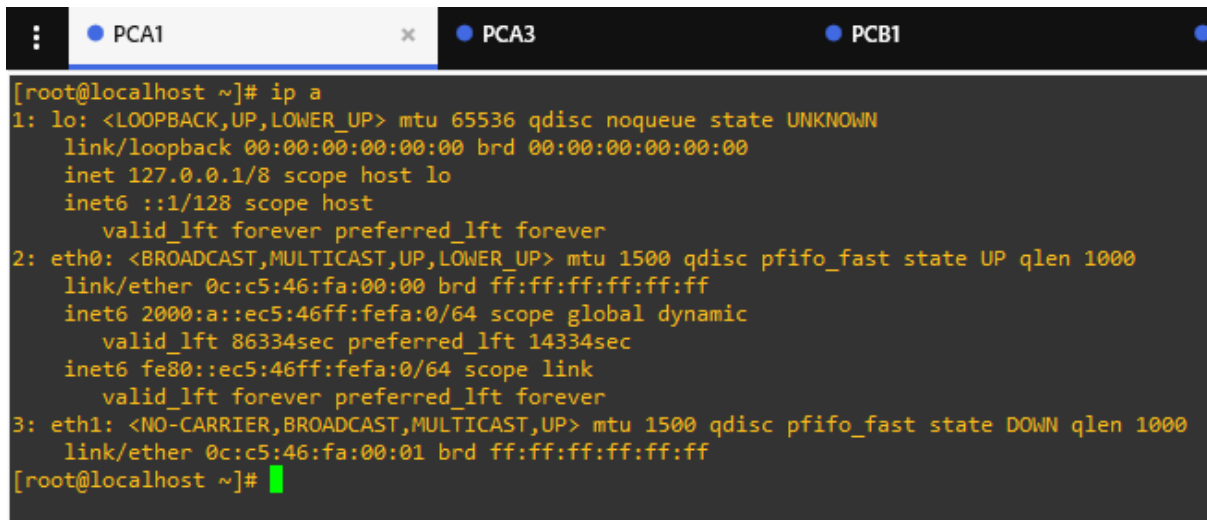
En la LAN A, se observa en las tramas 1 y 2 una pareja request/reply de PCA1 a PCB1 y viceversa.

Estos mismos paquetes se encuentran en las tramas 1 y 2 de LAN C, donde se encapsulan en un paquete IPv4 y envían a través del túnel al otro router, esta vez con las IPv4 de cada uno (192.168.7.10 para PCA3, 192.168.7.20 para PCB3).

Finalmente, se observa como llega el request y sale el reply en las tramas 1 y 2 de la red LAN B, utilizando solo IPv6.

Cuestión 5

Observa las direcciones IPv6 existentes en las interfaces de los PCs y pon un ejemplo de dirección local de enlace y dirección global. Muestra, en una de ellas, cómo se ha obtenido el identificador de interfaz de 64 bits (EUI-64).



```
[root@localhost ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 0c:c5:46:fa:00:00 brd ff:ff:ff:ff:ff:ff
    inet6 2000:a::ec5:46ff:fefa:0/64 scope global dynamic
        valid_lft 86334sec preferred_lft 14334sec
    inet6 fe80::ec5:46ff:fefa:0/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN qlen 1000
    link/ether 0c:c5:46:fa:00:01 brd ff:ff:ff:ff:ff:ff
[root@localhost ~]#
```

Figura 2: Dirección MAC e IPv6 de la interfaz eth0 de la máquina PCA1

A partir de la Figura 2, se puede determinar que la interfaz eth0 contiene las siguientes direcciones:

- Global: 2000:a::ec5:46ff:fefa:0/54
- Local de enlace: fe80::ec5:46ff:fefa:0

Se puede conocer el tipo de cada una a través del prefijo. Las locales de enlace siempre comienzan por fe80, mientras que las globales son del formato 2000::/3.

Además, la dirección MAC de la interfaz es 0c:c5:46:fa:00:00.

La mitad inferior de la dirección que identifica el equipo se obtiene usando EUI-64, la cual extiende la dirección MAC insertando FF:FE en la mitad de la dirección MAC de 48 bits, extendiéndose a 64 bits. Así, la dirección se crea de esta forma:

- Los primeros 16 bits se utilizan como los primeros 4 bytes de la dirección. El séptimo bit de la dirección, que indica si la MAC es universal o local, se invierte, por lo que el byte 0c se convierte en 0e.
- 46:fa es extendido a 45ff:fefa (se añade ff:fe).
- El resto es igual a lo que queda de la dirección.

Cuestión 6

A partir de la captura indica los dos casos de procedimiento DAD descritos especificando en ambos: dirección multicast (Solicited Node Address) a la que se dirige el mensaje de ND (Neighbor Discovery, ICMPv6) y dirección unicast por la que se pregunta (target).

Verifica la correspondencia entre las direcciones multicast y unicast identificadas. Muestra los paquetes de petición y respuesta (por parte del equipo y el router) de los parámetros necesarios para la autoconfiguración. Resalta dichos parámetros en el mensaje correspondiente.

Los procedimientos DAD se implementan para asegurar que una dirección IPv6 no esté duplicada en una red antes de que un dispositivo la configure de manera permanente.

Se pondrá el ejemplo de la autoconfiguración del equipo PCA1, cuyas IP y MAC se encuentran en la cuestión 5:

El procedimiento DAD para la dirección local de enlace se produce en la trama 4:

Al asignarse PCA1 a sí mismo una IP de enlace local, también ha comenzado a escuchar una dirección multicast (ff02::1:ffxx:xxxx, donde las x representan los últimos bits de la dirección IP solicitada). En nuestro caso, la ff02::1:fffa:0. Se utilizan los últimos 24 bits que corresponden al identificador único de la tarjeta de red.

A continuación, el equipo PCA1 (se sabe por su MAC origen en la trama Ethernet) realiza un multicast Solicited Address Node (la dirección anterior) desde una dirección no especificada (::). En el campo Target Address, pregunta por su dirección de enlace local, en nuestro caso fe80::ec5:46ff:fefa:0. Al no contestar nadie al envío multicast, entiende que la dirección es única. En caso de haber otro equipo con la misma dirección, respondería a través de este canal informando que la dirección ya está asignada.

A continuación, se realiza un procedimiento DAD para comprobar que se ha obtenido una dirección global única:

En la trama 5 el equipo PCA1 solicita al router (Router Solicitation) una IP global nueva desde su IP de enlace local fe80 (la vista en la cuestión 5). Lo realiza mediante un multicast a ff02::2. Esto indica que el envío se realiza a todos los routers conocidos.

En la trama 6, el router (mediante Router Advertisement) difunde a todos los dispositivos en la red (multicast ff02::1) que su prefijo de red es 2000:a::/64.

En la trama 7, PCA1 (se puede saber por la MAC de la trama Ethernet) envía un multicast de tipo Solicited Node Address de forma similar a la trama 4, preguntando si alguien de dicho multicast tiene asignado 2000:a::ec5:46ff:fefa:0. Si nadie responde, el equipo se ha autoconfigurado exitosamente.

Cuestión 7

Realiza las siguientes conexiones, identificando la correspondencia entre dirección MAC destino (dirección de nivel de enlace – link layer – lladdr) y dirección IPv6 destino del paquete capturado en el equipo origen del ping:

- PCA1 a PCA2
 - MAC destino: 0c:be:2c:d3:00:00
 - IPv6 destino: 2000:a::ebe:2cff:fed3:0
- PCA1 a PCB1
 - MAC destino: 0c:5d:90:73:00:00
 - IPv6 destino: 2000:b::e5d:90ff:fe73:0

Como se puede observar, se obtienen las direcciones con el método descrito en la cuestión 3.

Cuestión 8

Comprueba las conexiones (mediante varios ping, paso a paso) entre PCA1/PCB1 y PCB1/PCA1, es decir comprobando que funciona el ping a cada una de las direcciones intermedias del camino entre los extremos. Justifica los tiempos que tarda cada uno de los ping en función de la posición del destino.

- PCA1 -> PCA3

Se puede observar en las tramas 5 y 6 de LAN A. PCA3 tiene asignado 2000:a::3 como dirección.

- PCA1 -> PCB3

Se observa en las tramas 13 y 14 de la LAN A, y las tramas 16 y 17 de la LAN C. Se hace un ping a la dirección 2001::7:20, es decir, el extremo del túnel a través de IPv4 de PCB3.

- PCA1 -> PCC1

Se comprueba con las tramas 19 y 20 de la LAN A, 26 y 27 de la LAN C, y 3 y 4 de la LAN B. Ahora el envío llega a la LAN B a través del túnel anterior, y viceversa.

Cuestión 9

Modificar el MTU del interfaz eth1 de PCB3 a un valor de 1300 y el del interfaz eth0 de PCA3 a un valor de 1350. Observa qué sucede si se realiza un ping6 desde PCA1 hacia PCB1 con un tamaño de 1400 bytes. ¿Quién realiza la fragmentación? ¿Qué tramas se intercambian entre los equipos? ¿Qué diferencia habría si la red fuera totalmente IPv4?

NOTA: Las interfaces en nuestro caso están invertidas para que se correspondan con las interfaces de salida de cada router hacia LAN B.

La fragmentación en IPv6 no se realiza a lo largo del camino, sino que debe ser el emisor original quien fragmente con antelación los paquetes.

Se puede observar el proceso en las capturas:

Las tramas 2 y 3 corresponden al primer intento de envío. En este caso, PCA3 contesta que el paquete es demasiado grande, al superar el MTU de 1350.

En las tramas 4 y 5 de LAN A, se envía el paquete fragmentado en dos fragmentos de 1342 y 190 bytes respectivamente. En las tramas 4 y 6 de LAN C llegan los paquetes. PCB3 se da cuenta que la trama 4 es demasiado grande para su MTU de 1300 y envía en la trama 5 a PCA1 que el paquete es demasiado grande, que llega en la trama 6 de LAN A. El paquete 6 llega a la LAN B en la trama 2, pero al faltar el resto se ignora. Cabe destacar que el tamaño de los paquetes en la LAN C es más grande al incluir la cabecera IPv4.

Finalmente, se envían dos paquetes de 1310 (cabecera ethernet incluida) y 222 bytes en las tramas 8 y 9 de LAN A. Estos paquetes llegan a la LAN C en las tramas 7 y 8, que tras desencapsular si caben en el MTU de la interfaz, llegando a la LAN B en las tramas 3 y 4, finalmente respondiendo al ping.