Prácticas con NetGUI
Práctica 3: Análisis de los protocolos IP e ICMP

Arquitectura de Redes de Ordenadores
Arquitectura de Internet

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

Marzo de 2020

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: Toma nota de todo lo que hagas en un **cuaderno de laboratorio**, ya sea en papel o en electrónico. En él debería constar, para cada apartado de esta y de la siguientes prácticas, los pasos que has tenido que ir dando para obtener los resultados pedidos, los comandos que has empleado, las respuestas a las preguntas que se realizan en el enunciado, y cualquier otra información que consideres oportuna para dejar constancia de lo que vas aprendiendo en cada práctica. Este cuaderno de laboratorio te será muy útil para repasar lo aprendido.

1. Análisis de la cabecera IP

Carga en Wireshark el fichero de captura `cap1.cap`, disponible en la carpeta `P3-capturas` de la sección de la Práctica 3 en Aula Virtual.

Selecciona el primer paquete y despliega los campos de la cabecera IP, en la zona donde se muestran los detalles de los protocolos para el paquete que está seleccionado.

Responde a las siguientes preguntas:

1. ¿Cuál es la dirección IP origen y la dirección IP destino del paquete?
2. ¿Crees que las máquinas que se están comunicando son vecinas y se están comunicando directamente o crees que lo hacen a través de uno o más *routers*? Piensa en los argumentos y evidencias que pueden justificar tu respuesta.
3. Indica el valor del campo TTL para este paquete.
4. Indica cuál es la longitud total del campo de datos de este datagrama. Ahora selecciona el segundo paquete de la secuencia mostrada en el archivo de captura.
5. ¿Cuál es el valor del campo TTL en este caso?
6. Sabiendo que la captura de tráfico se ha realizado en la máquina destinataria del paquete, y que inicialmente el paquetelo envío la máquina origen con `TTL=128`, indica cuántos *routers* intermedios ha atravesado dicho paquete.
7. Indica cuál es la longitud total del campo de datos de este datagrama.
8. ¿Qué protocolo de nivel superior a IP debe recibir, en la máquina de destino el mensaje de datos encapsulado dentrodel datagrama?

2. Análisis de la fragmentación en IP

Carga en wireshark el fichero `cap2.cap`.

Responde a las siguientes preguntas:

1. ¿Crees que IP está aplicando fragmentación en alguno de los datagramas mostrados en la captura? Piensa en argumentos y evidencias que puedan justificar tu respuesta.
2. ¿Cuántos datagramas IP completos se pueden encontrar en esta captura? En caso de que se haya aplicado fragmentación sobre alguno de ellos, indica los siguientes datos para cada datagrama fragmentado:
   a) Identificador del datagrama.
   b) Número total de fragmentos en que ha sido dividido.
   c) Número de secuencia de captura en wireshark (panel superior, primera columna a la izquierda) del fragmento que ha permitido reconstruir por completo el datagrama.
   d) ¿Cuál es el primer fragmento? Indica su número de secuencia de captura en Wireshark. ¿Por qué sabemos que lo es?
   e) ¿Cuál es el último fragmento? Indica su número de secuencia de captura en Wireshark. ¿Por qué sabemos que lo es?
3. Estima cuál es el tamaño de la MTU de la capa por debajo de IP que está provocando que se realice fragmentación (si es que en verdad se produce fragmentación). Comprueba, para los fragmentos de datagramas que encuentres en la captura, el valor del campo offset de fragmentación. Verifica que los valores permiten reconstruir el datagrama original.

Introducción al análisis del escenario en NetGUI

Descarga de la página de la asignatura el fichero `p2-2020.tar.xz`, 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.

En una ventana de terminal, cámbiate con la orden `cd` al directorio dentro del cuál quieras guardar el escenario de red. Por ejemplo:

```
cd Practicas
```

Escribe en la ventana de terminal la siguiente orden para descomprimir el escenario de red:

```
tar -xvf ~/Practicas/p2-2020.tar.xz
```

El resultado de la ejecución de este comando creará una nueva carpeta que recibirá el nombre `p2-2020`, en la cual podrás encontrar los ficheros del escenario. La nueva carpeta `p2-2020` se creará dentro de la carpeta desde la que se ejecute la orden anterior (en el ejemplo anterior se creará dentro de la carpeta `Practicas`).

Entre los ficheros del escenario se incluye el *script* `reset-lab`, que devuelve el escenario a su estado inicial cuando se ejecuta. Para ejecutar el *script* hay que estar en la carpeta del escenario, y desde allí escribir en una ventana de terminal de la máquina real:

```
./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 encaminamiento, y sobre los comandos `ping` y `traceroute`. Dicha documentación la puedes encontrar en un enlace en Aula Virtual, junto a este enunciado.

3. Configuración de tablas de encaminamiento con `route`

Lanza ahora NetGUI. En el menú, elige File → Open y selecciona la carpeta `p2-2020` en la que está el escenario. Verás aparecer la red de la figura 3.

Arranca únicamente las siguientes máquinas: `pc2`, `pc5`, `r2` y `r3`.

Este escenario realiza una configuración asignando direcciones IP a todas las interfaces de las máquinas, excepto a `pc2`. 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.

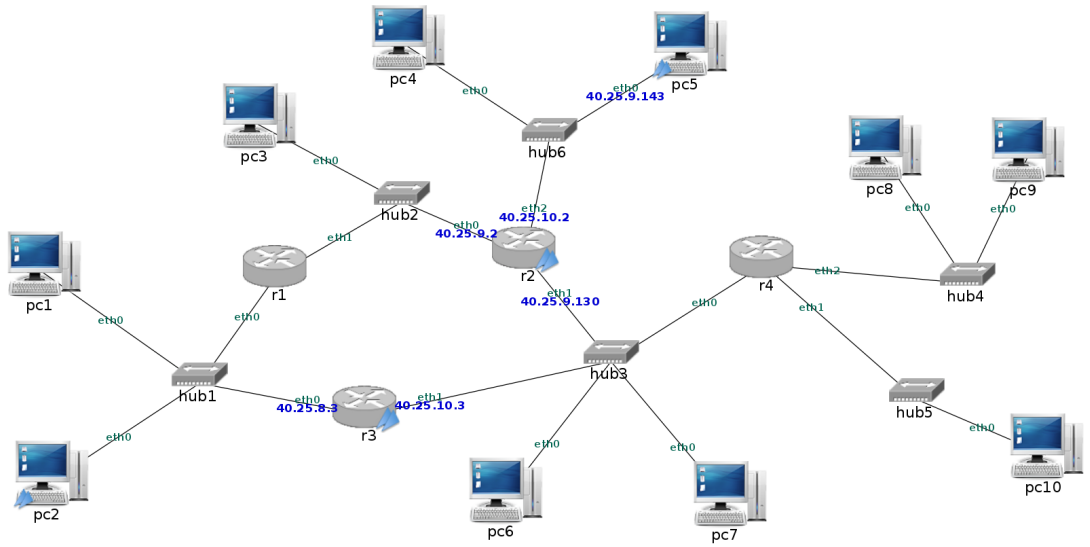

Figura 1: Sólo se arrancan: pc2, pc5, r2 y r3

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

1. Escribe en `pc2` la orden `ping 127.0.0.1`. ¿Obtienes mensajes de respuesta? ¿Quién está enviando esos mensajes de respuesta? Con la orden `route` puedes consultar la tabla de encaminamiento. Comprueba la tabla de encaminamiento de `pc2` para ayudarte a entender lo que está pasando.
2. Modifica el fichero `/etc/network/interfaces` de `pc2` para que `pc2` tenga una dirección IP acorde a 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 `pc2` y que estén arrancadas en este momento). Reinicia la red en `pc2` para que se aplique la configuración que has escrito en el fichero `/etc/network/interfaces`.
3. Comprueba con `route` cómo en `pc2`, tras asignar la dirección IP a su interfaz de red, se ha añadido automáticamente una nueva entrada en la tabla de encaminamiento. Con esta tabla de encaminamiento en `pc2`, ¿a qué otras direcciones IP crees que podrá `pc2` enviar datagramas IP?
4. Dado que el resto de las máquinas tienen ya configurada una dirección IP, deberías poder suponer cuál es el contenido de su tabla de encaminamiento:
   - ¿Cuál crees que será la tabla de encaminamiento de `pc5`?. Compruébalo consultando su tabla. Con esta tabla de encaminamiento, ¿a que otras direcciones IP crees que `pc5` podrá enviar datagramas IP?
   - ¿Cuál crees que será la tabla de encaminamiento de `r3`?. Compruébalo consultando su tabla. Con esta tabla de encaminamiento, ¿crees que `r3` puede enviar datagramas IP a `pc2` y `pc5`? ¿Y a `pc9`?.
   - ¿Cuál crees que será la tabla de encaminamiento de `r2`?. Compruébalo consultando su tabla. Con esta tabla de encaminamiento, ¿crees que `r2` puede enviar datagramas IP a `pc2` y `pc5`? ¿Y a `pc7`?.
5. Haz `ping` desde `pc2` a `pc5` y haz `ping` desde `pc5` a la dirección de `r3(eth0)`. Ten en cuenta que no puedes utilizar los nombres `pc2`, `pc5`, etc. en el comando `ping`, sino que **debes usar las direcciones IP correspondientes**. ¿Funcionan estos comandos `ping`? ¿Qué entradas de las tablas de encaminamiento se consultan en cada caso?
6. Haz un `ping` de `pc2` a la dirección de `r3(eth1)`. ¿Funcionan este `ping`? ¿Por qué?
7. Añade una ruta con el comando `route` en `pc2` para que los datagramas IP que no sean para su propia subred los envíe a través del *router* `r3` a otras direcciones (según corresponda a cada caso). Comprueba después que la nueva configuración ha funcionado en `r3`.

8. Haz ahora `ping` desde `pc2` a `r2(eth2)`. ¿Funciona este `ping`? ¿Qué entradas de las tablas de encaminamiento se consultan?
9. Haz un `ping` de `pc1` a `pc8`. ¿Por qué no funciona este `ping`?
10. En función del contenido actual de las tablas de encaminamiento de las máquinas y del *router*, explica qué máquinas de la red **no podrán comunicarse** con el resto, en la situación actual.
11. Añade las rutas que consideres necesarias utilizando el comado `route` para que funcione un `ping` de `pc2` a `pc5` y de `pc2` a `pc8`. Ten en cuenta que podrás utilizar, rutas de máquina, rutas de subred o ruta por defecto.
12. Indica si crees que con la configuración que has realizado funcionará un `ping` de `pc8` a `pc2` y de `pc9` a `pc2`. Compruébalo.

4. 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.

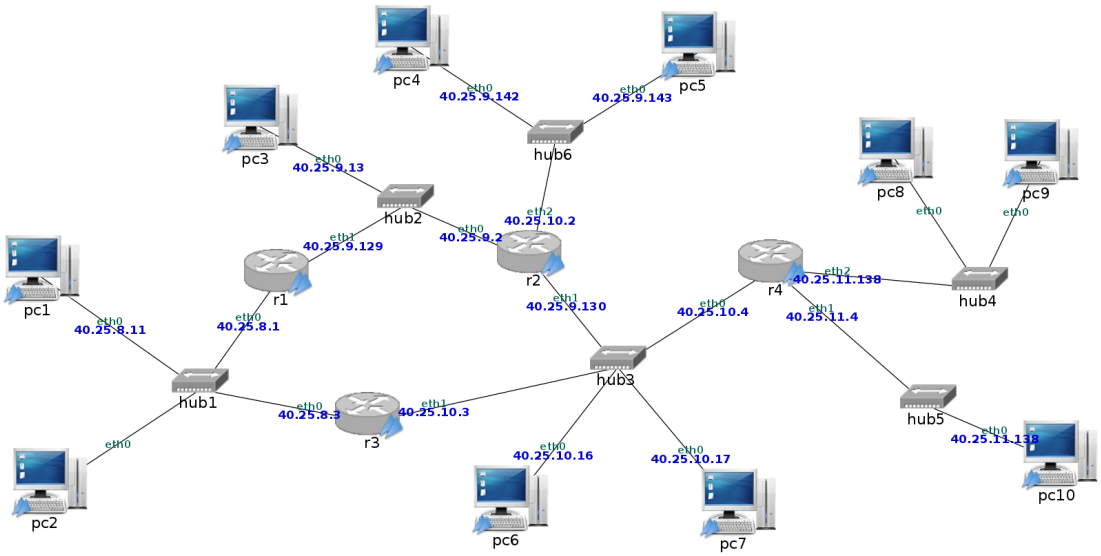

Figura 2: Todas las máquinas arrancadas

1. En base a la información que observas en las diferentes interfaces que muestra el esquema, indica la dirección de red y la máscara que se podría asignar para identificar a la red completa de la figura (es decir, que englobe a todas las subredes individuales que se muestran).
2. ¿Cuántas subredes distintas observas en la figura? Escribe la dirección IP que identifica a cada una de estas subredes junto con su máscara.
3. Reinicia las máquinas `pc2`, `r2` y `r3`.
4. 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 a las subredes a las que están directamente conectados. Por tanto sólo se podrán comunicar con sus máquinas vecinas en cada subred.
5. Con la configuración actual, indica qué máquinas se pueden comunicar entre sí, especificando sus direcciones IP (anota toda esta información en el cuaderno de bitácora para repasarla luego y comprenderla).
6. Modifica el fichero `/etc/network/interfaces` en los ordenadores y en los *routers* de la red de forma que funcionen las siguientes rutas. Podrás utilizar rutas de máquina, de subred o rutas por defecto:

   a) Conectividad entre `pc1` y `pc3` en los dos sentidos, a través de las siguientes rutas:
   - pc1⇒r1⇒pc3
   - pc3⇒r1⇒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`. A continuación en `r1` deberás ejecutar `route` y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar `pc3`. Esta entrada debería indicar que `r1` no necesita ningún router adicional para alcanzar `pc3`.

De forma análoga deberás consultar las tablas de encaminamiento en el sentido inverso: pc3⇒r1⇒pc1.

b) Conectividad entre `pc3` y `pc5` en los dos sentidos, a través de la siguientes rutas:
- pc3⇒r2⇒pc5
- pc5⇒r2⇒pc3

Ejecuta en `pc3` la orden `ping -c 3 <dirIPpc5>` para comprobar si hay conectividad entre las máquinas. Para verificar que el camino es el descrito previamente, deberás ejecutar `route` en `pc3` y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar `pc5`. 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 `pc5`. Esta entrada debería indicar que `r2` no necesita ningún router adicional para alcanzar `pc4`.

De forma análoga deberás consultar las tablas de encaminamiento en el sentido pc5⇒r2⇒pc3.

c) Conectividad entre `pc1` y `pc7` en los dos sentidos, a través de las siguientes rutas:
- pc1⇒r1⇒r2⇒pc7
- pc7⇒r2⇒r1⇒pc1

Ejecuta en `pc1` la orden `ping -c 3 <dirIPpc7>` 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 `pc7`. 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 `pc7`. 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 `pc7`. Esta entrada debería indicar que `r2` no necesita ningún router adicional para alcanzar `pc7`.

De forma análoga deberás consultar las tablas de encaminamiento en el sentido pc7⇒r2⇒r1⇒pc1.

7. Ejecuta en `pc1` un `traceroute` hacia `pc3` y en `pc3` un `traceroute` hacia `pc1`, para comprobar que las rutas son las especificadas.
8. Ejecuta en `pc3` un `traceroute` hacia `pc5` y en `pc5` uno hacia `pc3` para comprobar que las rutas son las especificadas.
9. Ejecuta en `pc1` un `traceroute` hacia `pc7` y en `pc7` uno hacia `pc1` para comprobar que las rutas son las especificadas. En este último `traceroute` observarás que aparecen unos `*`. ¿A qué crees que se debe? En la Práctica 3 se estudiarán más en detalle este tipo de casos.

4.1. Capturas de tráfico

Antes de comenzar a realizar los siguientes ejercicios asegúrate de que las rutas entre las máquinas son las especificadas en el apartado anterior, y que se pueden comunicar correctamente entre sí.

1. Lanza `tcpdump`, almacenando los paquetes capturados en ficheros diferentes, capturando tráfico en las siguientes interfaces: `r1(eth0)`, `r2(eth0)`, en `r3(eth1)` y `pc5(eth0)`.
2. Ejecuta en `pc1` un `ping` a `pc5` que envíe sólo 2 paquetes (`ping -c 2 <máquinaDestino>`).
3. Interrumpe las 4 capturas en todas las máquinas (ejecutando en cada ventana de terminal `Ctrl+C`).
4. En un terminal de la máquina real lanza la aplicación `wireshark` 4 veces, una para cada fichero de captura creado en el punto anterior, de forma que se puedan ver simultáneamente las distintas capturas. Observa en las capturas cómo los datagramas IP que se envían y reciben con la orden `ping` contienen un mensaje de ICMP. Comprueba en estos datagramas los siguientes datos de las cabeceras IP e ICMP:
   - Dirección IP origen.
   - Dirección IP destino.
   - TTL en la cabecera IP.
   - Tipo de Protocolo en la cabecera IP.
   - Tipo y Código en la cabecera ICMP.
5. 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.

6. Arranca de nuevo `tcpdump` en las mismas máquinas e interfaces que lo has hecho anteriormente pero guardando las capturas en otros ficheros diferentes: en `r1(eth0)`, en `r2(eth0)`, en `r3(eth1)` y en `pc5(eth0)`.
7. Ejecuta en `pc1` la orden `traceroute` a `pc3`.
8. Cuando la orden anterior haya terminado, interrumpe las capturas (`Ctrl+C`).
9. A la vista del resultado que se ha obtenido en `pc1`: ¿qué saltos intermedios ha atravesado un paquete para llegar de `pc1` a `pc5`?
10. Abre con `wireshark` los nuevos 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 como respuesta por `pc5`.
11. 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 `pc5`?