



Universidad Rey Juan Carlos

E.T.S. INGENIERÍA DE TELECOMUNICACIÓN

FUNDAMENTOS DE REDES DE ORDENADORES

Práctica 1

Autor:
Javier Izquierdo Hernández

October 12, 2022

Contenidos

1	Análisis de ficheros de captura de tráfico	2
1.1	Cap1.cap	2
1.2	Cap2.cap	5
2	Generación de tráfico Ethernet y análisis de la captura de tráfico	7
2.1	Paquete 1	7
2.2	Paquete 2	8
3	Dispositivos de interconexión: hub y switch	9
3.1	Diferencias en el comportamiento entre un hub y un switch	9
3.2	Influencia de los cambios de conexión física en la tabla de direcciones aprendidas de un switch	13

1 Análisis de ficheros de captura de tráfico

1.1 Cap1.cap

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=1460
2	0.004014	21.0.0.21	13.0.0.13	TCP	74	http > 54689 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
3	0.004322	13.0.0.13	21.0.0.21	TCP	66	54689 > http [ACK] Seq=1 Ack=1 Win=5840 Len=0
4	0.895756	13.0.0.13	21.0.0.21	HTTP	92	GET /index.html HTTP/1.1
5	0.896086	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 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 estadística 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.

1	0.000000	13.0.0.13	21.0.0.21	TCP	74 54689 > http [SYN] Seq=0 Win=58
2	0.004014	21.0.0.21	13.0.0.13	TCP	74 http > 54689 [SYN, ACK] Seq=0 A
3	0.004322	13.0.0.13	21.0.0.21	TCP	66 54689 > http [ACK] Seq=1 Ack=1
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
6	15.845293	13.0.0.13	21.0.0.21	HTTP	78 Continuation or non-HTTP traffi

▶ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)					
▶ Ethernet II, Src: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f), Dst: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)					
▶ Internet Protocol Version 4, Src: 13.0.0.13 (13.0.0.13), Dst: 21.0.0.21 (21.0.0.21)					
▶ Transmission Control Protocol					

Ethernet II, Src: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f)

Dst: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)

Destination: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)

Source: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f)

Type: IPv4 (0x0800)

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?

Significa que el protocolo encapsulado dentro de del campo de datos es un datagrama IP. Indica que se usara el 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.

Se utiliza el protocolo Ethernet (Nivel de enlace), IP (Nivel de red) y TCP (Nivel de transporte).

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.

Creo que lo envía otra máquina hacia la que envió el mensaje anterior.

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?

No lleva bits de relleno porque la cantidad de bytes es mayor a 60.

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?

Si que tiene 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.

Se utiliza el protocolo Ethernet (Nivel de enlace), IP (Nivel de red) y TCP (Nivel de transporte).

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.

No porque tiene el numero maximo de bytes.

1.2 Cap2.cap

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.

Ethernet II, Src: Cisco251_af:f4:54 (00:07:0d:af:f4:54),

Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: Cisco251_af:f4:54 (00:07:0d:af:f4:54)

Type: ARP (0x0806)

Padding: 0601040000000000201000302000005010301

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?

Pertenece al protocolo ARP

3. ¿Qué significa el valor del campo dirección destino Ethernet que aparece en ese primer paquete?

Indica que la trama será entregada a todas las estaciones de la subred (Broadcast).

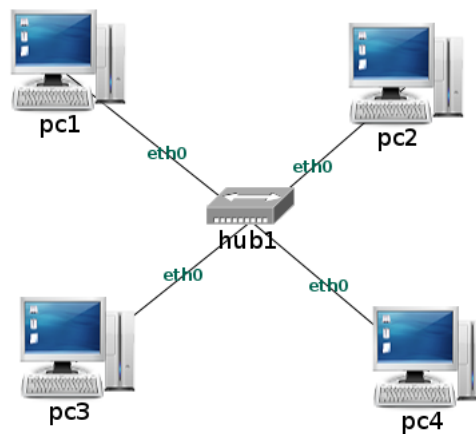
4. Fíjate en el campo longitud de la primera trama. ¿Cuánto es la longitud total de la trama contando el CRC?

Es de 64 bytes

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 seria 46 bytes y será necesario introducir relleno para alcanzar la longitud de trama minima en Ethernet (64 bytes). El relleno deberia ser 18 bytes.
6. Observa para este paquete el campo Padding. ¿Qué longitud tiene? ¿Qué crees que significa este campo?

Tiene una longitud de 18 bytes, que es igual al relleno, por lo que creo que es el relleno.

2 Generación de tráfico Ethernet y análisis de la captura de tráfico



2.1 Paquete 1

a Dirección Ethernet origen.

Es 00:07:e9:11:67:11

b Dirección Ethernet destino.

Es 00:07:e9:22:67:22

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?

Hubiera ocurrido lo mismo, porque están conectados a un hub.

- d Indica qué máquinas reciben la primera trama capturada y qué máquinas la procesan y se la entregan al protocolo de nivel superior.

El mensaje es recibido por el hub que lo envía al pc2 para que este lo procese y se lo entregue al protocolo superior al protocolo de nivel superior.

- e 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.

El hub recibiría la trama, y se la enviaría a todos los pc conectados a dicho hub.

2.2 Paquete 2

- a Dirección Ethernet origen.

Es 00:07:e9:22:67:22

- b Dirección Ethernet destino.

Es 00:07:e9:11:67:11

- 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?

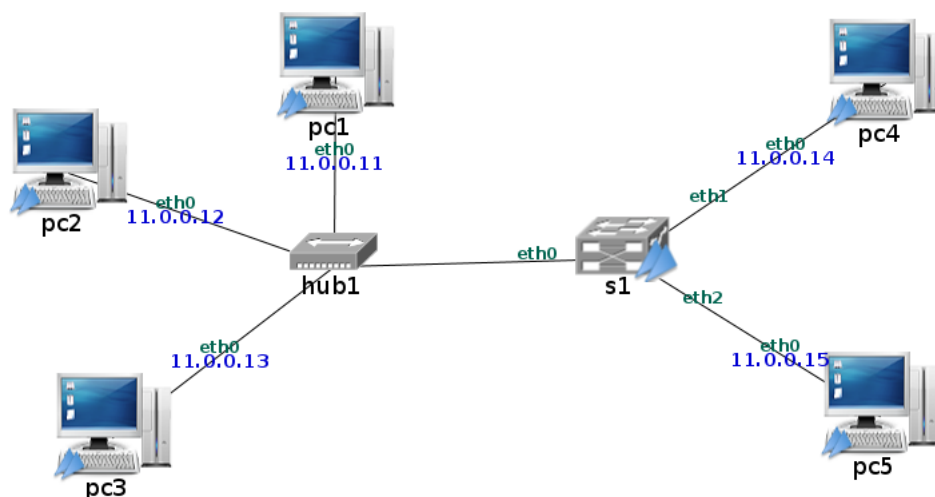
Hubiera ocurrido lo mismo, porque están conectados a un hub.

- d Indica qué máquinas reciben la segunda trama capturada y qué máquinas la procesan y se la entregan al protocolo de nivel superior.

El mensaje es recibido por el hub que lo envía al pc1 para que este lo procese y se lo entregue al protocolo superior

3 Dispositivos de interconexión: hub y switch

3.1 Diferencias en el comportamiento entre un hub y un switch



1. Indica cuál es la dirección Ethernet de pc3.
La dirección Ethernet es 00:07:e9:33:67:33
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 arpinger desde pc1 a pc3?

El hub reenviara el mensaje a todos los ordenadores, y estos comprobaran si el mensaje va dirigido a ellos, si es así lo procesarán, y si no, lo descartarán.

4. ¿Qué crees que ocurrirá en s1 cuando se ejecuta el comando arping desde pc1 a pc3?

El switch asignará la dirección Ethernet del pc1 a un puerto en la tabla de direcciones, y enviará los mensajes igual que el hub. Cuando pc3 envía la respuesta al mensaje también asignará este a la tabla de direcciones, y no hará nada más porque sabe que pc1 y pc3 están conectados a través del hub juntos.

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.

```
s1 login: root (automatic login)
Last login: Mon Oct 10 12:27:50 UTC 2022 on tty0
s1:~# brctl showmacs s1
```

port	no	mac addr	is local?	ageing timer
1		00:07:e9:11:67:11	no	64.61
1		00:07:e9:33:67:33	no	64.61
2		5a:11:71:9b:44:74	yes	0.00
1		6e:b6:0b:0f:3c:d7	yes	0.00
3		d2:b2:c7:18:fb:94	yes	0.00

El switch s1 ha aprendido las direcciones de pc1 y pc3 como he explicado en el apartado anterior. Ahora los mensajes que vayan hacia pc1 o pc3 no serán reenviados como en un hub, sino que tendrían asignada una salida determinada hasta que pasen 5 min sin recibir uno de los dos, que en ese caso se borra su dirección de la tabla.

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.

Pc2: captura los 6 mensajes porque estos son distribuidos por el hub.

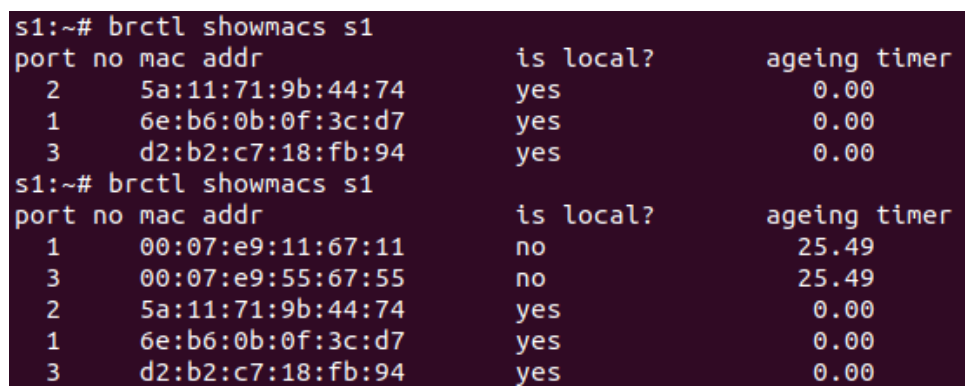
Pc4: solo captura el primer mensaje, porque es el único en el que la dirección de destino no estaba en la tabla.

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?

El switch asignará la dirección Ethernet del pc1 a un puerto en la tabla de direcciones, y enviará los mensajes igual que el hub. Cuando pc5 envía la respuesta al mensaje también asignará este a la tabla de direcciones, y se lo enviará al hub de donde venía pc1.

Luego, los mensajes serán dirigidos a las direcciones asignadas en la tabla.

8. Comprueba tu suposición previa 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.



```
s1:~# brctl showmacs s1
port no mac addr          is local?    ageing timer
 2    5a:11:71:9b:44:74    yes          0.00
 1    6e:b6:0b:0f:3c:d7    yes          0.00
 3    d2:b2:c7:18:fb:94    yes          0.00
s1:~# brctl showmacs s1
port no mac addr          is local?    ageing timer
 1    00:07:e9:11:67:11    no          25.49
 3    00:07:e9:55:67:55    no          25.49
 2    5a:11:71:9b:44:74    yes          0.00
 1    6e:b6:0b:0f:3c:d7    yes          0.00
 3    d2:b2:c7:18:fb:94    yes          0.00
```

Las direcciones aprendidas son las de pc1 y las de pc5. Como había explicado anteriormente pc2 captura todos los mensajes porque está conectado al mismo hub que pc1, pc5 captura todos los mensajes porque iban o salían de él, y pc4 solo captura el primero porque era el único en que el switch no tenía asignado la dirección de destino.

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`.

En la tabla de direcciones se puede ver que las direcciones de pc1 y pc5 se les ha reiniciado el tiempo de envejecimiento. El tiempo máximo es 5 min o 300 seg.

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):

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

Habrá enviado tramas a pc2 y a pc5

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

Que las reenviaría como si fuera un hub.

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

Añadiría la dirección de pc4 a la tabla de direcciones y le enviaría el mensaje a la dirección que tiene guardada como pc5, reseteando el tiempo de envejecimiento de pc5.

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

Faltan 74.40 segundos para que sean eliminadas.

11. Supón que s1 recibe la siguiente trama Ethernet:

Dir Eth. Destino	Dir Eth. Origen	Protocolo	Mensaje
ff:ff:ff:ff:ff:ff	dir_Ethernet_pc1	Arp	...

Indica cómo se comportaría el switch en las siguientes situaciones:

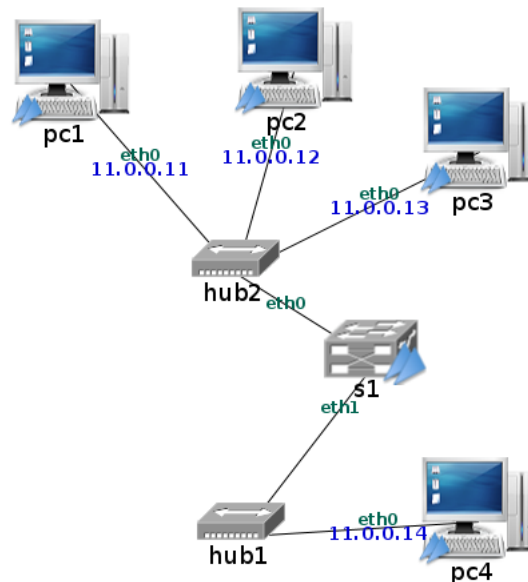
a El switch s1 tiene la tabla de direcciones aprendidas vacías.

Guardaría la dirección de s1 y reenviaría el mensaje a todas los pc ya que la dirección de destino es de broadcast.

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

Reiniciaría el tiempo de envejecimiento de pc1 y reenviaría el mensaje a todas los pc ya que la dirección de destino es de broadcast.

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



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.

```
s1 login: root (automatic login)
s1:~# brctl showmacs s1
port no mac addr          is local?    ageing timer
  1    7a:fd:d3:97:11:e0    yes          0.00
  2    e2:de:5e:d1:eb:1e    yes          0.00
s1:~# brctl showmacs s1
port no mac addr          is local?    ageing timer
  1    00:07:e9:11:67:11    no           4.16
  2    00:07:e9:44:67:44    no           4.16
  1    7a:fd:d3:97:11:e0    yes          0.00
  2    e2:de:5e:d1:eb:1e    yes          0.00
```

3. Ejecuta el comando que te muestra la tabla de direcciones aprendidas cada segundo, para ver cómo va a variar su contenido.

port	no	mac addr	is local?	ageing timer
1		00:07:e9:11:67:11	no	73.01
2		00:07:e9:44:67:44	no	73.01
1		7a:fd:d3:97:11:e0	yes	0.00
2		e2:de:5e:d1:eb:1e	yes	0.00

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.

El puerto de pc1 cambia de 1 a 2.

port	no	mac addr	is local?	ageing timer
2		00:07:e9:11:67:11	no	1.10
2		00:07:e9:44:67:44	no	206.30
1		7a:fd:d3:97:11:e0	yes	0.00
2		e2:de:5e:d1:eb:1e	yes	0.00

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?

El mensaje de pc3 no hubiera llegado al nuevo pc1 porque el switch lo reenviaría a la antigua dirección que este tiene guardada, hasta que o se eliminara la dirección de pc1 por tiempo o pc1 mandase un mensaje.