Prácticas con NetGUI
Práctica 1: Ethernet, Hub, Switch

Fundamentos de Redes de Ordenadores

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

Octubre de 2022

Resumen

En esta práctica se mostrará el encapsulamiento entre unidades de datos de diferentes protocolos 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`, y a analizarlas con la herramienta `wireshark`. Para la creación de una red Ethernet se usarán hubs y switches, mostrando las diferencias en el comportamiento de cada uno de estos dispositivos.

IMPORTANTE: Toma nota de todo lo que hagas en un **cuaderno de laboratorio** 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 y tendrás que entregarlo en el plazo establecido.

1. Análisis de ficheros de captura de tráfico

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

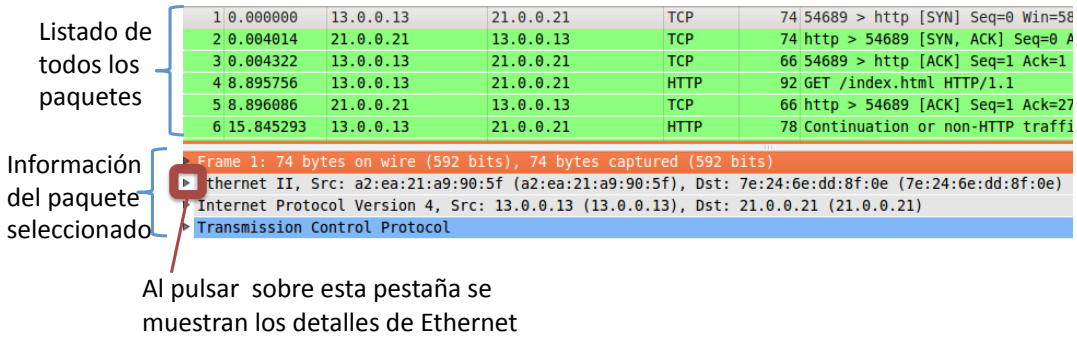
1. Selecciona el primer paquete que aparece en la captura, pulsando sobre la primera línea del Panel 1 (lista de paquetes). Éste quedará marcado en un color diferente:

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 importantes contenida en los protocolos reconocidos en el paquete (columna `Info`).

   Con el primer paquete seleccionado, observa 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. Para ello, puedes seleccionar la pestaña Ethernet dentro de Wireshark y con el botón derecho del ratón selecciona la entrada 'Copy all visible selected tree items' para que los campos de la cabecera Ethernet se queden copiados en el portapapeles y puedas pegarlos en el documento de la memoria.



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?
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 y análisis de la captura de tráfico

Descárgate de la siguiente página todos los escenarios de red, uno de estos ficheros será utilizado en este apartado. El resto de ficheros los utilizarás en apartados posteriores. Ten en cuenta que deberás introducir tu DNI para acceder a dicho escenario porque cada alumno partirá de una configuración diferente:

`https://mobiquo.gsyc.urjc.es/practicas/fro/p1.html`

Descomprime el fichero `p1-ethernet.tgz` usando el botón derecho (opción Extraer a).

Desde un terminal ejecuta: `netgui.sh`

Carga el escenario que acabas de descomprir: `File` → `Open` y navega por la ventana hasta la carpeta donde hayas dejado el escenario de NeGUI, de forma que en la casilla `Folder name` debe aparecer todo el trayecto hasta dicha carpeta y terminar con la palabra `p1-ethernet` que es la carpeta que contiene la configuración del escenario. Al pulsar sobre el botón `Open` deberías ver un dibujo similar al mostrado en la figura 1:

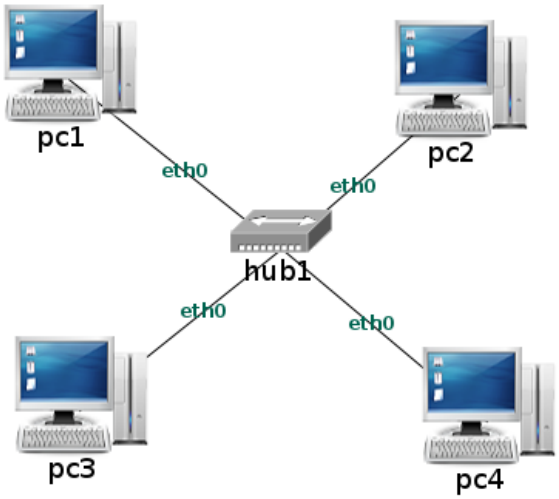


Figura 1: Escenario p1-ethernet.tgz

Arranca cada uno de los PCs, 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
   ```

   Apunta las direcciones Ethernet de cada interfaz de todos los pcs.

2. Inicia una captura de tráfico en `pc3`. Para ello ejecuta los siguientes comandos.

   En `pc3`:

   ```
   pc3:~# tcpdump -i eth0 -s 0 -w /hosthome/p1-ethernet.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`, susituyendo previamente donde dice `<direcciónEthernetPc2>` por la dirección Ethernet de la máquina `pc2`:

   ```
   pc1:~# arping -c 1 <direcciónEthernetPc2>
   ```

   Donde:

   - La dirección Ethernet que estamos utilizando 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 a la máquina `pc2` y que ésta le responda.

Interrumpe la captura pulsando `Ctrl+C` en la ventanas de `pc3`.

Analiza las tramas Ethernet que aparecen en la captura. Para cada paquete indica:

(a) Dirección Ethernet origen.
(b) Dirección Ethernet destino.
(c) ¿Qué crees que se hubiera capturado en las interfaces de `pc1(eth0)`, `pc2(eth0)`, `pc4(eth0)` si hubiéramos arrancado también `tcpdump` en dichas interfaces? ¿Por qué?
(d) Indica qué máquinas reciben la primera trama capturada y qué máquinas la procesan y se la entregan al protocolo de nivel superior.
(e) Indica qué máquinas reciben la segunda trama capturada y qué máquinas la procesan y se la entregan al protocolo de nivel superior.
(f) 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. Dispositivos de interconexión: hub y switch

3.1. Diferencias en el comportamiento entre un hub y un switch

Descomprime el fichero `p1-hub-switch.tgz` y carga el escenario en NetGUI, similar al que se muestra en la figura 2. Arranca los pcs de uno en uno. Cuando todos los pcs estén arrancados, inicia el switch.

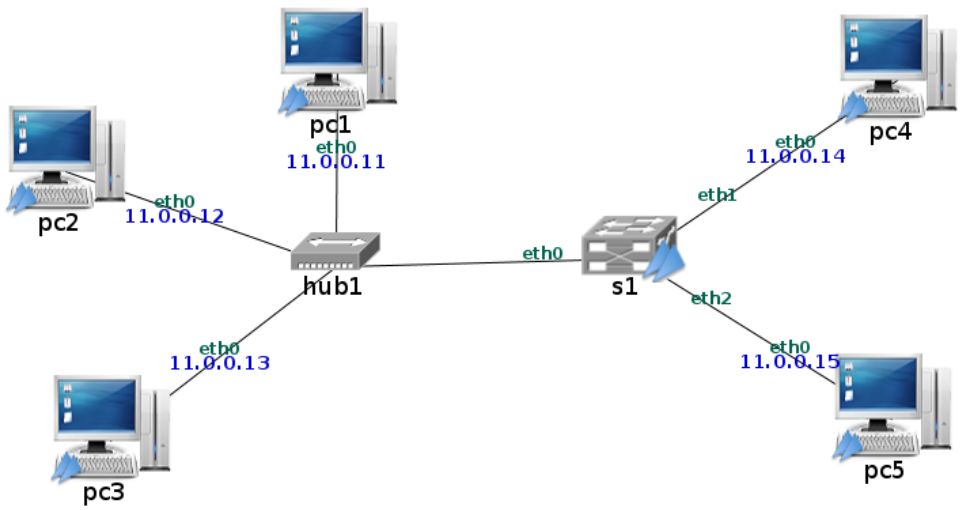


Figura 2: Escenario hub-switch.tgz

1. Indica cuál es la dirección Ethernet de `pc3`.
2. Comprueba que la tabla de direcciones Ethernet aprendidas en `s1` está vacía (sólo tiene información de las interfaces locales del switch).
3. ¿Qué crees que ocurrirá en el `hub1` cuando se ejecuta el comando `arping` desde `pc1` a `pc3`?
4. ¿Qué crees que ocurrirá en `s1` cuando se ejecuta el comando `arping` desde `pc1` a `pc3`?
5. Inicia una captura de tráfico en `pc2` y otra en `pc4` y guarda los paquetes capturados en 2 ficheros diferentes (`p1-switch1.cap` y `p1-switch2.cap` respectivamente). Ejecuta el comando `arping -c 3` desde `pc1` a `pc3` (la opción -c 3 hace que se envíen 3 paquetes de `pc1` a `pc3` y se reciba una respuesta por cada envío). Observa la tabla de direcciones Ethernet aprendidas en `s1` y explica su contenido.
6. Interrumpe las capturas de tráfico y explica justificadamente los mensajes capturados en `pc2` y `pc4`. Relaciona la información de las capturas con el contenido de la tabla de direcciones aprendidas por `s1`.
7. Borra la tabla de direcciones aprendidas en `s1`. ¿Qué crees que ocurrirá en `s1` cuando se ejecuta el comando `arping` desde `pc1` a `pc5`?

8. Comprueba tu suposición previa ejecutando ejecutando el comando `arping -c 3` en la máquina `pc1` dirigido a `pc5` y realizando las capturas de tráfico en `pc2` (en el fichero `p1-switch3.cap`), `pc4` (en el fichero `p1-switch4.cap`) y `pc5` (en el fichero `p1-switch5.cap`) que muestren el tráfico intercambiado. Explica el contenido de la tabla de direcciones aprendidas, interrumpe las capturas y explica las direcciones aprendidas en relación con el tráfico capturado.

9. Para ver cómo varía la tabla de direcciones aprendidas en un switch ejecuta el siguiente comando en `s1`:

   ```
   watch -n 1 brctl showmacs s1
   ```

   Este comando `watch` ejecuta cada segundo (`-n 1`) el comando `brctl showmacs s1`. Ejecuta `arping -c 5` desde `pc1` a `pc5`. Explica qué es lo que ves en la tabla de direcciones aprendidas. Indica en qué momento desaparecen las direcciones Ethernet de `pc1` y `pc5`. Cuando hayas terminado este apartado, puedes interrumpir el comando `watch` pulsando `Ctrl+c`.

10. Imagina que en un momento dado, la tabla de direcciones aprendidas del switch es similar a la siguiente (no se muestran las direcciones locales del propio switch):

    ```
    s1:~# brctl showmacs s1
    port no mac addr                is local?       ageing timer
      1     <dir_Ethernet_pc2>       no                225.60
      3     <dir_Ethernet_pc5>       no                225.60
    ```

    a) Indica qué tramas Ethernet habrá reenviado s1 para que esa tabla sea posible.

    b) ¿Qué ocurriría si el switch recibiera una trama Ethernet de `pc5` dirigida a `pc3`?

    c) ¿Qué ocurriría si el switch recibiera una trama Ethernet de `pc4` dirigida a `pc5`?

    d) ¿Cuánto tiempo falta para que el switch elimine de la tabla de direcciones aprendidas las direcciones de `pc2` y `pc5`?

11. Supón que `s1` recibe la siguiente trama Ethernet:

Dir Eth. Destino	Dir Eth. Origen	Protocolo	Contenido
ff:ff:ff:ff:ff:ff	`<dir_Ethernet_pc1>`	ARP	...

    Indica cómo se comportaría el switch en las siguientes situaciones:

    a) El switch `s1` tiene la tabla de direcciones aprendidas vacías.

    b) El switch `s1` tiene aprendida la dirección Ethernet de `pc1` en el puerto 1.

3.2. Influencia de los cambios de conexión física en la tabla de direcciones aprendidas de un switch

Descomprime el fichero `p1-hub-switch2.tgz` y carga el escenario en NetGUI, similar al que se muestra en la figura 3. Arranca las máquinas y el switch.

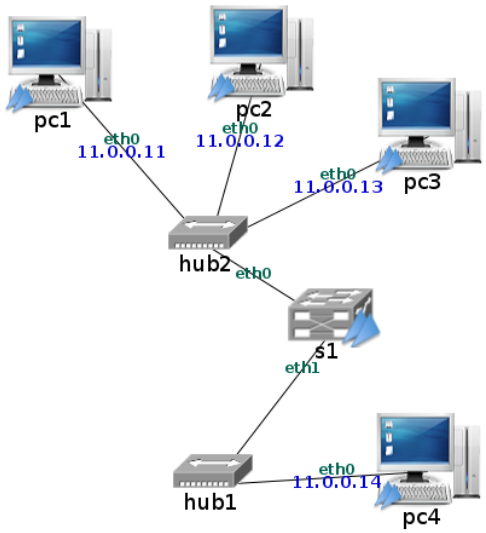


Figura 3: Escenario hub-switch2.tgz

1. Ejecuta el comando `arping` en `pc1` para que envíe un mensaje Ethernet `pc1` a `pc4`.
2. Consulta la tabla de direcciones aprendidas en `s1` y fíjate bien en los puertos donde `s1` ha aprendido.

3. Ejecuta el comando que te muestra la tabla de direcciones aprendidas cada segundo, para ver cómo va a variar su contenido.
4. Inicia una captura en `pc4` guarda su contenido en el fichero `p1-switch6.cap`
5. Antes de que caduquen las entradas de la tabla de direcciones aprendidas en `s1` (caducan a los 5 minutos), apaga `pc1` y borra el cable que le une al `hub2`. Crea un nuevo cable que una `pc1` y `hub1` y arranca `pc1`. Al arrancar `pc1` se generan automáticamente unos mensajes de autoconfiguración que provocan que el switch `s1` aprenda el nuevo sitio de `pc1`. Comprueba como se han modificado las entradas en la tabla de direcciones aprendidas en `s1` y observa el tiempo que muestra la tabla para la entrada de `pc1`.
6. Interrumpe la captura y observa cómo la máquina `pc1` ha generado mensajes al arrancar que han provocado la actualización de la tabla de direcciones aprendidas del switch.
7. ¿Qué crees que pasaría si `pc1` no hubiera generado ningún trafico automático al arrancar y en `pc3` se ejecutara `arping` hacia `pc1`?

4. Entrega de la práctica

Para entregar la práctica sube a aula virtual 2 ficheros:

- El fichero con la memoria de la práctica en formato pdf: las respuestas a las preguntas de la práctica.
- Las capturas `p1-ethernet.cap` y desde `p1-switch1.cap` a `p1-switch6.cap` dentro de un fichero comprimido: `p1.zip`. Para ello, primero crea una carpeta `p1` y mete dentro de esa carpeta todas los ficheros de captura. Desde el navegador de archivos pulsa con el botón derecho del ratón sobre el nombre de la carpeta y selecciona `'Comprimir'`, nombre del archivador `'p1'` y extensión `'.zip'`.