Fundamentos de Redes de Ordenadores
Práctica 3: Tablas de encaminamiento IP, ARP, ICMP

GSyC – URJC
Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación

Octubre de 2022

Resumen

En esta práctica se aprende a configurar las las tablas de encaminamiento de las máquinas utilizando dos métodos distintos: interactivamente mediante el uso del mandato `route` y estáticamente utilizando ficheros de configuración.

IMPORTANTE: En las figuras se muestra un escenario de red en que aparecen direcciones IP con una X entre medias (ej.: 200.X.0.40). Cada alumno tendrá en su escenario unas IPs con un valor concreto de X.

Introducción

Descarga tu escenario introduciendo tu DNI en el enlace:

`https://mobiquo.gsyc.urjc.es/practicas/fro/p3.html`

Obtendrás un fichero llamado `p3-lab.tgz`, que contiene un escenario de red. Si al pulsar sobre el enlace aparece una ventana de diálogo, elige "Guardar archivo". Guárdalo, por ejemplo, en la carpeta de Descargas. Desde el navegador de archivos pulsa con el botón derecho del ratón sobre el fichero y selecciona la opción "Extraer aquí". Esta acción creará una carpeta con el nombre `p3-lab`, en la cuál estarán los ficheros de configuración de tu escenario.

Entre los ficheros del escenario se incluye el *script* `reset-lab`, que devuelve el escenario a su estado inicial cuando se ejecuta. Esto puede resultar útil durante la realización de la práctica. Para ejecutar el *script* hay que abrir un terminal de la máquina real y estar dentro de la carpeta que contiene el escenario, desde allí escribir:

```
./reset-lab
```

Si se desea simplemente devolver algunas máquinas a su estado inicial, pero no todas, es decir, si por ejemplo se desea devolver al estado inicial solo pc1 y r1, se escribirá:

```
./reset-lab pc1 r1
```

Tras descomprimir el escenario éste se encuentra en su estado inicial, por lo que no es necesario ejecutar `reset-lab` al principio.

NOTA: Para realizar esta práctica tendrás que consultar la documentación adicional sobre los comandos para modificar la tabla de *routing*, y sobre los comandos `arp`, `ping` y `traceroute`.

1. Configuración de tablas de encaminamiento con `route`

Lanza ahora NetGUI. En el menú, elige File → Open y selecciona la carpeta `p3-lab` en la que está el escenario. Verás aparecer la red de la figura 1.

Arranca únicamente las siguientes máquinas: `pc1`, `pc4`, `r3` y `pc2`.

Este escenario aplica una configuración asignando direcciones IP a todas las interfaces de las máquinas, excepto a `pc1`. Esta configuración inicial está almacenada en el fichero `/etc/network/interfaces` de cada una de las máquinas, tal y como se ha visto en la práctica anterior.

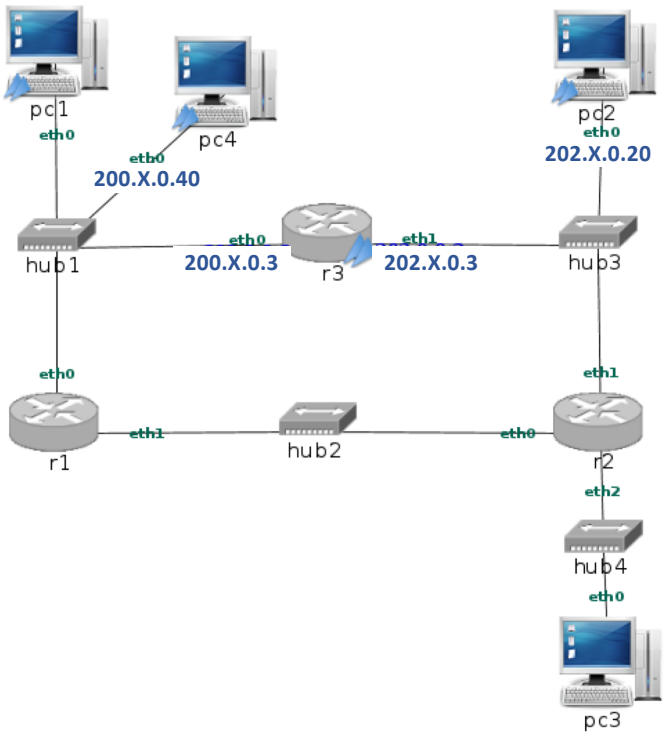

Figura 1: Sólo se arrancan: pc1, pc2, pc4 y r3

Teniendo en cuenta que sólo están estas máquinas arrancadas, responde a las siguientes cuestiones:

1. Escribe en `pc1` la orden `ping 127.0.0.1`. ¿Por qué se obtiene respuesta pese a no tener configurada `pc1` una dirección IP? Utilizando `route` comprueba el contenido actual de la tabla de encaminamiento (*routing*) de `pc1`.
2. Modifica el fichero `/etc/network/interfaces` de `pc1` para que tenga una dirección IP acorde a la de la subred a la que está conectado. (Nota: Deberás consultar previamente la máscara de la subred que tienen las otras máquinas conectadas a la misma subred que `pc1`). Reinicia la red en `pc1` para que se aplique la configuración que has escrito en el fichero `/etc/network/interfaces`.
3. Comprueba con `route` el contenido actual de su table de encaminamiento. Verás cómo, tras asignar la dirección IP a su interfaz de red, se ha añadido automáticamente una entrada en la tabla. Con esta tabla actual `pc1`, ¿a qué otras direcciones IP crees que `pc1` podrá enviar datagramas IP?
4. Dado que el resto de las máquinas encendidas tienen ya configurada una dirección IP, podrás suponer fácilmente cuál es el contenido de su tabla de encaminamiento. Mira la tabla de encaminamiento de `pc2` y `pc4`. ¿A que otras direcciones IP crees que esas máquinas podrán enviar datagramas IP?
5. Intenta deducir cuál crees que será la tabla de encaminamiento de `r3`,dado que tiene dos interfaces con IP asignada. Compruébalo consultando su tabla. Con esta tabla de encaminamiento, ¿crees que `r3` puede enviar datagramas IP a `pc1` y `pc4`? ¿Y a `pc2`.
6. Haz `ping` desde `pc1` a `pc4` y haz `ping` desde `pc1` a la dirección `r3(eth0)`. Ten en cuenta que no puedes utilizar los nombres `pc1`, `pc4`, etc. en el `ping`, sino que debes usar las direcciones IP correspondientes. ¿Funcionan estos `ping`? ¿Qué entradas de las tablas de encaminamiento se consultan en cada caso?
7. Haz un `ping` de `pc1` a `pc2` y haz un `ping` de `pc1` a la dirección `r3(eth1)`. ¿Funcionan estos `ping`? ¿Por qué?
8. Añade una ruta con el comando `route` en `pc1` para que los datagramas IP que no sean para su propia subred los envíe a través del *router* `r3`.

9. Haz ahora `ping` desde `pc1` a `r3(eth1)`. ¿Funciona este `ping`? ¿Qué entradas de las tablas de encaminamiento se consultan?
10. Haz un `ping` de `pc1` a `pc2`. ¿Por qué crees que no funciona este `ping`?
11. Añade las rutas necesarias utilizando el comado `route` para que funcione un `ping` de `pc1` a `pc2` y un `ping` de `pc4` a `pc2`. Ten en cuenta que podrás utilizar, rutas de máquina, rutas de subred o ruta por defecto.
12. ¿Crees que con la configuración que has realizado funcionará un `ping` de `pc2` a `pc1` y un `ping` `pc2` a `pc4`. Compruébalo.
13. Antes de continuar espera unos 10 minutos después de haber ejecutado el último `ping` del apartado anterior. Consulta el estado de las cachés de ARP en los pcs y en el *router* hasta que estén vacías.

    Arranca en `pc4` un `tcpdump` para capturar tráfico en su interfaz `eth0`, guardando la captura en el fichero `p3-a-01.cap`.

    Ejecuta en `pc1` un `ping` a `pc4` que envíe sólo 1 paquete (`ping -c 1 <máquinaDestino>`).

    Interrumpe la captura en `pc4` (`Ctrl+C`).

    Comprueba el estado de las cachés de ARP en `pc1`, `pc4`, `pc2` y `r3` y explica su contenido.
14. Analiza la captura con `wireshark`. Observa los siguientes campos en los mensajes:
    - Mensaje de solicitud de ARP que envía `pc1` a `pc4`.
      - Dirección Ethernet destino
      - Dirección Ethernet origen
      - Tipo en la cabecera Ethernet
      - Contenido del mensaje de solicitud de ARP: localiza el campo que contiene la dirección IP de la máquina sobre la que se está preguntando su dirección Ethernet.
    - Mensaje de respuesta de ARP que envía `pc4` a `pc1`.
      - Dirección Ethernet destino
      - Dirección Ethernet origen
      - Tipo en la cabecera Ethernet
      - Contenido del mensaje de respuesta de ARP: localiza el campo que contiene la dirección Ethernet solicitada.
    - Datagrama IP que envía `pc1` a `pc4`.
      - Dirección Ethernet destino
      - Dirección Ethernet origen
      - Tipo en la cabecera Ethernet
      - Dirección IP origen
      - Dirección IP destino
      - Campo TTL
    - Datagrama IP que envía `pc4` a `pc1`.
      - Dirección Ethernet destino
      - Dirección Ethernet origen
      - Tipo en la cabecera Ethernet
      - Dirección IP origen
      - Dirección IP destino
      - Campo TTL

    NOTA: Si tu captura ha durado más de 5 segundos, podrás ver que, 5 segundos después de la solictud de ARP de `pc1` preguntado por `pc4`, `pc4` hace una solicitud de ARP preguntando por `pc1`, pero esta solicitud de ARP no tiene dirección de destino broadcast, sino la dirección Ethernet de `pc1`. Esto demuestra que `pc4` ya tenía en su caché de ARP la dirección Ethernet de `pc1` (la aprendió de la solicitud recibida de `pc1`), y este ARP es simplemente de confirmación. No todas las implementaciones de TCP/IP realizan esta confirmación, y en esta asignatura nunca le prestaremos atención ni preguntaremos sobre ella.
15. Espera a que la caché de ARP de `pc1` esté vacía. Ahora vamos a analizar el tráfico desde `pc1` a `pc2`. ¿Cuántas capturas de tráfico crees que son necesarias para ver todos los paquetes que se generan en el escenario cuando se comunican `pc1` y `pc2`?

    Arranca un `tcpdump` en `r3(eth0)` guardando la captura en el fichero `p3-a-02.cap`.

    Arranca otro `tcpdump` en `pc2` guardando la captura en el fichero `p3-a-03.cap`.

    Ejecuta en `pc1` un `ping` a `pc2` que envíe sólo 1 paquete (`ping -c 1 <máquinaDestino>`).

    Interrumpe las capturas (`Ctrl+C`).

    Comprueba el estado de las cachés de ARP en `pc1`, `pc2`, `pc4` y `r3`. Explica su contenido.
16. Analiza las capturas realizadas con `wireshark`. Observa en los mensajes los mismo campos que analizaste el apartado anterior. Presta especial atención a los datagramas IP. Identifica los mensajes en las dos capturas que contienen el mismo datagrama IP. ¿Qué direcciones Ethernet tiene la trama que contiene esos datagramas en cada captura? ¿Qué valor tiene el campo TTL de la cabecera IP en cada uno?

2. Configuración de tablas de encaminamiento mediante ficheros de configuración

Arranca el resto de las máquinas y routers de la figura y obtendrás un diagrama similar a la figura 2. Ten en cuenta que en `pc1` ya tendrás configurada una dirección IP, mantén esta configuración.

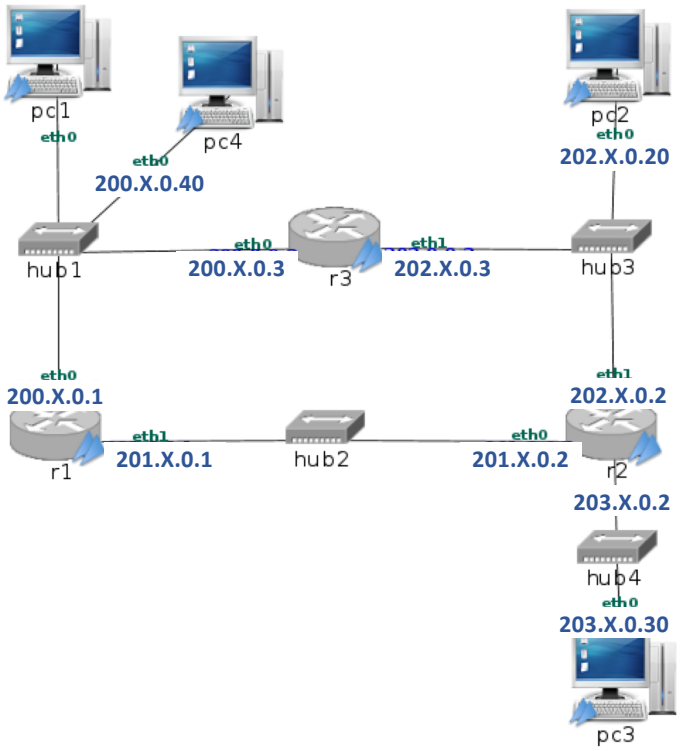

Figura 2: Todas las máquinas arrancadas

1. ¿Cuántas subredes observas en la figura? Escribe la dirección de cada una de estas subredes junto con su máscara.
2. Reinicia las máquinas `pc1`, `pc2` y `pc4`.

   Consulta las tablas de encaminamiento en todas las máquinas y *routers*, comprobarás que las rutas que configuraste en el apartado anterior han desaparecido. Los pcs y *routers* sólo tienen ruta hacia las subredes a las que están directamente conectados. Por tanto sólo podrán enviar paquetes a sus máquinas vecinas.
3. Añade rutas en las máquinas adecuadas modificando su fichero `/etc/network/interfaces` de forma que funcionen las siguientes rutas:

   a) Conectividad entre `pc1` y `pc2` en los dos sentidos, a través de las siguientes rutas:
   - pc1⇒r3⇒pc2
   - pc2⇒r3⇒pc1

   NOTA: Puedes emplear rutas de máquina, rutas de red o rutas por defecto.

   Ejecuta en `pc1` la orden `ping -c 3 <dirIPpc2>` para comprobar si hay conectividad entre las máquinas. Para verificar que el camino es el descrito previamente, deberás ejecutar `route` en `pc1` y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar `pc2`. Esta entrada debería indicar que el siguiente salto es `r3`. A continuación en `r3` deberás ejecutar `route` y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar `pc2`. Esta entrada debería indicar que `r3` no necesita ningún router adicional para alcanzar `pc2`.

   De forma análoga deberás consultar las tablas de encaminamiento en el sentido pc2⇒r3⇒pc1.

   b) Conectividad entre `pc2` y `pc3` en los dos sentidos, a través de la siguientes rutas:
   - pc2⇒r2⇒pc3
   - pc3⇒r2⇒pc2

   Ejecuta en `pc2` la orden `ping -c 3 <dirIPpc3>` para comprobar si hay conectividad entre las máquinas. Para verificar que el camino es el descrito previamente, deberás ejecutar `route` en `pc2` y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar `pc3`. Esta entrada debería

indicar que el siguiente salto es `r2`. A continuación en `r2` deberás ejecutar `route` y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar `pc3`. Esta entrada debería indicar que `r2` no necesita ningún router adicional para alcanzar `pc3`.

De forma análoga deberás consultar las tablas de encaminamiento en el sentido pc3⇒r2⇒pc2.

c) Conectividad entre `pc1` y `pc3` en los dos sentidos, a través de las siguientes rutas:
- pc1⇒r1⇒r2⇒pc3
- pc3⇒r2⇒r3⇒pc1

Ejecuta en `pc1` la orden `ping -c 3 <dirIPpc3>` para comprobar si hay conectividad entre las máquinas. Para verificar que el camino es el descrito previamente, deberás ejecutar `route` en `pc1` y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar `pc3`. Esta entrada debería indicar que el siguiente salto es `r1`. Después, deberás ejecutar `route` en `r1` y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar `pc3`. Esta entrada debería indicar que el siguiente salto es `r2`. A continuación en `r2` deberás ejecutar `route` y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar `pc3`. Esta entrada debería indicar que `r2` no necesita ningún router adicional para alcanzar `pc3`.

De forma análoga deberás consultar las tablas de encaminamiento en el sentido pc3⇒r2⇒r3⇒pc1.

4. Ejecuta en `pc1` un `traceroute` hacia `pc2` y en `pc2` uno hacia `pc1` para comprobar que las rutas son las especificadas.
5. Ejecuta en `pc2` un `traceroute` hacia `pc3` y en `pc3` uno hacia `pc2` para comprobar que las rutas son las especificadas.
6. Ejecuta en `pc1` un `traceroute` hacia `pc3` y en `pc3` uno hacia `pc1` para comprobar que las rutas son las especificadas. En este último `traceroute` observarás que aparecen unos `*`, en el final del tema 4 de teoría veremos a qué se deben. En la siguiente práctica se estudiarán más en detalle estas situaciones.
7. Antes de continuar asegúrate de que las rutas entre las máquinas son las especificadas en el apartado anterior.

   Lanza con `tcpdump` capturas en las siguientes máquinas, guardando los ficheros con el nombre que se indica:
   - captura en `r1(eth0)` con nombre de fichero `p3-b-01.cap`
   - captura en `r2(eth0)` con nombre de fichero `p3-b-02.cap`
   - captura en `r3(eth1)` con nombre de fichero `p3-b-03.cap`
   - captura en `pc3(eth0)` con nombre de fichero `p3-b-04.cap`

   Ejecuta en `pc1` un `ping` a `pc3` que envíe sólo 2 paquetes (`ping -c 2 <máquinaDestino>`).

   Interrumpe las 4 capturas (`Ctrl+C`).

   Analiza con `wireshark` las 4 capturas. Observa en ellas cómo los datagramas IP que se envían y reciben con la orden `ping` contienen un mensaje de ICMP. Comprueba en estos datagramas:
   - Dirección IP origen
   - Dirección IP destino
   - TTL en la cabecera IP
   - Campo Protocolo (tipo de protocolo) en la cabecera IP
   - Campos Tipo y Código en la cabecera ICMP.

   Consultando las capturas, responde a las siguientes cuestiones:

   a) ¿En qué se distinguen los mensajes "de ida" del `ping` de los mensajes "de vuelta"?

   b) ¿En qué capturas se pueden ver los mensajes "de ida" del `ping`? ¿Y los mensajes de vuelta? ¿Por qué?

   c) Comprueba los valores del campo TTL de la cabecera IP de todos los datagramas de todas las capturas y explica dichos valores.
8. Arranca de nuevo `tcpdump` en las mismas máquinas e interfaces que lo has hecho anteriormente pero guardando las capturas en otros ficheros diferentes:
   - captura en `r1(eth0)` con nombre de fichero `p3-b-05.cap`
   - captura en `r2(eth0)` con nombre de fichero `p3-b-06.cap`
   - captura en `r3(eth1)` con nombre de fichero `p3-b-07.cap`
   - captura en `pc3(eth0)` con nombre de fichero `p3-b-08.cap`

   Ejecuta en `pc1` la orden `traceroute` a `pc3`.

   Cuando la orden anterior haya terminado completament, interrumpe las capturas (`Ctrl+C`).

   A la vista del resultado que se muesta en `pc1`: ¿por qué *router* intermedios ha pasado un paquete para llegar de `pc1` a `pc3`?
9. Abre con `wireshark` los ficheros de captura que has obtenido. Identifica en los ficheros de capturas los siguientes paquetes:

- Los 3 mensajes enviados por `pc1` con TTL=1
- Los 3 ICMP de TTL excedido enviados por `r1`
- Los 3 mensajes enviados por `pc1` con TTL=2
- Los 3 ICMP de TTL excedido enviados por `r2`
- Los 3 mensajes enviados por `pc1` con TTL=3
- Los 3 ICMP de puerto inalcanzable enviados por `pc3`

10. Consultando las capturas, responde a las siguientes cuestiones:
    a) ¿Por qué ruta van viajando los mensajes enviados por `pc1` con TTL creciente?
    b) ¿Por qué ruta viajan los ICMP enviados por `r1`? ¿Qué dirección IP usa `r1` como IP de origen el enviar esos ICMP?
    c) ¿Por qué ruta viajan los ICMP enviados por `r2`? ¿Qué dirección IP usa `r2` como IP de origen el enviar esos ICMP?
    d) ¿Por qué ruta viajan los ICMP enviados por `pc3`?

3. Entrega de la práctica

Sube al enlace que encontrarás en Aula Virtual, y antes de que termine el plazo de entrega, los siguientes ficheros

- Memoria
- Un único fichero `p3.zip` que contenga una carpeta `p3` con los ficheros de captura:
  - `p3-a-01.cap`, `p3-a-02.cap`, `p3-a-03.cap`
  - `p3-b-01.cap`, `p3-b-02.cap`, `p3-b-03.cap`, `p3-b-04.cap`, `p3-b-05.cap`, `p3-b-06.cap`, `p3-b-07.cap`, `p3-b-08.cap`