Prácticas con NetGUI
Práctica 0: Ethernet

Arquitectura de Redes de Ordenadores
Arquitectura de Internet

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

Febrero de 2017

Resumen

En esta práctica se mostrará el encapsulamiento de las unidades de datos de protocolos de diferentes niveles dentro de la arquitectura TCP/IP. Se dedicará especial atención al funcionamiento de Ethernet. Además se aprenderá a realizar capturas de tráfico con la herramienta `tcpdump` dentro de nodos del entorno de virtualización de redes NetGUI/Netkit, y a analizar el tráfico capturado con la herramienta `wireshark`.

IMPORTANTE: Toma nota de todo lo que hagas en un **cuaderno de laboratorio**, ya sea en papel o en formato electrónico. En él debería constar lo que vas aprendiendo en cada apartado de la práctica, 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. Este cuaderno de laboratorio te será muy útil para repasar lo aprendido.

1. Análisis de ficheros de captura de tráfico

El fichero `cap1.cap` contiene tráfico capturado en la interfaz de alguna máquina. Antes de analizar los contenidos del fichero se desconocen los detalles de las máquinas conectadas a la red en la que se ha realizado la captura.

Abre el fichero de captura `cap1.cap` con `wireshark` y responde a las siguientes preguntas:

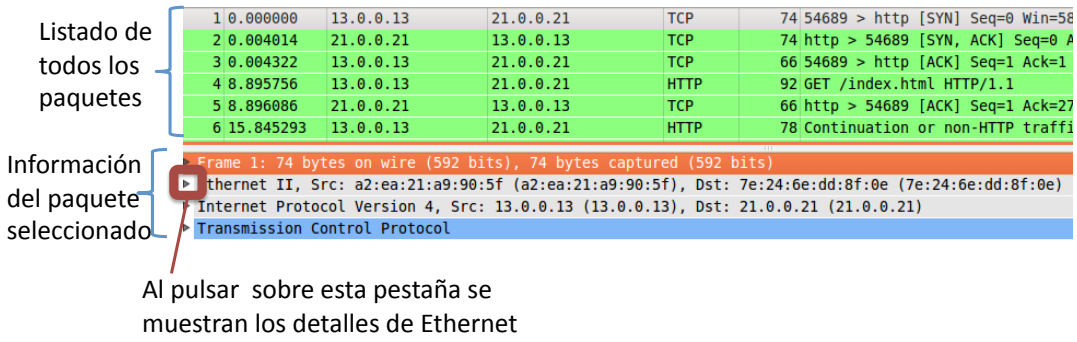
1. Selecciona el primer paquete que aparece en la captura, pulsando sobre la primera línea del Panel 1 (lista de paquetes). Éste quedará marcado en un color diferente:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	13.0.0.13	21.0.0.21	TCP	74	54689 > http [SYN] Seq=0 Win=5840 Len=0 MSS=146
2	0.004014	21.0.0.21	13.0.0.13	TCP	74	http > 54689 [SYN, ACK] Seq=0 Ack=1 Win=5792 Le
3	0.004322	13.0.0.13	21.0.0.21	TCP	66	54689 > http [ACK] Seq=1 Ack=1 Win=5840 Len=0 T
4	8.895756	13.0.0.13	21.0.0.21	HTTP	92	GET /index.html HTTP/1.1
5	8.896086	21.0.0.21	13.0.0.13	TCP	66	http > 54689 [ACK] Seq=1 Ack=27 Win=5792 Len=0
6	15.845293	13.0.0.13	21.0.0.21	HTTP	78	Continuation or non-HTTP traffic

2. En el Panel 1 (lista de paquetes), para cada paquete se muestra:
   - Su número de orden dentro de la captura (columna `No.`). El número 1 es el primer paquete capturado.
   - Tiempo en segundos que ha pasado desde que se capturó el primer paquete (columna `Time`). El primer paquete marca el origen de tiempos, por lo que el valor de tiempo es 0.000000 segundos. El segundo paquete muestra 0.004014 segundos lo que significa que el segundo paquete se capturó transcurridos 0.004014 segundos desde que se capturó el primer paquete. Y así sucesivamente.
   - Dirección de origen del paquete (columna `Source`). En este caso muestra la dirección origen de nivel de red (dirección IP).
   - Dirección destino del paquete (columna `Destination`). En este caso muestra la dirección destino de nivel de red (dirección IP).
   - Protocolo de más alto nivel reconocido dentro del paquete (columna `Protocol`).
   - Longitud total de la trama capturada en bytes (columna `Length`), sin contar el campo CRC (4 bytes).
   - Resumen de la información más importante contenida en los protocolos reconocidos en el paquete (columna `Info`).

Con el primer paquete seleccionado, observa en el Panel 2 de `wireshark` los detalles de los protocolos para ese paquete. Indica qué protocolos se usan en ese primer paquete y a qué nivel de la arquitectura TCP/IP corresponden dichos protocolos.

3. Teniendo seleccionado el primer paquete de la captura, en la primera pestaña (`Frame`) del Panel 2 se muestra información estadísitica relativa a la captura de ese paquete. Es la única pestaña que no tiene información de ningún protocolo contenido en el paquete, y en general no necesitaremos consultar dicha pestaña.
4. El resto de pestañas del Panel 2 contiene las cabeceras de los protocolos reconocidos en el paquete, empezando por `Ethernet` y siguiendo con los protocolos de niveles superiores.
5. Teniendo seleccionado el primer paquete de la captura, despliega la pestaña que se corresponde con el protocolo Ethernet. Indica qué campos observas en la cabecera de Ethernet, comprueba que la longitud de estos campos se corresponde con lo que hemos visto en la parte de teoría. Apunta los valores de estos campos.



6. Pulsa sobre el campo `Type` de la cabecera `Ethernet` y observa cómo en la zona del Panel 3 que muestra el contenido del paquete en hexadecimal, se colorea dicho valor. Observa que `wireshark` interpreta el valor de `Type` 0x0800 como el código asociado al protocolo IP. ¿Qué significa que el valor del campo `Type` se corresponda con el código asociado al protocolo IP?
7. Observa que en las capturas no aparecen los bytes ni el preámbulo, ni el comienzo de trama. El hardware de la tarjeta Ethernet elimina estos campos, pues no forman parte propiamente de la trama Etherente. Observa que tampoco aparece el CRC: el hardware de la tarjeta Ethernet comprueba que es correcto y lo elimina también de la trama. Si no fuera correcto descartaría la trama y no aparecería en la captura.
8. Selecciona el segundo paquete y observa en el Panel 2 de `wireshark` los detalles de los protocolos para ese paquete. Indica qué protocolos se usan en ese segundo paquete y a qué nivel de la arquitectura TCP/IP corresponden dichos protocolos.
9. Con el segundo paquete seleccionado, despliega la pestaña que se corresponde con el protocolo Ethernet. Indica qué campos observas en la cabecera de Ethernet. A la vista de los valores de estos campos indica si crees que este segundo paquete lo envía la misma máquina que envía el primer paquete.
10. Fíjate en la longitud del primer paquete que aparece en su columna `Length` del Panel 1. Dicha longitud hace referencia a la longitud de toda la trama Ethernet sin el CRC. Para calcular la longitud de toda la trama Ethernet habría que sumar a la columna `Length` de una trama los 4 bytes del CRC que no aparecen en la trama capturada. ¿Crees que la primera trama lleva bits de relleno en Ethernet?
11. Si la columna `Length` de la trama tuviera un valor igual a 60 bytes (longitud total de la trama igual a 64 bytes: 60 más 4 bytes del CRC) ¿podrías decir si dicha trama tiene o no relleno?
12. Observa el paquete número 18. Indica qué protocolos se usan en ese paquete y a qué nivel de la arquitectura TCP/IP corresponden dichos protocolos.
13. Observa el campo longitud de la trama Ethernet asociada al paquete número 18. Si la máquina que está enviando esa información hubiese tenido más datos para enviar dentro de la trama 18, explica si hubiera podido incluirlos también en el campo de datos de dicha trama.

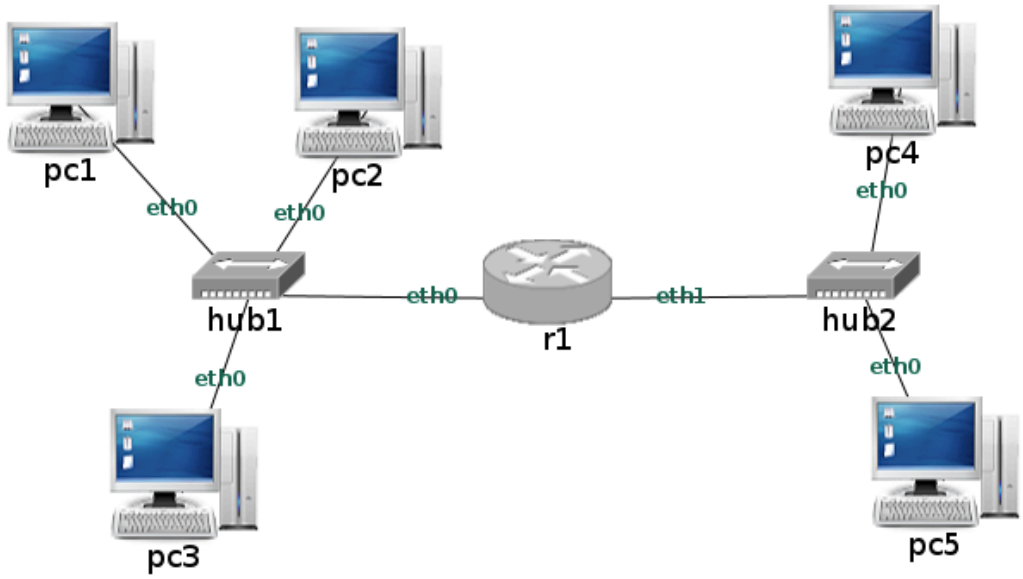
Cierra el fichero de captura `cap1.cap` y abre el fichero de captura `cap2.cap` con `wireshark` y responde a las siguientes preguntas:

1. Teniendo seleccionado el primer paquete de la captura, despliega la pestaña que se corresponde con el protocolo Ethernet. Indica qué campos observas en Ethernet. Apunta los valores de estos campos.
2. Fíjate en el campo `Type`. El valor es diferente al que viste en el fichero de captura anterior. ¿A qué protocolo se refiere este valor?
3. ¿Qué significa el valor del campo dirección destino Ethernet que aparece en ese primer paquete?
4. Fíjate en el campo longitud de la primera trama. ¿Cuánto es la longitud total de la trama contando el CRC?

5. En este caso, el paquete es un mensaje del protocolo ARP que va encapsulado dentro de Ethernet. Todos los mensajes del protocolo ARP tienen la misma longitud, 28 bytes. La cabecera de Ethernet ocupa 14 bytes y el CRC 4 bytes. Por tanto la longitud total de la trama sería 46 bytes y será necesario introducir relleno para alcanzar la longitud de trama mínima en Ethernet (64 bytes). El relleno debería ser 18 bytes.
6. Observa para este paquete el campo `Padding`. ¿Qué longitud tiene? ¿Qué crees que significa este campo?

2. Generación de tráfico Ethernet, captura y análisis de tráfico

Arranca NetGUI y dibuja el siguiente diagrama con dos redes unidas mediante el encaminador (*router*) `r1`:



Antes de arrancar las máquinas guarda este escenario de red en una carpeta nueva denominada `p0-lab`. Para ello utiliza la opción del menú `File->Save`. No arranques aún las máquinas.

Para poder realizar esta parte de la práctica es necesario realizar una configuración inicial en las máquinas cuando éstas arranquen. Esta configuración es el objetivo de estudio de los siguientes temas, por eso, para realizar esta práctica te damos la configuración dentro del fichero `p0-config.tgz`. Descarga dicho fichero de la página de la asignatura, guárdalo, por ejemplo, dentro de la carpeta `Descargas`. Desde un terminal de la máquina real ejecuta los siguientes comandos, por ejemplo, suponiendo que estás en zeta25:

```
usuario@zeta25:~$ cd p0-lab
usuario@zeta25:~/p0-lab$ tar xzvf ../Descargas/p0-config.tgz
```

Arranca cada uno de los PCs y el router, de uno en uno, esperando que termine de arrancar una máquina para arrancar la siguiente. Observarás que el icono de las máquinas aparece ahora con dos triángulos azules, que indican que las máquinas están ejecutándose. Al arrancar las máquinas se configuran con una dirección de nivel de red, una dirección IP. El protocolo IP será objeto de estudio del tema siguiente.

1. Consulta las direcciones Ethernet que hay configuradas en cada una de las interfaces de las máquinas, para ello ejecuta por ejemplo en `pc1`:

   ```
   pc1:~# ifconfig eth0
   ```

   Ten en cuenta que en `r1` deberás ejecutarlo tanto para `eth0` como para `eth1`.

   Apunta las direcciones Ethernet de cada interfaz y dispositivo.

2. Inicia una captura en `pc3` y otra en `pc4`. Para ello ejecuta los siguientes comandos.

   En `pc3`:

   ```
   pc3:~# tcpdump -i eth0 -s 0 -w /hosthome/pc3.cap
   ```

   En `pc4`:

   ```
   pc4:~# tcpdump -i eth0 -s 0 -w /hosthome/pc4.cap
   ```

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

   ```
   pc1:~# arping -c 1 00:07:e9:22:22:22
   ```

   Donde:

   - La dirección Ethernet que estamos utilizando (00:07:e9:22:22:22) es la dirección Ethernet destinataria de las tramas, en este caso la de `pc2`.

- La opción `-c 1` hace que `arping` envíe un único paquete ARP en una trama Ethernet destinada a la máquina `pc2`, y que ésta responda con otro paquete ARP.

Interrumpe las capturas pulsando `Ctrl+C` en cada una de las ventanas de `pc3` y `pc4`.

Analiza las tramas Ethernet que aparecen en ambas capturas. Para cada paquete indica:

(a) Dirección Ethernet origen.

(b) Dirección Ethernet destino.

(c) ¿Qué ocurre en la captura de `pc4`?

(d) ¿Qué crees que se hubiera capturado en las interfaces de `pc1(eth0)`, `pc2(eth0)`, `r1(eth0)`, `r1(eth1)` y `pc5(eth0)` si hubiéramos arrancado también `tcpdump` en dichas interfaces? ¿Por qué?

(e) Indica qué máquinas reciben la primera trama capturada y qué máquinas la procesan y se la entregan al protocolo de nivel superior.

(f) Indica qué máquinas reciben la segunda trama capturada y qué máquinas la procesan y se la entregan al protocolo de nivel superior.

(g) Si la primera trama llevara como dirección destino ff:ff:ff:ff:ff:ff indica qué máquinas recibirían dicha trama y qué máquinas se la entregarían al protocolo de nivel superior.

3. Supón qué ocurriría si se enviara una trama Ethernet de `pc4` a `pc5` y se capturara el tráfico en las siguientes interfaces: `pc1(eth0)` y `r1(eth1)`. Realiza la prueba y comprueba si tus suposiciones son ciertas.

4. Supón qué ocurriría si se enviara una trama Ethernet de `pc1` a `pc4` y se capturara el tráfico en `pc2(eth0)` y en `pc5(eth0)`. Realiza la prueba y comprueba si tus suposiciones son ciertas.