Práctica 2: Formato del datagrama IP y configuración de direcciones IP

Arquitectura de Internet

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

Marzo de 2022

Resumen

En esta práctica se aprende a configurar las interfaces de red de *hosts* y *routers* utilizando dos métodos distintos: interactivamente mediante el uso de los mandatos `ifconfig` o `ip`, y estáticamente utilizando ficheros de configuración. Además se estudiarán con detalle los campos de la cabecera IP.

IMPORTANTE: En el apartado 2 de la práctica se mencionan direcciones IP con una X entre medias (ej.: 151.X.0.1). Cada alumno debe utilizar como valor de X el que aparezca al introducir su DNI en el enlace:

`http://mobiquo.gsyc.es/practicas/ai/p2.html`

1. Campos de la cabecera IP

Carga en wireshark el fichero `cap1.cap`.

Selecciona el primer y único 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*?
3. Indica el valor del campo TTL.
4. Sabiendo que la captura de tráfico se ha realizado en la máquina destinataria del paquete y que inicialmente el paquete lo envío la máquina origen con TTL=64, indica cuántos *routers* intermedios ha atravesado dicho paquete.

2. Configuración de direcciones IP

2.1. El comando `ifconfig/ip`

- Arranca NetGUI. En las aulas de prácticas, la forma de arrancarlo es ejecutando en una ventana de terminal la orden `netgui.sh`.
- Crea una red como la de la figura 1 donde `pc1`, `pc2` y `pc3` son tres ordenadores y `r1` es un *router*.

  Coloca un *hub* para conectar `pc1`, `pc2` y `r1` y otro *hub* para conectar `pc3` y `r1`.

  Es importante que tengas en cuenta que cada vez que dibujas un cable desde un PC o un *router* hacia un *hub* se crea una interfaz Ethernet `ethX`, siendo X un número. Estas interfaces se numeran siguiendo el orden en el que se hayan dibujado sus cables, comenzando por `eth0`. Por eso, observa que para reproducir el mismo diagrama de la figura 1 deberás dibujar primero el cable desde `r1` al *hub1* para que esta interfaz se genere con el primer identificador `eth0`.

- Guarda la configuración de la red con Archivo → Guardar. Elige como nombre `p2-ifconfig`, **sin espacios**.
- Arranca los ordenadores y el encaminador de uno en uno. **Espera a que una máquina termine completamente de arrancar antes de arrancar la siguiente**. Los *hubs* en NetGUI son elementos pasivos que no hay que arrancar.

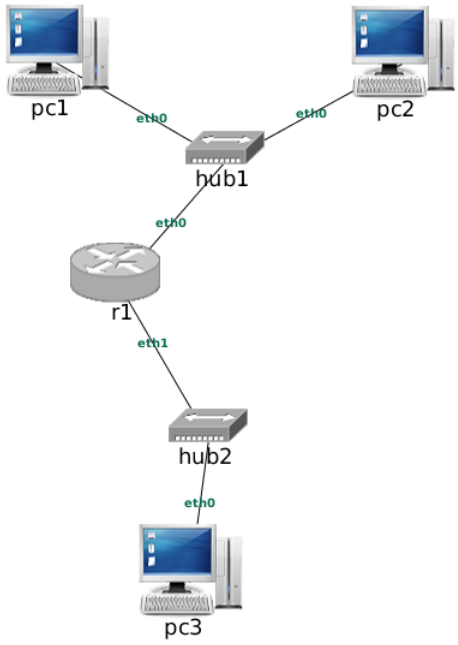


Figura 1: Red formada por tres PCs y un *router*.

1. Comprueba la configuración de la red en cada una de las máquinas y en el encaminador mediante el comando `ifconfig`. ¿Qué interfaces de red tienen configuradas cada una de ellas, y qué dirección IP tiene configurada cada interfaz?
2. Utilizando la orden `ifconfig` o la orden `ip`, asigna las direcciones IP a las interfaces de red de las máquinas y el router de la siguiente forma:
   - Como `netmask` usa en todos los casos `255.255.255.0`.
   - A todas las interfaces conectadas al `hub1` asígnales una dirección que empiece por `151.X.0...` [1]
   - A todas las interfaces conectadas al `hub2` asígnales una dirección que empiece por `152.X.0...`

   NOTA: Ten en cuenta que `r1`, al estar conectado a dos *hubs*, tendrá dos direcciones IP, una para cada interfaz (`eth0` y `eth1`).
3. Observa que las direcciones IP que has configurado se muestran en la interfaz de NetGUI. Comprueba en cada máquina virtual las direcciones de sus interfaces mediante `ifconfig` o `ip`. Incluye en la memoria de la práctica una imagen del escenario de NetGUI que muestre las direcciones IP que has configurado.
4. Inicia una captura de tráfico en `pc2`. Para ello ejecuta en `pc2`:

   ```
   pc2:~# tcpdump -i eth0 -s 0 -w /hosthome/p2-1.cap
   ```

   Ahora vas a generar tráfico de la siguiente forma: `pc1` va a enviar paquetes a `pc2` y `pc2` va a responder. Para ello ejecuta en `pc1`:

   ```
   pc1:~# ping -c 1 151.X.0.Y
   ```

   Donde:
   - La dirección IP que tienes que utilizar es la dirección IP destinataria de los paquetes, en este caso la de `pc2` (escribe en lugar de la X y la Y los valores de la dirección IP de la máquina `pc2` de tu escenario).
   - La opción `-c 1` hace que `ping` envíe un único paquete a la máquina `pc2` y que ésta le responda.

   Interrumpe la captura pulsando `Ctrl+C` en la ventana de `pc2`.

   Analiza los paquetes que aparecen en la captura. Para cada paquete indica:
   - Dirección Ethernet origen.
   - Dirección Ethernet destino.
   - Tipo de protocolo encapsulado (campo `Type`). Si el tipo de protocolo es IP, indica también:
     - Dirección IP origen
     - Dirección IP destino
5. Apaga el router `r1` y una vez apagado vuelve a arrancarlo. Comprueba que ha desparecido su configuración de direcciones IP.

[1] Recuerda que debes sustituir la X por el número que aparezca para ti en `http://mobiquo.gsyc.es/practicas/ro/p2.html`

2.2. El fichero /etc/network/interfaces

- Arranca NetGUI y construye una red como la de la figura 2. **Ten cuidado con el orden en que dibujas los cables de red de los *routers* a los *hubs***. Recuerda que para que las interfaces se ordenen en tu dibujo de la misma forma que en la figura, en los *routers* tienes que dibujar primero el cable que en la figura aparece etiquetado como `eth0`, después el que aparece etiquetado como `eth1`, y así sucesivamente.

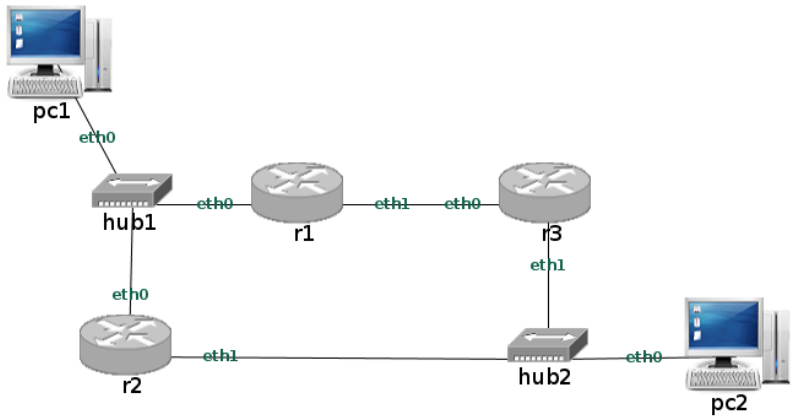


Figura 2: Red formada por 2 pcs y 3 *routers*

- Guarda la configuración de la red con Archivo → Guardar. Elige como nombre `p2-interfaces`, **sin espacios**.

1. ¿Cuántas redes distintas (grupos de interfaces que son vecinas o adyacentes entre sí) crees que hay en la figura?
2. Arranca las máquinas de una en una. Comprueba que sus interfaces de red no están configuradas ejecutando `ifconfig`.
3. Edita el fichero `/etc/network/interfaces` de cada máquina y añade direcciones IP de la siguiente forma:
   - Como `netmask` usa en todos los casos `255.255.255.0`.
   - A todas las interfaces conectadas a una de las redes asígnales una dirección que empiece por `201.X.0` ...
   - A todas las interfaces conectadas a otra de las redes asígnales una dirección que empiece por `202.X.0` ... dirección que empiece por `203.X.0` ...
4. Ejecuta en cada una de las máquinas la orden necesaria para que se configuren las interfaces de red según lo que has escrito en el fichero de configuración. Comprueba que las interfaces están configuradas, utilizando para ello `ifconfig`. Observa que las direcciones IP que has configurado se muestran también en la interfaz de NetGUI. Incluye en la memoria de la práctica una imagen del escenario de NetGUI que muestre las direcciones IP que has configurado.
5. Ejecuta en `r1` la orden necesaria para desactivar la configuración de la red. Comprueba con `ifconfig` cómo se ha perdido la configuración de las interfaces de red en `r1`.
6. Vuelve a ejecutar la orden necesaria para activar la configuración la red y que se configuren las interfaces de red en función de lo especificado en `/etc/network/interfaces`.
7. Modifica la dirección IP de `r3(eth1)` en el fichero `/etc/network/interfaces` de `r3` para asignarle otra dirección IP diferente a la que ya habías asignado, teniendo en cuenta que debería pertenecer a la misma subred que antes. No olvides ejecutar el comando para reactivar la configuración de la red cada vez que modifiques el fichero `/etc/network/interfaces`.
8. Los cambios que has hecho en el fichero `/etc/network/interfaces` permanecerán si rearrancas las máquinas. Compruébalo apagando `r1` y volviendo a arrancarlo. Ejecuta `ifconfig` una vez que haya rearrancado y comprueba cómo las dos interfaces de `r1` están configuradas.
9. Inicia una captura de tráfico en `r2`, interfaz `eth0`. Para ello ejecuta en `r2`:

   ```
   r2:~# tcpdump -i eth0 -s 0 -w /hosthome/p2-2.cap
   ```

   Ahora vas a generar tráfico de la siguiente forma: `pc1` va a enviar paquetes a `r1` y `r1` va a responder. Para ello ejecuta en `pc1`:

   ```
   pc1:~# ping -c 2 A.B.C.D
   ```

   Donde:

   - La dirección IP que tienes que utilizar es la dirección IP destinataria de los paquetes, en este caso la de la interfaz `eth0` de `r1` (escribe en A.B.C.D los valores de la dirección IP de `r1-eth0` de tu escenario).

- La opción `-c 2` hace que `ping` envíe 2 paquetes a la máquina `r1` y que ésta le responda a cada uno de ellos.

Interrumpe la captura pulsando `Ctrl+C` en la ventana de `r2`.

Analiza los paquetes que aparecen en la captura. Para cada paquete indica:

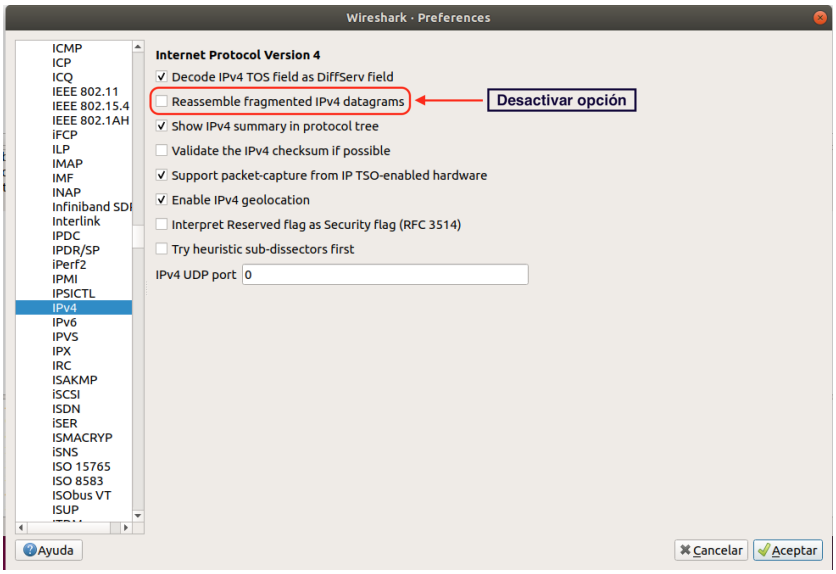
- Dirección Ethernet origen.
- Dirección Ethernet destino.
- Tipo de protocolo encapsulado (campo `Type`). Si el tipo de protocolo es IP, indica también:
  - Dirección IP origen
  - Dirección IP destino

10. Prueba ahora (sin capturar el tráfico) a realizar el ping desde `pc1` a la dirección IP de la interfaz `eth1` de `r1`. ¿Qué ocurre? ¿A qué crees que se puede deber?

3. Fragmentación IP

Carga en wireshark el fichero `cap2.cap`.

Abre el menú `Edit` → `Preferences`, despliega la sección `Protocols` y busca el protocolo `IPv4`. Desactiva la opción señalada en la figura:



La captura muestra 3 paquetes que son 3 fragmentos de un datagrama IP original. Responde a las siguientes preguntas:

1. ¿Cómo se puede saber que los 3 paquetes pertenecen al mismo datagrama original?
2. Indica cuántos datos IP (cantidad de bytes de datos del campo de datos del datagrama IP original) viajan en cada uno de los datagramas en los que se ha fragmentado el datagrama original. ¿El primer y segundo datagrama IP podrían llevar más datos IP? ¿Por qué?
3. Indica cuántos datos IP formarían el datagrama IP original sin fragmentar.
4. Dado que los datagramas IP podrían desordenarse en el camino, indica cómo podría el destino reordenar los fragmentos y reconstruir el datagrama original.
5. Explica cómo puede saberse que el primer paquete de la captura es el primer fragmento de un datagrama fragmentado, en vez de ser un datagrama normal sin fragmentar. Observa que wireshark no muestra en este primer paquete nada que haga pensar que es un fragmento (a diferencia de lo que ocurre en los otros).
6. Explica cómo puede saberse que el último paquete de la captura es el último fragmento de un datagrama fragmentado, en vez de ser un datagrama normal sin fragmentar.
7. Activa ahora la opción de wireshark que desactivaste antes. Observa cómo cambia la información mostrada para los paquetes:
   - Ahora wireshark identifica al primer paquete como fragmento, y también el segundo, pero no lo marca en el último
   - wireshark señala en el primer y segundo paquete que ha reensamblado los 3 fragmentos en el tercer paquete
   - En el tercer paquete se mantiene la cabecera tal y como es, pero se detalla (al final de la cabecera IP) los campos de los 3 fragmentos: `[3 IPv4 Fragments (4008 bytes): #1(1480), #2(1480), #3(1048)]`
   - En el tercer paquete se incluye en la parte de datos los datos agregados de los 3 fragmentos.

4. Entrega de la práctica

Guarda los ficheros de captura en una carpeta que se llame `p2` que contenga `p2-1.cap` y `p2-2.cap`. Comprime esa carpeta en formato .zip para generar el fichero `p2.zip`.

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

- Memoria en formato pdf
- `p2.zip`: resultado de comprimir la carpeta p2 que contiene los ficheros de captura de la práctica