Taller sobre IPv6

Universidad Rey Juan Carlos

8 de junio de 2011

Resumen

Estos ejercicios están orientados a entender el funcionamiento de IPv6.

1. Funcionamiento básico de IPv6

Para la realización de los siguientes ejercicios es necesario descomprimir el fichero `IPv6-lab.tgz`.

Al descomprimir este fichero se generará un directorio `IPv6-lab` con los archivos de configuración de esta práctica necesarios para NetGUI.

Al arrancar NetGUI, debes abrir el escenario definido dentro del directorio `IPv6-lab`. Este escenario es el que se muestra en la figura 1.

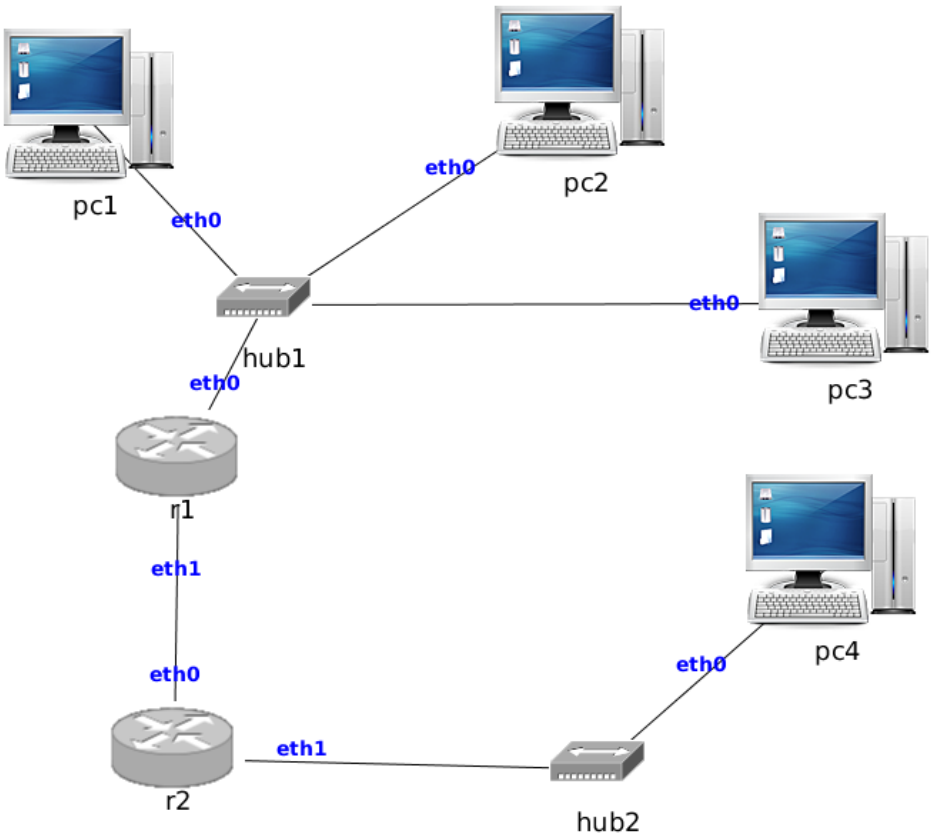

Figura 1: Escenario de IPv6

1.1. Autoconfiguración de direcciones IPv6 locales de enlace

Para empezar arranca únicamente `pc1`.

1. Indica cuál es la dirección IPv6 local de enlace que se ha configurado en `pc1`.
2. Indica a qué dirección IPv6 multicast de nodo solicitado pertenece `pc1`.

Arranca `tcpdump` en `pc1` para que capture paquetes de la siguiente forma:

```
tcpdump -i eth0 -s 0 -w /hosthome/iniciarPc2.cap
```

Arranca `pc2`.

3. Indica cuál es la dirección IPv6 local de enlace que se ha configurado en `pc2`.
4. Indica a qué dirección IPv6 multicast de nodo solicitado pertenece `pc2`.
5. Interrumpe la captura que estabas realizando en `pc1` con Ctl+C. Carga la captura en `wireshark` y localiza el mensaje enviado por `pc2` que indica que `pc2` está detectando si existen direcciones IPv6 duplicadas con su dirección local de enlace.
6. Fíjate en las direcciones IPv6 y en las direcciones Ethernet que lleva este mensaje. Indica si la máquina `pc1` procesa los mensajes dirigidos a esa dirección de destino.
7. Explica los mensajes ICMPv6 Router Solicitation observas en la captura y explica su contenido.

Arranca `tcpdump` en `pc1` para que capture paquetes de la siguiente forma:

```
tcpdump -i eth0 -s 0 -w /hosthome/iniciarPc3.cap
```

Arranca `pc3`.

8. Indica cuál es la dirección IPv6 local de enlace que se ha configurado en `pc3`.
9. Indica a qué dirección IPv6 multicast de nodo solicitado pertenece `pc3`.
10. Interrumpe la captura que estabas realizando en `pc1` con Ctl+C. Carga la captura en `wireshark` y localiza el mensaje enviado por `pc3` que indica que `pc3` está detectando si existen direcciones IPv6 duplicadas con su dirección local de enlace.
11. Fíjate en las direcciones IPv6 y en las direcciones Ethernet que lleva este mensaje. Indica si las máquinas `pc1` y `pc2` procesan los mensajes dirigidos a esa dirección de destino.
12. Observa si `pc1` o `pc2` responden al mensaje enviado por `pc3`. Explica qué está ocurriendo.
13. Ejecuta el siguiente comando en `pc1`, `pc2` y `pc3`.

    ```
    ip addr show eth0
    ```

    Explica qué ocurre con la dirección local de enlace de `pc3`.
14. Desactiva la interfaz `eth0` de `pc2` (`ip link set eth0 down`) y ejecuta `ping6` (con la opción `-I`) desde `pc1` a `pc3`. Explica qué ocurre.

    Cuando termines este apartado activa nuevamente la interfaz `eth0` de `pc2` (`ip link set eth0 up`).

Para resolver el problema que tiene pc3, cambia su dirección Ethernet utilizando ip y reinicia la interfaz:

```
ip link set eth0 down
ip link set eth0 address 00:14:22:aa:aa:33
ip link set eth0 up
```

15. Indica cuál es la nueva dirección IPv6 local de enlace que se ha configurado en pc3.

1.2. Tráfico IPv6 entre 2 máquinas directamente conectadas

1. Comprueba con el comando route las rutas IPv6 que tiene configuradas las máquinas pc1, pc2 y pc3 y explica el significado de las mismas:

   ```
   ip -6 route
   ```

2. Ejecuta tcpdump en pc3 (guardando los paquetes en un fichero) y realiza un ping6 (con la opción -I) desde pc1 a la dirección local de enlace de pc2. Explica el contenido de la captura.

3. Comprueba que tras la realización del ping6, las direcciones Ethernet de máquinas vecinas que han aprendido pc1 y pc2. Para ello, ejecuta tanto en pc1 como en pc2 el siguiente comando:

   ```
   ip neigh show
   ```

4. Comprueba que pc3 no ha aprendido ninguna dirección IPv6.

1.3. Autoconfiguración de direcciones IPv6 globales

Arranca la máquina pc4, pero todavía no arranques los *routers* r1 y r2.

Los *routers* r1 y r2 tienen configurado el protocolo *Router Advertisement de IPv6*. Estos *routers* mandan mensajes *ICMPv6 Router Advertisements* para enviar anuncios de los prefijos de subred a los que pertenecen sus interfaces. De esta forma, las máquinas que estén directamente conectadas a dichas interfaces podrán configurar su dirección IPv6 en función de los anuncios que reciban.

Arranca una captura en pc4 y guárdala en un fichero.

1. Indica qué direcciones y rutas ha configurado pc4.

Arranca r2.

2. Indica qué direcciones y rutas tiene ahora configuradas pc4.

3. Interrumpe la captura en pc4 y explica los mensajes que observas en dicha captura. Fíjate en las direcciones IPv6 origen y destino de cada paquete.

4. Muestra las direcciones Ethernet de vecinos aprendidas por r2 y pc4 y justifica tu respuesta.

5. Indica los valores *Valid Lifetime (valid_lft)* y *Preferred Lifetime (preferred_lft)* de la dirección IPv6 global que se ha configurado en pc4.

6. Interrumpe la ejecución del protocolo *Router Advertisement* en `r2`:

   ```
   /etc/init.d/radvd stop
   ```

   Indica qué ocurre con los valores *valid_lft* y *preferred_lft.* en `pc4`. Indica también qué ocurre con la dirección IPv6 global que se había configurado en `pc4`. Muestra las direcciones Ethernet aprendidas por `pc4` y justifica tu respuesta.

Inicia en `r2` el protocolo *Router Advertisement*:

```
/etc/init.d/radvd start
```

Arranca `r1`.

7. Indica qué direcciones IPv6 globales se han configurado en `pc1`, `pc2` y `pc3`.

8. Indica qué rutas IPv6 se han configurado en `pc1`, `pc2` y `pc3`. Ejecuta repetidas veces en uno de los pcs el comando que visualiza las rutas y fíjate en lo que ocurre con el campo *expires* y trata de explicarlo.

9. Explica qué ocurre si haces un `ping6` entre dos máquinas que no están directamente conectadas, por ejemplo, `pc1` y `pc4`.

1.4. IPv6 entre 2 máquinas de subredes diferentes

Los *routers* sólo tienen configurada ruta hacia máquinas vecinas. Para que dos máquinas de diferentes subredes puedan intercambiar tráfico es necesario añadir rutas en los *routers*

1. Añade las rutas que consideres necesarias para que todas las máquinas de la figura puedan intercambiar tráfico entre ellas.

2. Túnel IPv6 in IPv4

Descomprime el laboratorio `IPv6-tun-lab.tgz` y carga el escenario dentro de NetGUI. Arranca de una en una todas las máquinas del escenario.

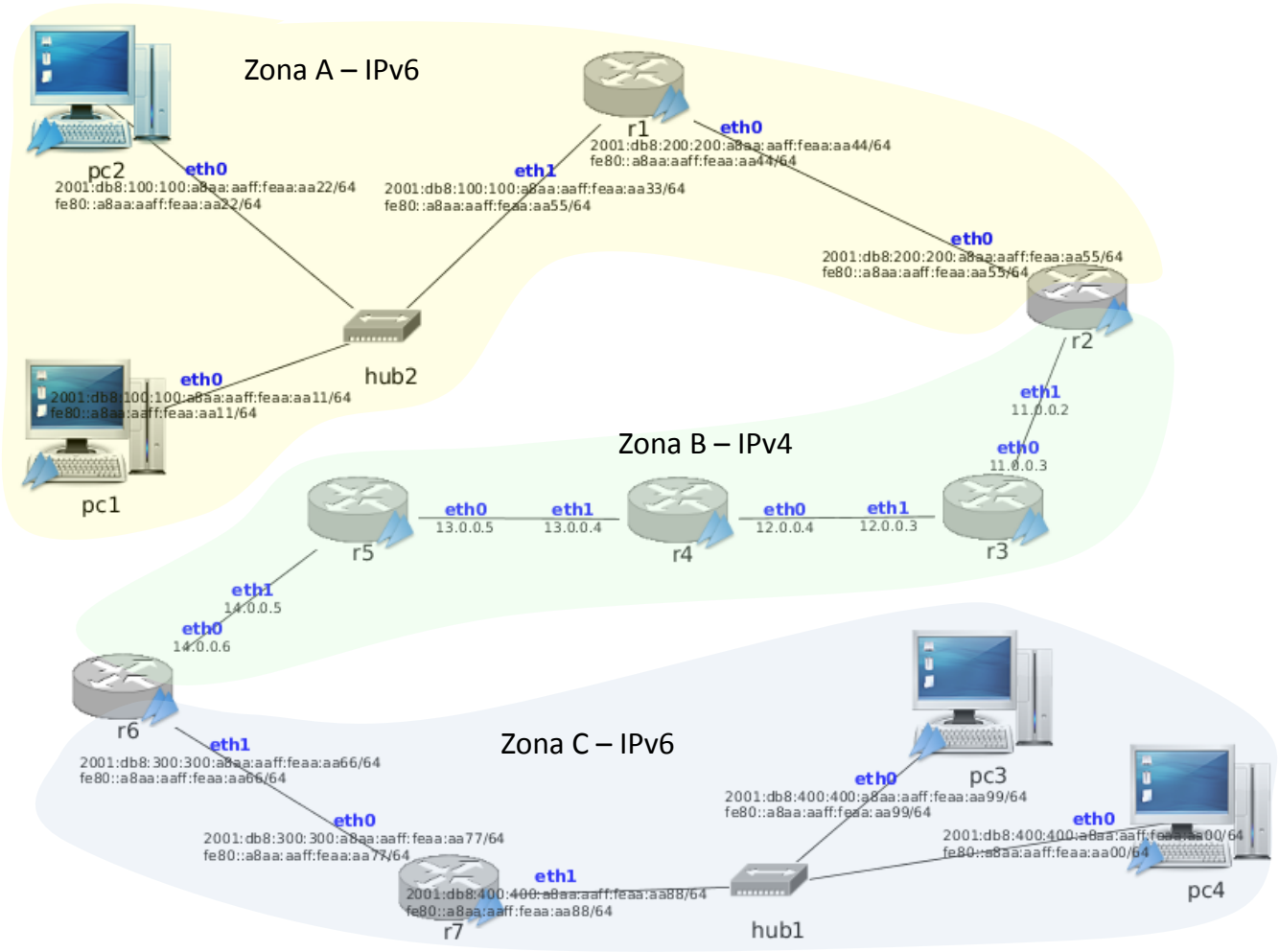

Figura 2: Zonas IPv6 a través de una zona IPv4

Observa en la figura 2 que hay 3 zonas diferenciadas en el escenario:

- Zona A - Zona IPv6: `pc1`, `pc2` y `r1`.
- Zona B - Zona IPv4: `r3`, `r4` y `r5`
- Zona C - Zona IPv6: `r7`, `pc3` y `pc4`.

Los *routers* `r2` y `r6` son *routers* que conectan las zonas diferentes. Estos *routers* se comunican a través de IPv4 en una de sus interfaces y por IPv6 en la otra. Son *routers* frontera que tienen la doble pila (IPv4 e IPv6) instalada.

Todos los *routers* y máquinas tienen configuradas sus direcciones IP y rutas válidas para comunicarse con los nodos de su misma zona.

Si haces `ping6` desde `pc1` a `pc3` observarás que no funciona. Ambas máquinas están utilizando IPv6, sin embargo, tienen que atravesar una zona que sólo está utilizando IPv4.

Para solucionar este problema vamos a configurar un túnel IP punto a punto, metiendo los paquetes IPv6 que se generen en ambas zonas IPv6 dentro de paquetes IPv4. De esta forma, las máquinas IPv6 de diferentes zonas podrán comunicarse.

1. Indica qué *routers* deberían ser los extremos del túnel IPv6 dentro de IPv4.
2. Configura en `r2` un extremo del túnel, con ttl 32, y añade la/s ruta/s necesaria/s en `r2` para que los paquetes IPv6 generados en la zona A puedan llegar a la Zona C.
3. Realiza un `ping6` desde `pc1` a `pc3`. Explica qué ocurre.
4. Configura en `r6` el otro extremo del túnel, con ttl 32 y añade la/s ruta/s necesaria/s en `r6` para que los paquetes IPv6 generados en la zona C puedan llegar a la Zona A.
5. Prueba a realizar un `ping6` desde cualquier máquina de una de las zonas IPv6 a otra máquina de la otra zona IPv6. Explica qué ocurre.
6. Arranca 3 `tcpdump`:
   - `tcpdump` en la interfaz `eth1` de `r4`.
   - `tcpdump` en la interfaz `eth1` de `r1`.
   - `tcpdump` en la interfaz `eth1` de `r7`.

   Realiza de un `ping6` desde `pc1` a `pc3`. Interrumpe las capturas y analízalas. Para los paquetes de cada una de las capturas, observa los siguientes campos y explica sus valores:

   a) Versión del protocolo IP que hay en la cabecera IP que va justo detrás de la cabecera Ethernet.
   b) direcciones IP origen y destino de esa cabecera
   c) `TTL` (IPv4) o `Hop limit` (IPv6)
   d) `Protocol` (IPv4) o `Next Header` (IPv6)
   e) Contenido del datagrama IPv4 o IPv6.