Yolanda Lillo Mata ISAM

**PRÁCTICA 1**

**1. Funcionamiento de hubs y switch.**

**1.1. Comunicación entre máquinas con s1 apagado**

1. Piensa en qué paquetes se capturará en pc2, pc3 y en pc5 si se hace un ping desde pc1 a pc2.

Creo que solo se capturan paquetes en pc2 ya que tenemos el switch apagado y las máquinas pc1 y pc2 al ser vecinas se conecta directamente gracias al hub.

2. Lanza tcpdump en pc2, pc3 en pc5. A continuación ejecuta la siguiente orden en pc1 para hacer un ping a pc2: pc1:~# ping -c 3 11.0.0.2

(-c 3 hace que el ping solo enve 3 paquetes ICMP)

Observa el tráfico capturado en pc2, pc3 y pc5 y comprueba si ha ocurrido lo que pensabas.

Observamos que solo captura pc2 paquetes. El ping entre pc1 y pc2 funciona porque están conectados al mismo hub y en la misma subred.

3. Comprueba que no existe conectividad (es decir, que no puede hacerse ping) entre máquinas que estén en diferentes hubs.

**1.2. Comunicación entre máquinas con s1 arrancado**

1. Arranca el switch s1.

2. Piensa en qué paquetes se capturará ahora en pc2, pc3 y en p5 repitiendo el mismo ping.

Pc3 y pc5 aunque no sean máquinas que interfieran en el ping reciben una solicitud ARP puesto que el switch la envía a todas las máquinas de su interfaz en busca de pc2 pero, pc3 y pc3 no la contestan puesto que no es para ellos.

3. Comprueba la caché de ARP en pc1. Si aún está en ella la dirección Ethernet de pc2 borra esa entrada de la caché de ARP.

4. Lanza tcpdump en pc2, pc3 y en pc5. A continuación vuelve a hacer en pc1 el ping a pc2: pc1:~# ping -c 3 11.0.0.2 Observa el tráfico capturado en pc2, pc3 y pc5 y comprueba si ha ocurrido lo que pensabas.

5. Responde a estas preguntas:

¿Por qué llega a pc3 y a pc5 la solicitud de ARP enviada por pc1?

Porque el switch envía la solicitud ARP a todos los pcs.

¿Por qué NO llega a pc3 y a pc5 la respuesta de ARP enviada por pc2?

Porque como la respuesta no es para ellos, llega directamente a pc1 que es quien la necesita, es decir, como s1 ya ha aprendido que pc1 y pc2 está en su interfaz eth0

¿Por qué NO llega a pc3 y a pc5 el ICMP echo request enviado por pc1?

¿Por qué NO llega a pc3 y a pc5 el ICMP echo reply enviado por pc2?

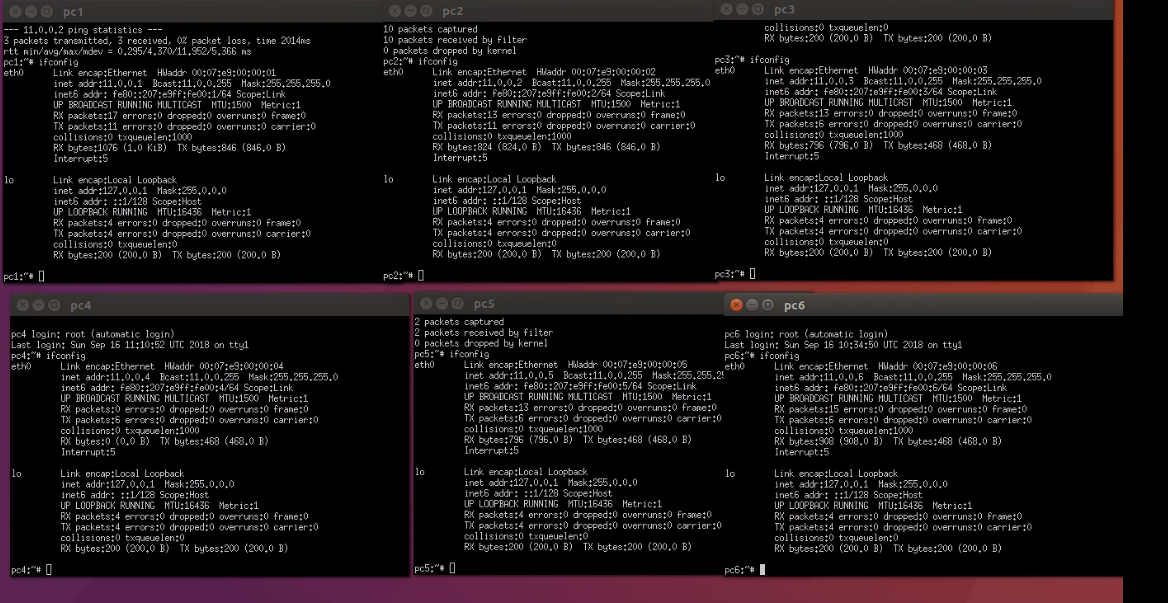
En estas dos pregunta ocurre lo mismo porque s1 solo reenvía por la eth0.

6. Comprueba las direcciones Ethernet que tiene cada interfaz de cada máquina de la figura (usando ifconfig), y apúntalas.

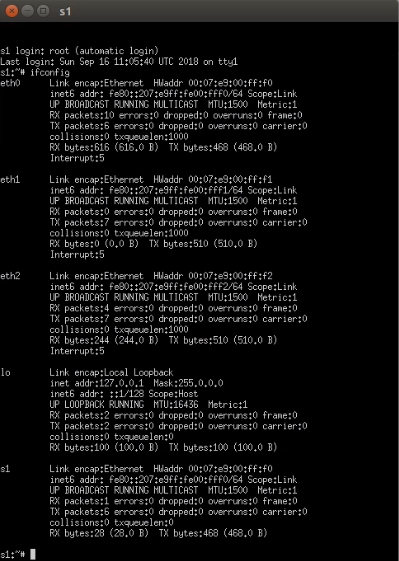
Pc1 → 00:07:e9:00:00:01 Pc2 → 00:07:e9:00:00:02 Pc3 → 00:07:e9:00:00:03

Pc4 → 00:07:e9:00:00:04 Pc5 → 00:07:e9:00:00:05 Pc6 → 00:07:e9:00:00:06

Adjunto captura utilizando el comando ifconfig que es como he mirado las direcciones Ethernet.



7. Mira la tabla de direcciones aprendidas por el switch s1 utilizando la orden brctl showmacs s1.



Vemos que están las direcciones Ethernet de pc1 y pc2 puesto que, con anterioridad hemos realizado un ping entre esas dos máquinas.

8. Comprueba que ahora sı existe conectividad entre todas las m´aquinas de la figura utilizando la orden ping.

Lo he comprobado y si existe conectividad gracias al switch que ya está encendido,

**2. Redes conectadas a través de switch y router.**

**2.1. Comunicación entre pc2 y pc4**

1. Observa la configuración que hay en el escenario para que pc2 y pc4 puedan intercambiar tráfico. ¿Cuál de los siguientes caminos crees que seguirán los mensajes ICMP echo request desde pc2 a pc4?

pc2 → s1 → s2 → pc4 Esta será la ruta que seguiran los mensajes lo he comprobado tras capturar tráfico(*tcpdump -i ethX -s 0 -s /hosthome/X.cap*) en diferentes lugares.

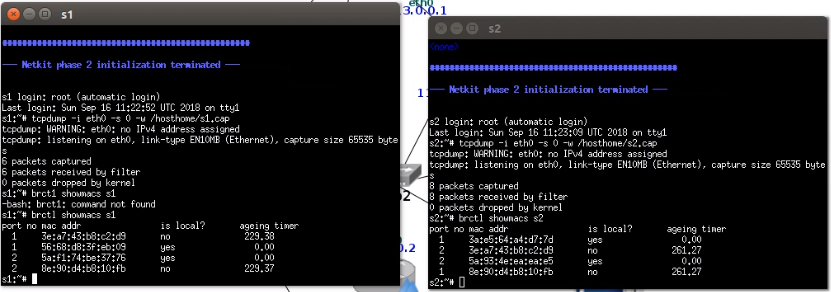
2. Indica cuántas solicitudes y respuestas de ARP ser´ıan necesarias para que dicho ping funcionase.

Se realizará una solicitud de pc2 a pc4 directamente ya que no pasa por ningún router solo por dos switches y la respuesta es de pc4 a pc2 atravesando también esos switches.

3. Indica qué direcciones Ethernet habrán aprendido s1 y s2 después de ejecutar el ping. Compruébalo.

Aquí vemos las direcciones que han aprendido cada uno de los routers son todas las que llevan un *no* en la pregunta *is local?*.

tcpdump -i eth0 -s 0 -v /hosthome/hub-switch-02.cap



4. ¿Crees que habr´a llegado alguno de los mensajes ICMP echo request a pc1, pc3 o pc5? Justifica la respuesta.

Observando las capturas se que sigue llegan por el switch cuando envía la solicitud a todos aunque no sea para ellos.

**2.2.Comunicación entre pc1 y pc3**

1. Observa la configuración que hay en el escenario para que pc1 y pc3 puedan intercambiar tráfico. ¿Cual de los siguientes caminos crees que seguirán los mensajes ICMP echo request desde pc1 a pc3?

Sigue el siguiente camino pc1→r1 → pc3, decido capturar en r1, s1 , r2 y pc3 hacemos de comprobar con route su tabla de encaminamiento.

2. Indica cuantas solicitudes y respuestas de ARP serán necesarias para que dicho ping funcionase.

Vemos como hay una solicitud ARP de pc1 a r1 y viceversa otra de r1 a pc3 pero la vuelta la hace por pc3 a r2 y de hay a r1 por tanto vemos cuatro solicitudes y cuatro respuestas. Vemos que la vuelta es por r2 por el TTL visto en las capturas y también por las tablas de encaminamiento.

3. Indica que direcciones Ethernet habrán aprendido s1 y s2 después de ejecutar el ping.

Con ifconfig vemos como s1 tiene las direcciones de pc1, r1eth0, pc3eth0,r2 y por último y en s2 vemos las direcciones de pc4, r2eth1, r2eth0.

4. ¿Crees que habrá llegado alguno de los mensajes ICMP echo request a pc2, pc4 o pc5? Justifica la respuesta.

Llegan mensajes ICMP a pc2 y pc4 pero no a pc5 donde solo llega la solicitud ARP.

**2.3. Comunicación entre pc2 y pc5.**

1. Observa la configuración que hay en el escenario para que pc2 y pc5 puedan intercambiar tráfico. ¿Cual de los siguientes caminos crees que seguirán los mensajes ICMP echo request desde pc2 a pc5?

Vemos que se sigue el siguiente camino pc2 →s1 → r1 → r2 → pc5.

2. Indica cuántas solicitudes y respuestas de ARP serán necesarias para que dicho ping funcionase.

Una solicitud de pc2 a r1 y una respuesta de r1 a pc2, otra solicitud de r1 a r2 y una respuesta de r2 a r1 y por último una solicitud ARP de r2 a pc5 y una respuesta de pc5 a r2.

3. Indica que direcciones Ethernet habrán aprendido s1 y s2 después de ejecutar el ping. Compruebalo.

En s1 vemos las direcciones Ethernet de r1eth0, r1eth1, r2eth0, r2eth1, pc2 y en s2 vemos r1eth0, r1eth1, r2eth1, pc2 y pc5.

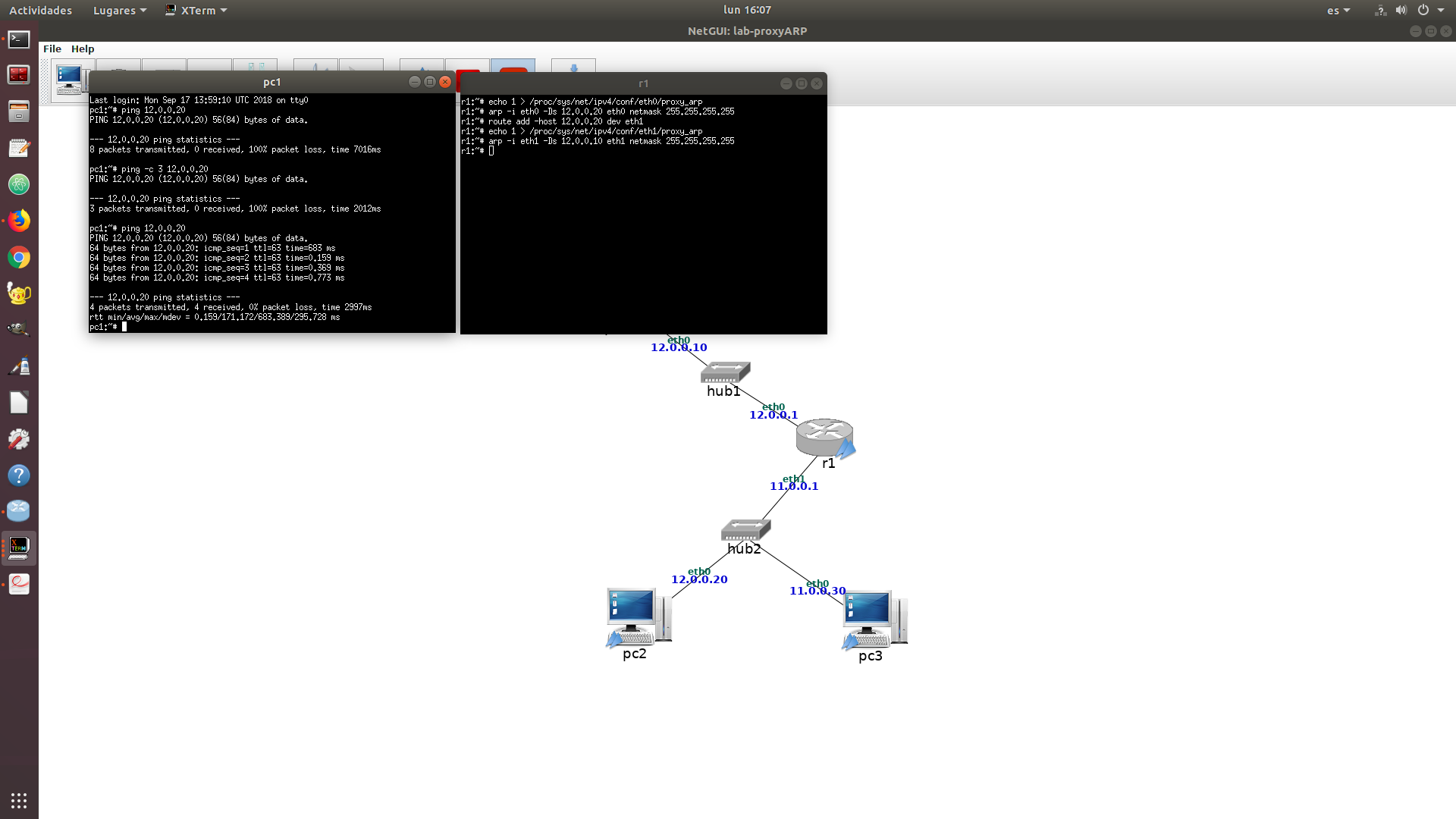
4. ¿Crees que habrá llegado alguno de los mensajes ICMP echo request a pc1, pc3 o pc4?

Llega a esas tres máquinas por el hub.

**3.Proxy ARP**

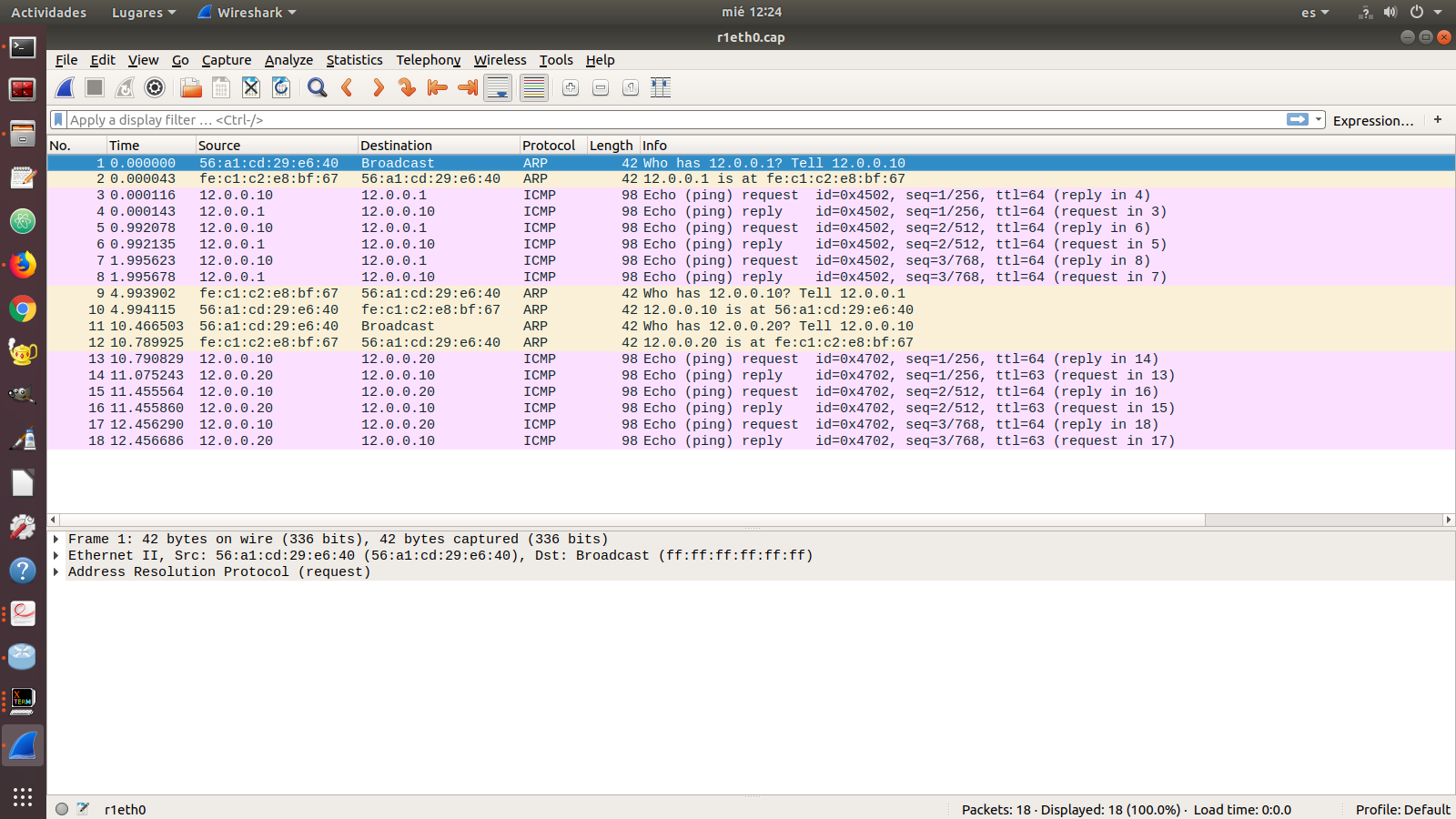
1. Activa proxy ARP en la configuración del router r1 para que las máquinas pc1 y pc2 tengan conectividad IP entre ellas en ambos sentidos. Explica qué modificaciones han sido necesarias y por qué.

He realizado los cambios que vemos en la captura de r1 utilizando los comandos necesarios de ARP para que así r1 pueda “mentir” utilizando una dirección distinta para que se pueda llevar a cabo el ping.

****

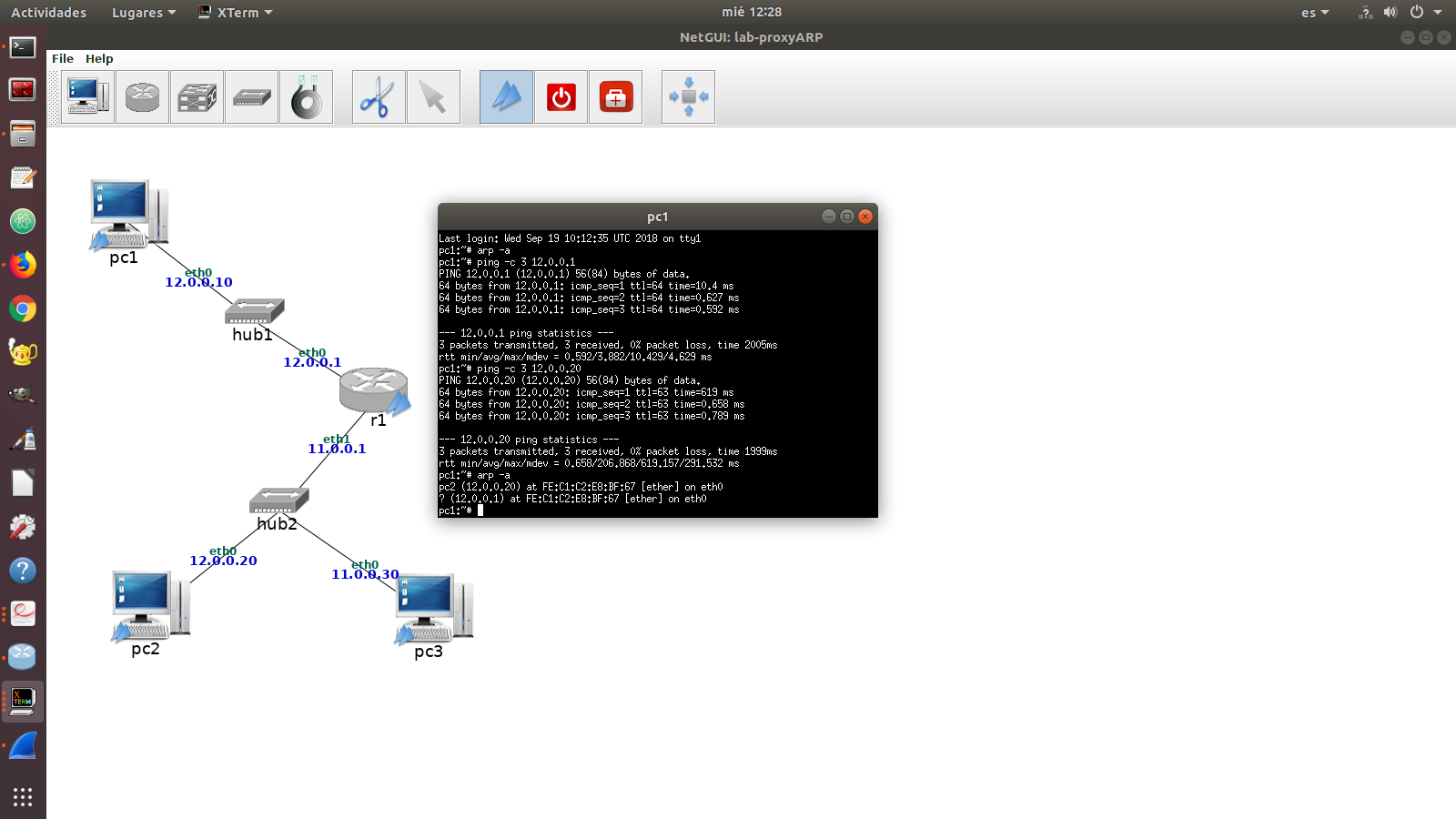
2. Con las cachés de ARP vacas, realiza una captura en la interfaz r1(eth0) guardando su contenido en un fichero y ejecuta un ping desde pc1 a 12.0.0.1, enviando solo 3 paquetes, y después un ping desde pc1 a pc2, enviando solo 3 paquetes. Interrumpe la captura y fíjate en las solicitudes de ARP que ves en el tráfico capturado. A partir de la captura y de las direcciones IP de r1: ¿como puedes saber que r1 está realizando proxy ARP?

Podemos ver como en el paquete 2 contesta con su dirección r1 y en el paquete 12 vuelve a responder con su dirección de r1 que ya sabía de antes eso quiere decir, que utiliza ARP proxy porque para distintas solicitudes el router contesta con la misma dirección. Adjunto captura.

****

3. Si se ha borrado la caché de ARP de pc1 vuelve a ejecutar los 2 pings anteriores y consulta la caché de ARP de pc1, indica que observas.

Observamos lo que vemos en la captura que tenemos debajo en la que podemos ver que proxy ARP funciona puesto que en pc1 vemos la dirección Ethernet de pc2.

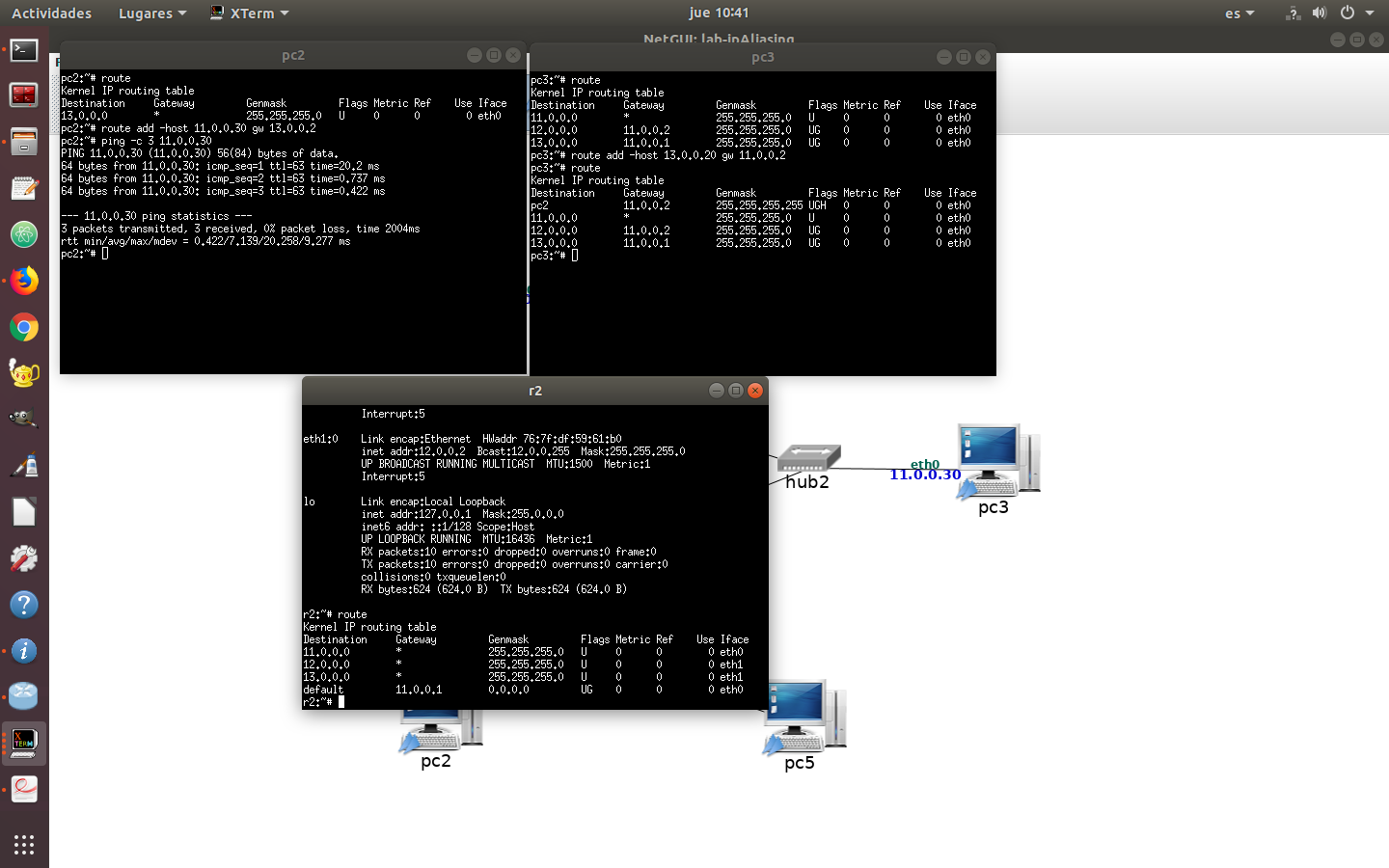
****

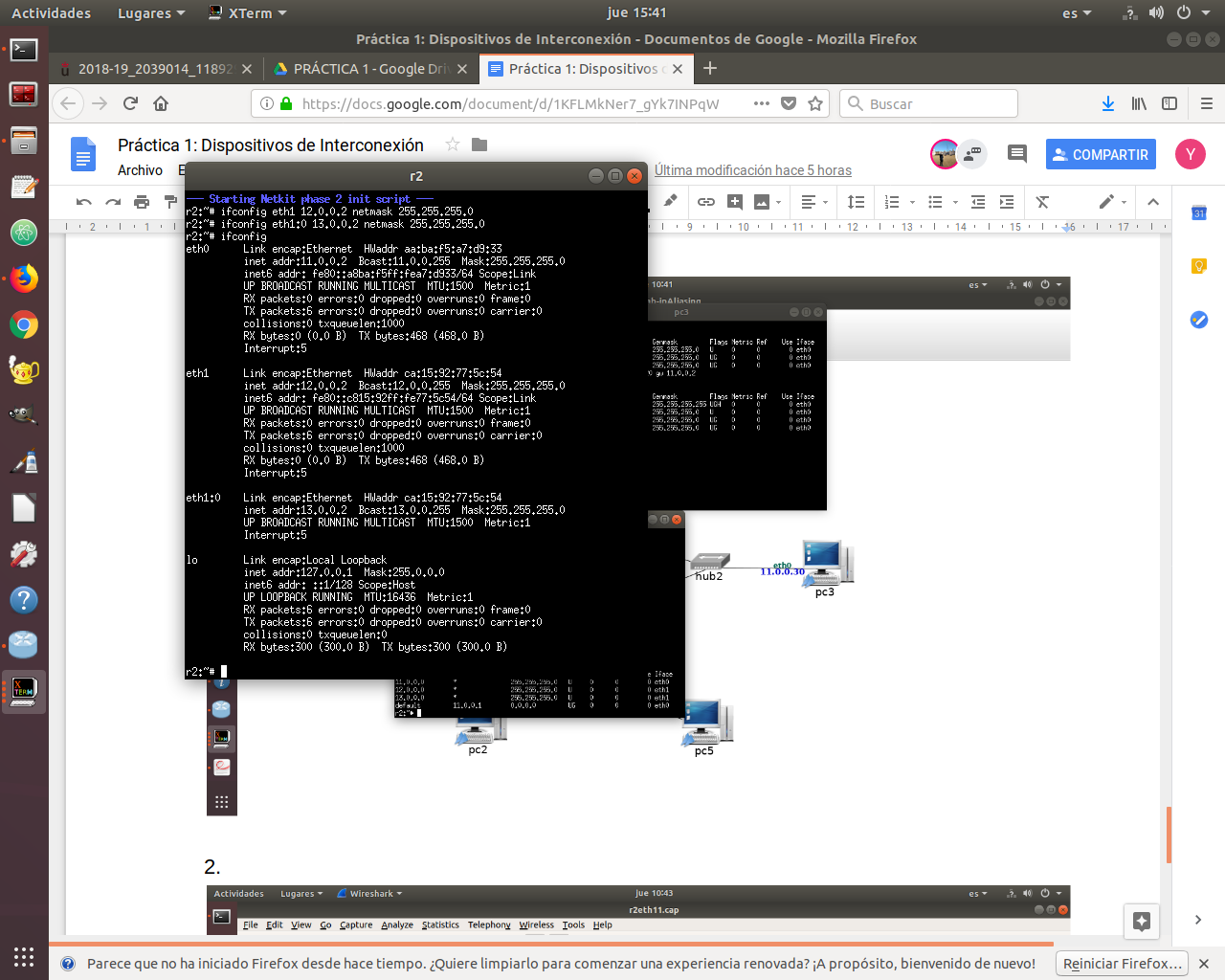
**4.IP aliasing**

1. Asigna direcciones IP adicionales en los routers mediante IP aliasing, y configura las tablas de encaminamiento que sean necesarias para que pc2 pueda hacer ping a pc3, ten en cuenta que desde r2 se deberá poder alcanzar también a pc1. Nótese que cuando añades una dirección por IP aliasing a una tabla de encaminamiento se añade automáticamente una entrada para la subred a la que pertenece, entrada que a

veces es necesario borrar para que no haya en la misma tabla dos rutas diferentes a la misma subred.

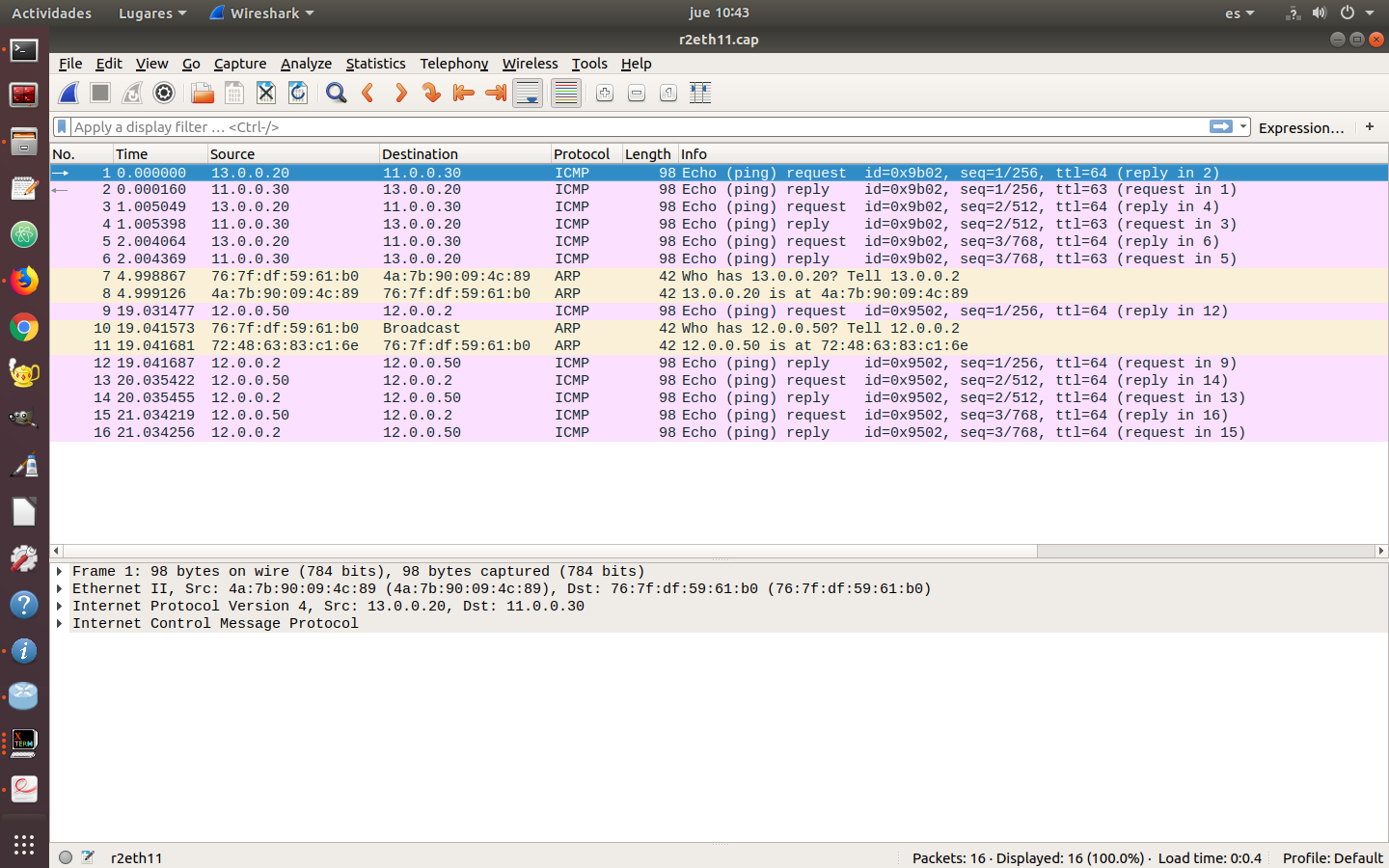
En r2 hemos realizado los comandos de Ip aliasing con ifconfig para que así no se nos eliminen como observamos en la segundo imagen de este apartado he puesto la dirección que tenía y además, he añadido en esa misma interfaz la IP 13.0.0.2 para que pc2 y pc3 puedan conectarse. Después, he añadido una ruta en pc2 para que que llegue a pc3 por la nueva IP y también en pc3 una ruta para que llegue a pc2 por la dirección 11.0.0.2 que es el r2 y no por el r1.





2. Realiza una captura en r2(eth1) guardando su contenido en un fichero y ejecuta un ping desde pc2 a pc3 enviando 3 paquetes y después ejecuta un ping desde pc5 a 12.0.0.2. Interrumpe la captura y observa las solicitudes de ARP. ¿Se puede saber solo mirando el chero de captura que en r2 no se ha configurado proxy ARP?

Si lo podemos ver aunque es muy difícil diferenciarlo yo diría que cuando pregunto por la misma interfaz o la ruta pasa por esa interfaz que es r2eth1 vemos que una vez nos contesta con la IP 12.0.0.2 y otra con 13.0.0.2 y así vemos que en una misma interfaz hay dos IPs lo que quiere decir que estamos utilizando IP aliasing y no proxy ARP.

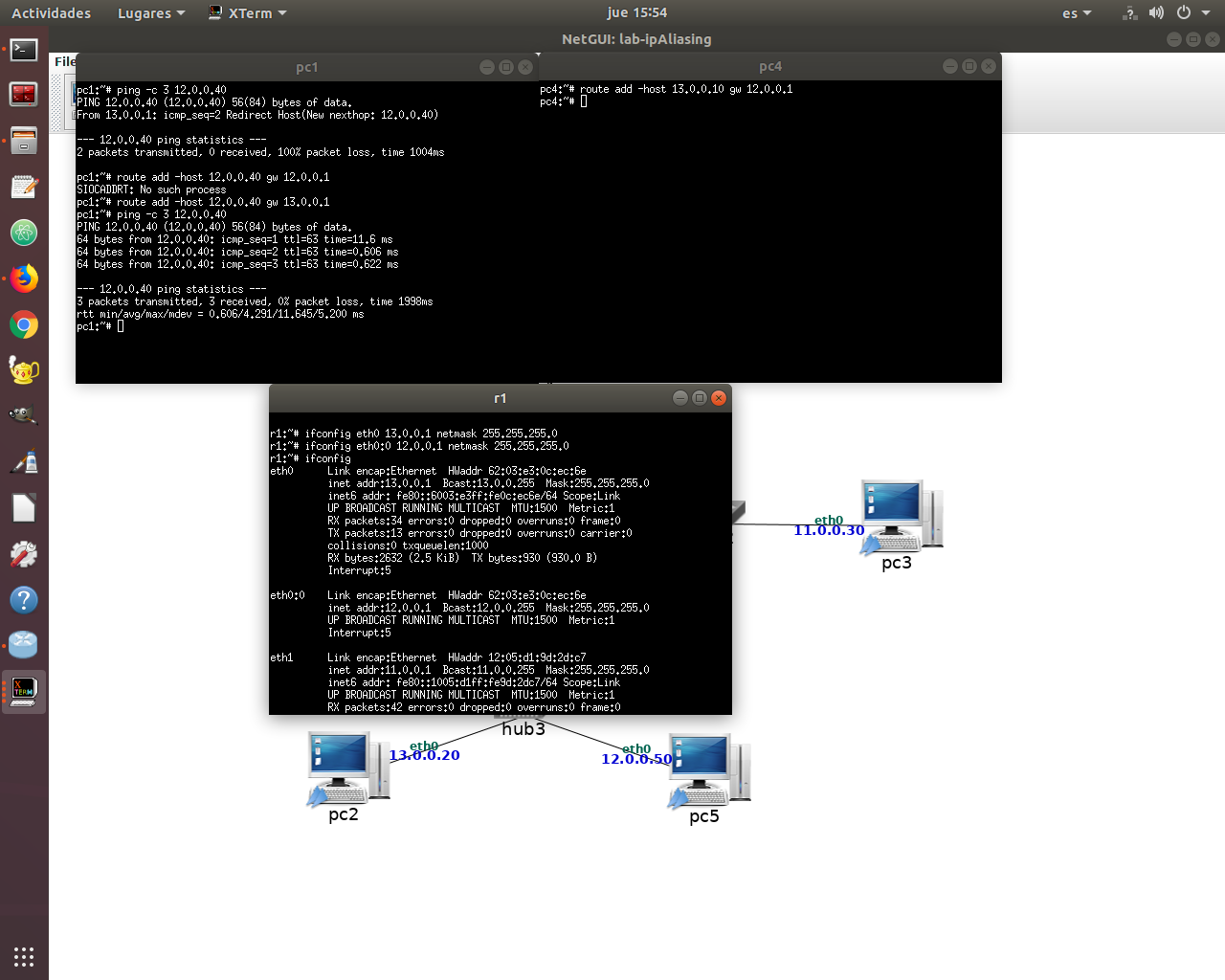


3. Con la configuración que has realizado previamente ¿pueden comunicarse pc1 y pc5?

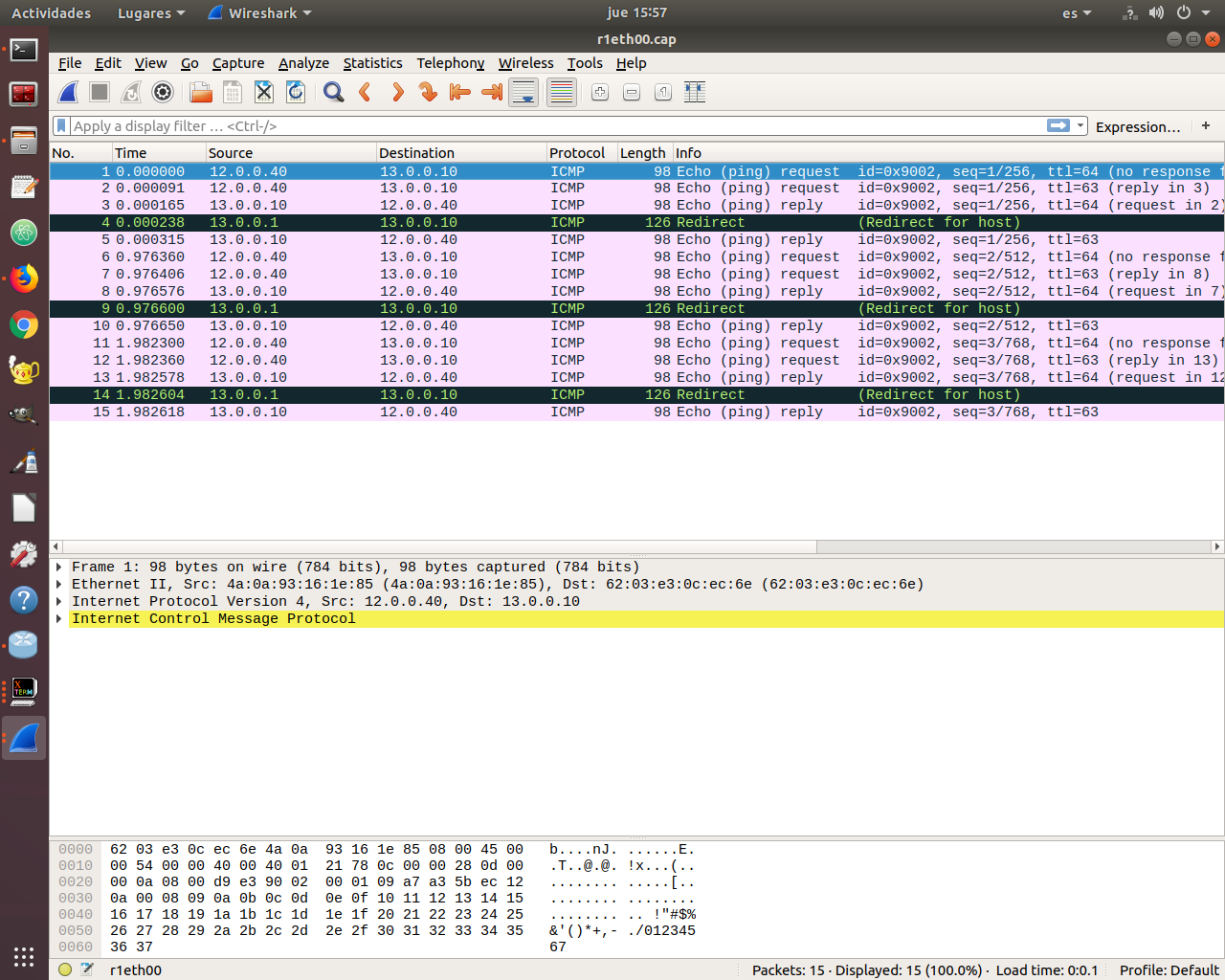
No se pueden comunicar porque cuando he realizado el apartado anterior además de añadir una nueva IP también he añadido dos rutas por defecto que afectan también a esta comunicación entre pc1 y pc5.

4. Utiliza de nuevo IP aliasing para que pc4 pueda hacer ping a pc1, ten en cuenta que desde r1 se deberá poder alcanzar también a pc5.

En la siguiente captura se observan los pasos que he realizado, son similares a los del apartado 1.



5. Realiza una captura en r1(eth0) (sin necesidad de guardarlo en un fichero) para ver qué paquetes se intercambian cuando pc4 hace ping a pc1.



**5.VLANs**

1. Explica que máquinas se pueden comunicar entre ellas.

Compruébalo realizando ping.

Todas se pueden comunicar entre ellas porque los switches todavía no tienen ninguna VLAN y por tanto mandan las solicitudes a todos y como son para ellos todos se conectan.

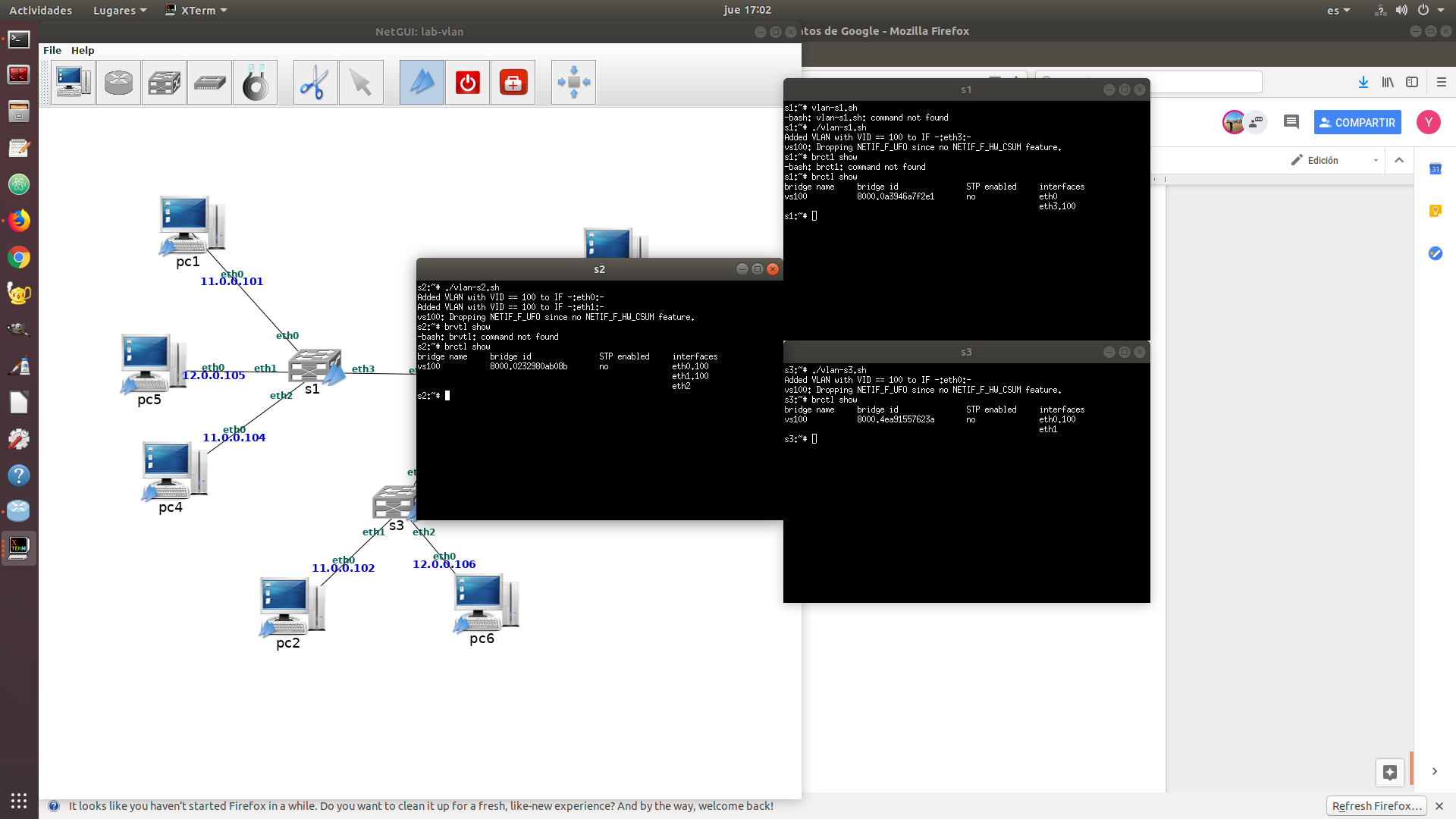
2. Suponiendo que la caché de ARP de pc1 está vacía, indica donde se puede capturar un

solicitud de ARP que la máquina pc1 envía preguntando por la dirección Ethernet de la máquina pc2. Compruebalo realizando capturas. Para este caso puedes utilizar tcpdump -i <interfaz> -s 0 sin necesidad de guardar la captura en un chero, de esta forma veras el resultado mostrado en pantalla. (Comprueba antes que en la cache de ARP de pc1 no se encuentra la direccion Ethernet de pc2; si estuviera, borrala).

Se puede capturar en todas las máquinas porque los switches envían la solicitud a todas las máquinas.

**5.1.Configuración de VLAN100.**

Podemos ver en esta captura los cambios que he realizado en cada uno de los switches para que tengan VLAN100 que ya nos la daban solo tenia que utilizar el comando ./vlan-sX.sh



3. Indica que maquinas se pueden comunicar entre ellas.

Solo se pueden conectar pc1 y pc2 puesto que están en la misma VLAN.

4. Suponiendo que la caché de ARP de pc1 esta vacía, indica donde se puede capturar un solicitud de ARP que la máquina pc1 envía preguntando por la dirección Ethernet de la máquina pc2.

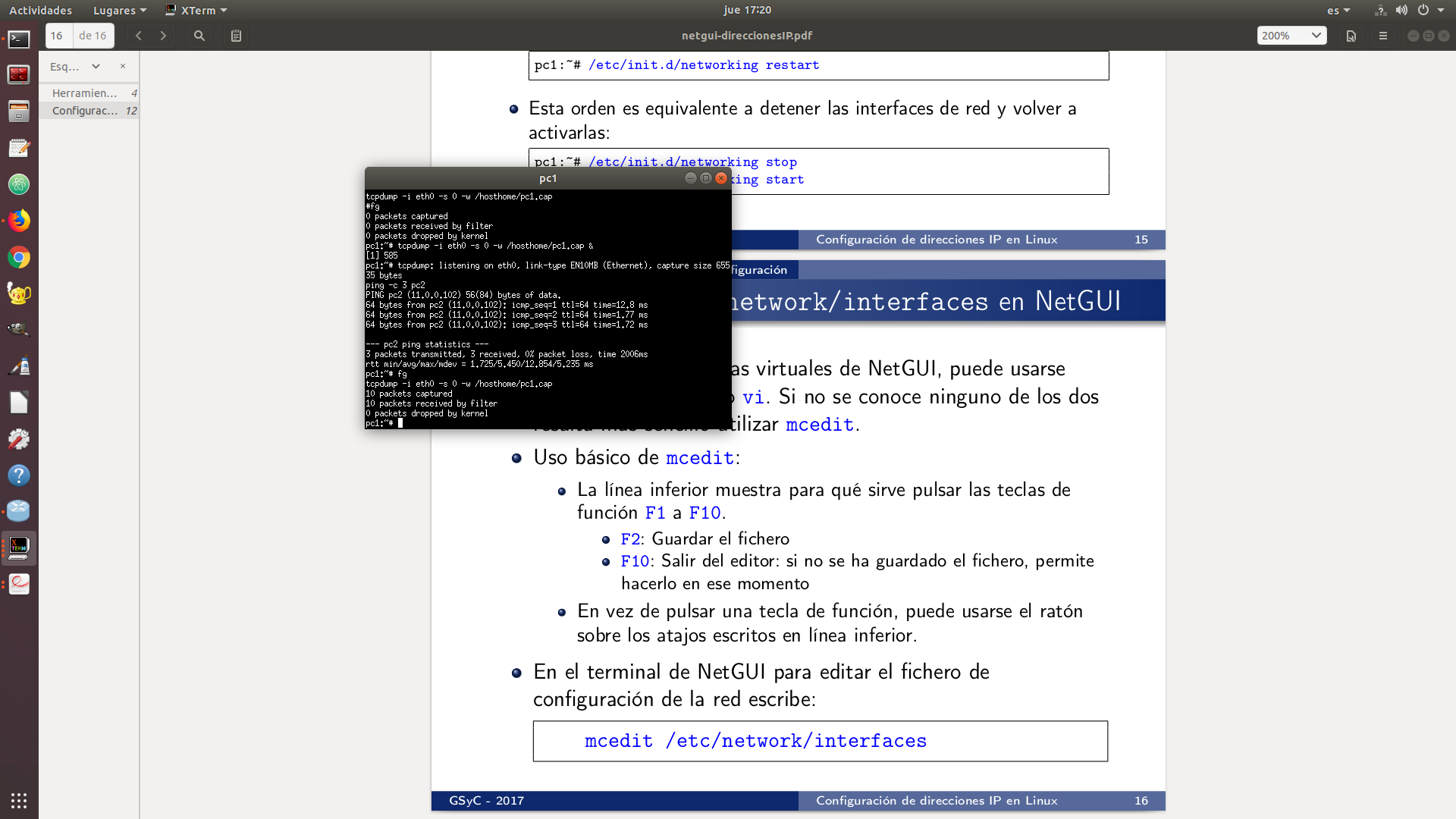
Podemos capturar una solicitud de ARP en s1, s2 ,s3 o r1 que también están en la VLAN100.

5. Indica que ocurre cuando se hace un ping desde pc1 a pc2, teniendo en cuenta que ambas máquinas se encuentran en la misma subred.

El ping funciona porque además de estar en la misma subred están en la misma VLAN porque sino no funcionaria aunque estuvieran en la misma subred.

6. Asegurate de que la caché de ARP de pc1 esta vacía, borrala si es necesario. Arranca tcpdump en las siguientes interfaces: pc1(eth0), s1(eth3), s2(eth2), s3(eth0) y pc2(eth0), guardando esta vez el tráfico capturado en un fichero. Realiza un ping desde pc1 a pc2.

Adjunto captura para recordar como hacer varias cosas en pc1, es decir, en segundo plano como por ejemplo en pc1 que quiero hacer una captura y a la vez un ping.



8. Analiza las 5 capturas, indica en que capturas se observa la etiqueta de VLAN en el traco y que identificador de VLAN contiene.

a) ¿Qué switch introduce dicha etiqueta?

b) ¿Qué switch elimina dicha etiqueta?

No necesita etiqueta porque solo tenemos configurada una VLAN.

c) ¿pc1 y pc2 tienen alguna forma de saber si están usando una VLAN para comunicarse?

No porque VLAN no afecta a las máquinas finales.

d) ¿Por que solo se ve una trama Ethernet en la captura realizada en la interfaz s2(eth2)?

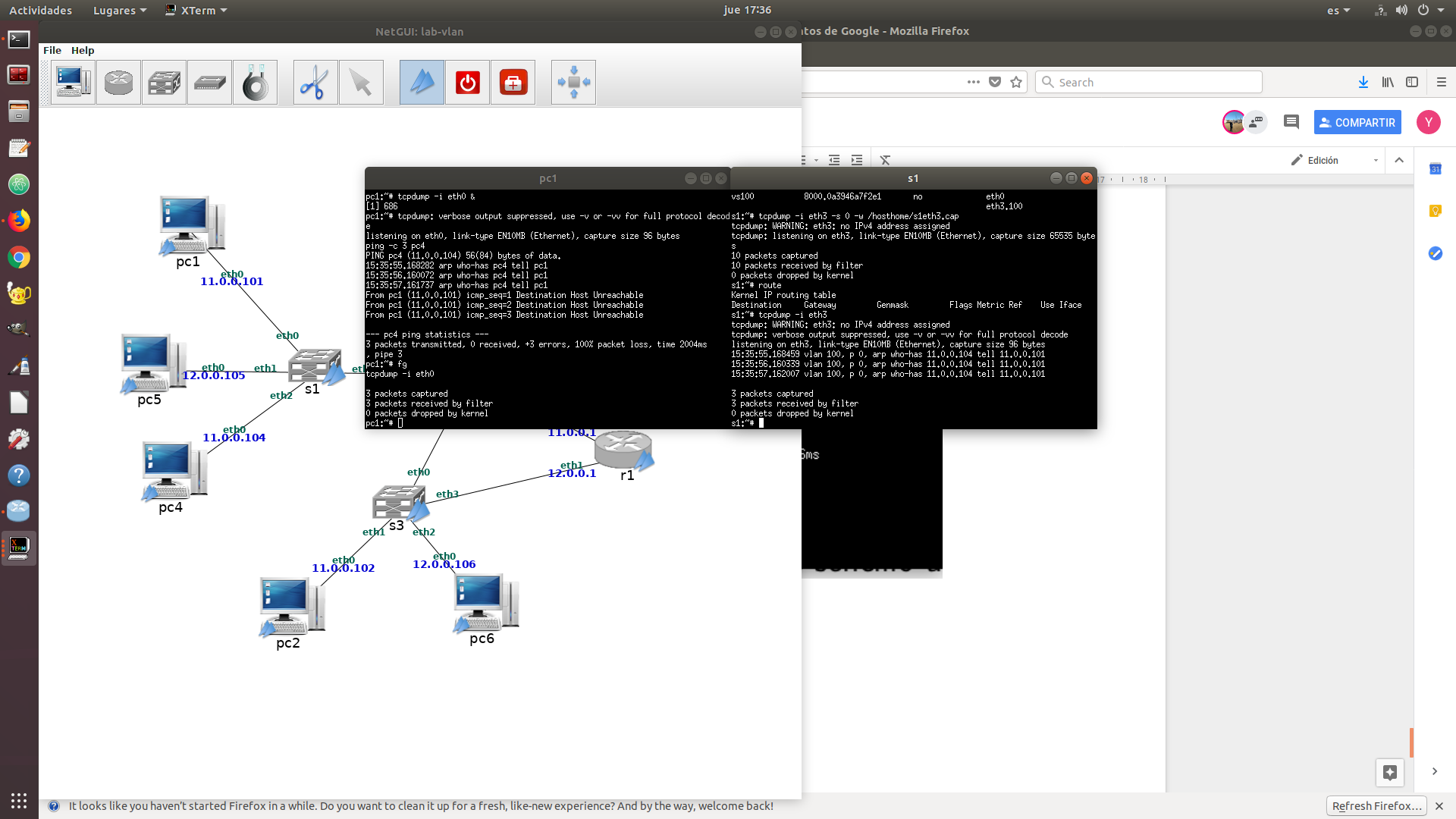
e) ¿En qué se diferencia la solicitud de ARP que se captura en pc1(eth0) de la misma solicitud que se captura en s1(eth3)?

f ) ¿En qué se diferencia el mensaje ICMP Echo request que se captura en pc1(eth0) del mismo mensaje que se captura en s1(eth3)?

PREGUNTAR DUDAS D) E) F)

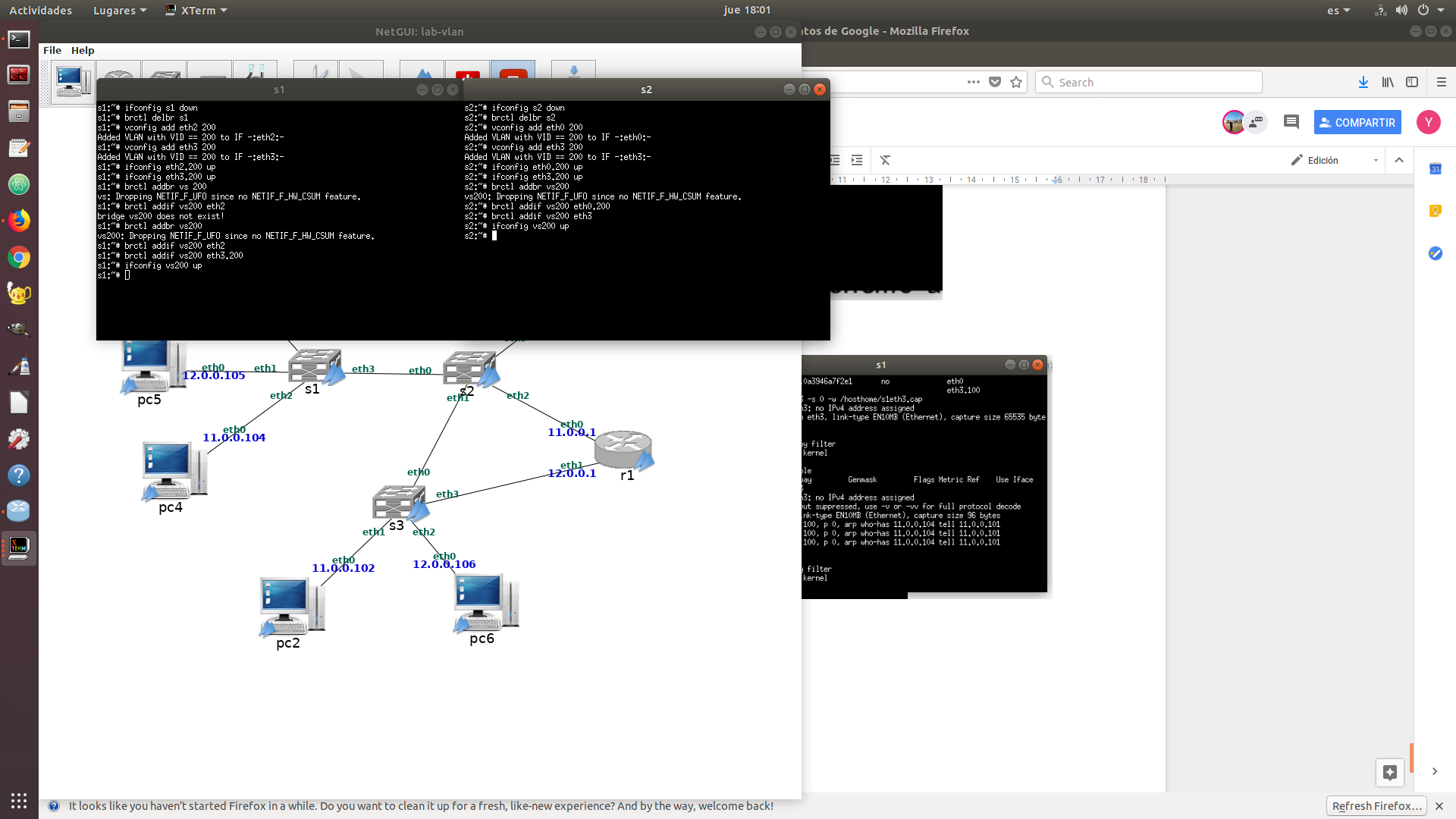
9. Indica que ocurre cuando se hace un ping desde pc1 a pc4, teniendo en cuenta que ambas máquinas se encuentran en la misma subred y conectadas al mismo switch.

No funciona porque s1 funciona con VLAN y como pc1 y pc4 no están en la misma por eso no funciona el ping.



**5.2. Configuración de VLAN200.**

En la siguiente captura observamos como editar para que funcione VLAN200 porque esta vez no nos la dan hecha.



1. Indica que máquinas se pueden comunicar entre ellas con la configuración de VLAN200.

Solo las que están dentro de esa VLAN200, es decir, pc5, pc6 y también con el r1.

2. Asegurate de que la caché de ARP de pc4 esta vaca, borrala si es necesario. Arranca tcpdump en las siguientes interfaces: pc4(eth0), s1(eth3), pc3(eth0)y pc1(eth0) guardando esta vez el tráfico capturado en un fichero. Realiza un ping desde pc4 a pc3.

El ping funcionará ya que comparten la misma VLAN200.

3. Interrumpe las capturas y observa las direcciones Ethernet aprendidas por los switches s1, s2 y s3.

Como tenemos VLAN 200 el tráfico de paquetes está controlado y tanto los paquetes ARP como ICMP van por la misma ruta: pc4 a s1, s1 a s2 y s2 a pc3.

4. Analiza las 4 capturas, indica en que capturas se observa la etiqueta de VLAN en el tráfico y que identificador de VLAN contiene.

Solo lo vemos en los switches además en s1 se observa VLAN pero luego s2 eliminaría esta etiqueta al salir por eth3.

5. Indica que ocurre ahora cuando se hace un ping desde pc1 a pc4, teniendo en cuenta que ambas máquinas se encuentran en la misma subred, conectadas al mismo switch y las interfaces de dicho switch tienen configurada una VLAN.

No llega porque pc1 está asilado por VLAN 100 y cuando pasa por s1 el paquete no pasaría por pc4. Por otro lado, pc4 también se aísla en su VLAN 200. Por tanto, la comunicación entre ambos no es posible.

**5.3.Configuración de VLAN300.**

1. Realiza un ping desde pc6 a pc1. ¿Qué crees que está ocurriendo?

Mediante VLAN 300 aislamos la comunicación entre pc5, pc6 y r1. Por tanto, pc5 y pc6 tienen comunicación entre sí pero también tendrán comunicación con pc1 y pc2 por medio de r1 al que llegan VLAN100 y VLAN300.

2. Realiza un ping desde pc6 a pc5. ¿Qué crees que está ocurriendo?

Estos dos pcs están conectados a la misma vlan pero como pc6 tiene distinta subred debe ir primero a r1, si no tuviéramos este router la conexión sería imposible aunque esten en la misma VLAN.

3. Suponiendo que la caché de ARP de pc6 está vacía, al realizar un ping de pc6 a pc1, ¿que solicitudes de ARP hay y en qué interfaces aparecen? ¿Cuáles de ellas tendrán etiqueta VLAN e indica que etiqueta?

Las solicitudes ARP al hacer el ping aparecerán en s3 (todos los ARP en eth3 y el primero en eth1), en r1 (todos), en s2 (todos en eth2 y el primero en eth1), en s1 (todos en

eth3), en pc2 (solo el primero), y por supuesto en pc6 y pc1.

4. Arranca tcpdump en las siguientes interfaces: pc6(eth0), s3(eth1), r1(eth0), s2(eth0) y pc1(eth0), guardando esta vez el tráfico capturado en un chero. Realiza un ping desde pc6 a pc1.Supón en que interfaces aparecerá el tráfico etiquetado y su identificador de VLAN. Comprueba tus suposiciones analizando las capturas, indica en que capturas se observa la etiqueta de VLAN en el tráfico y que identificador de VLAN contiene.

VLAN aparece en s2(eth0) con VLAN100. Ya que es la única interfaz “trunk”. s1(eth3) también recibiría VLAN.