ELENA MARÍA DEL RÍO GALERA

Octubre de 2020

**PRÁCTICA 1**

Para la realización de la práctica, descargue mis escenarios, y tengo mis propias direcciones. La X en mi caso es 15.

**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.

Solo capturará paquetes pc2, porque el switch está apagado y no es posible la conexión con pc5 y pc3. Pc2 y pc1 están en la misma interfaz conectados a la misma interfaz, por lo que no necesitan del switch para comunicarse.

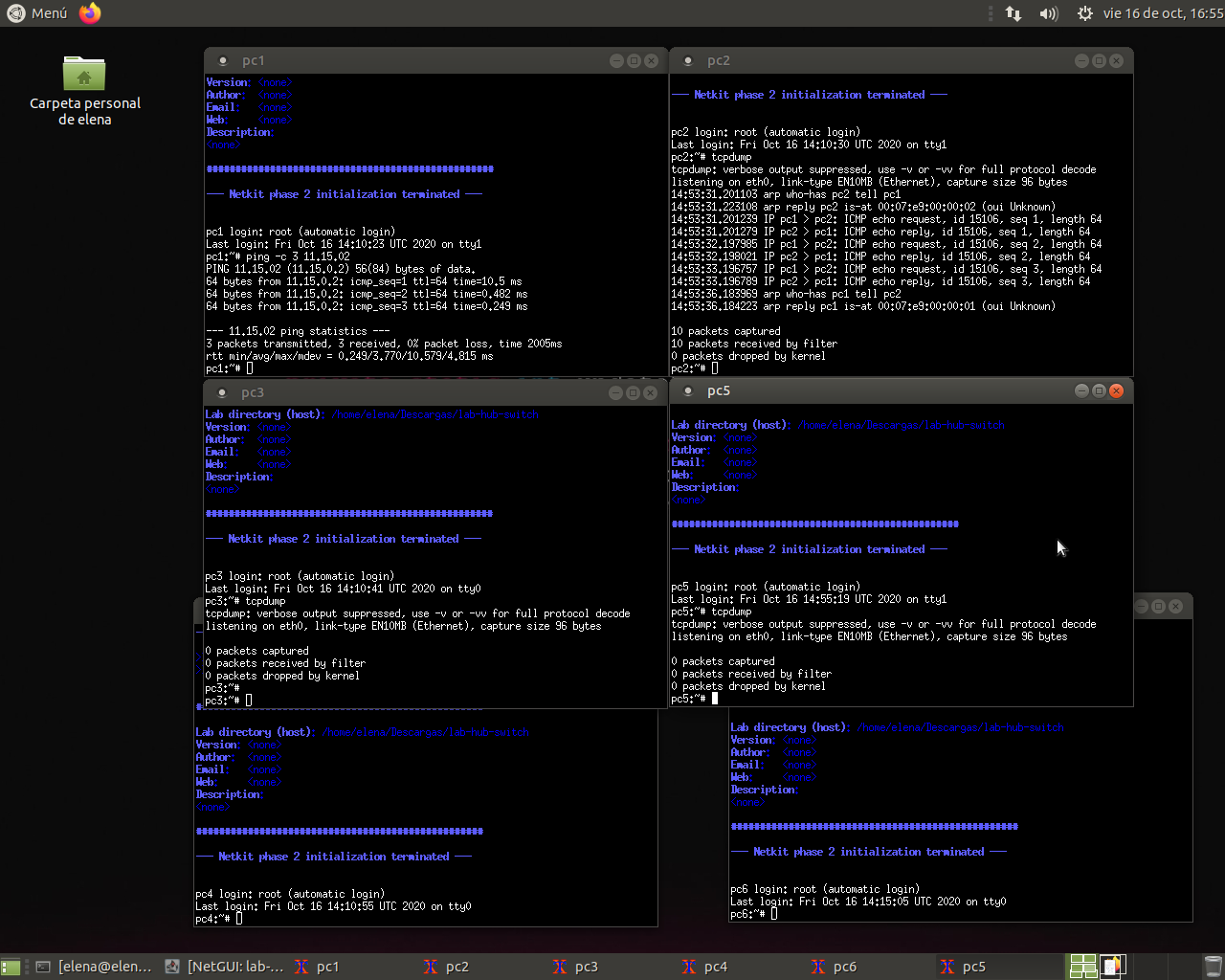
2. Lanza tcpdump en pc2, pc3 en pc5. A continuación ejecuta la siguiente orden en pc1 para hacer un ping a pc2: pc1:~# ping -c 3 11.0.0.2

(-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.

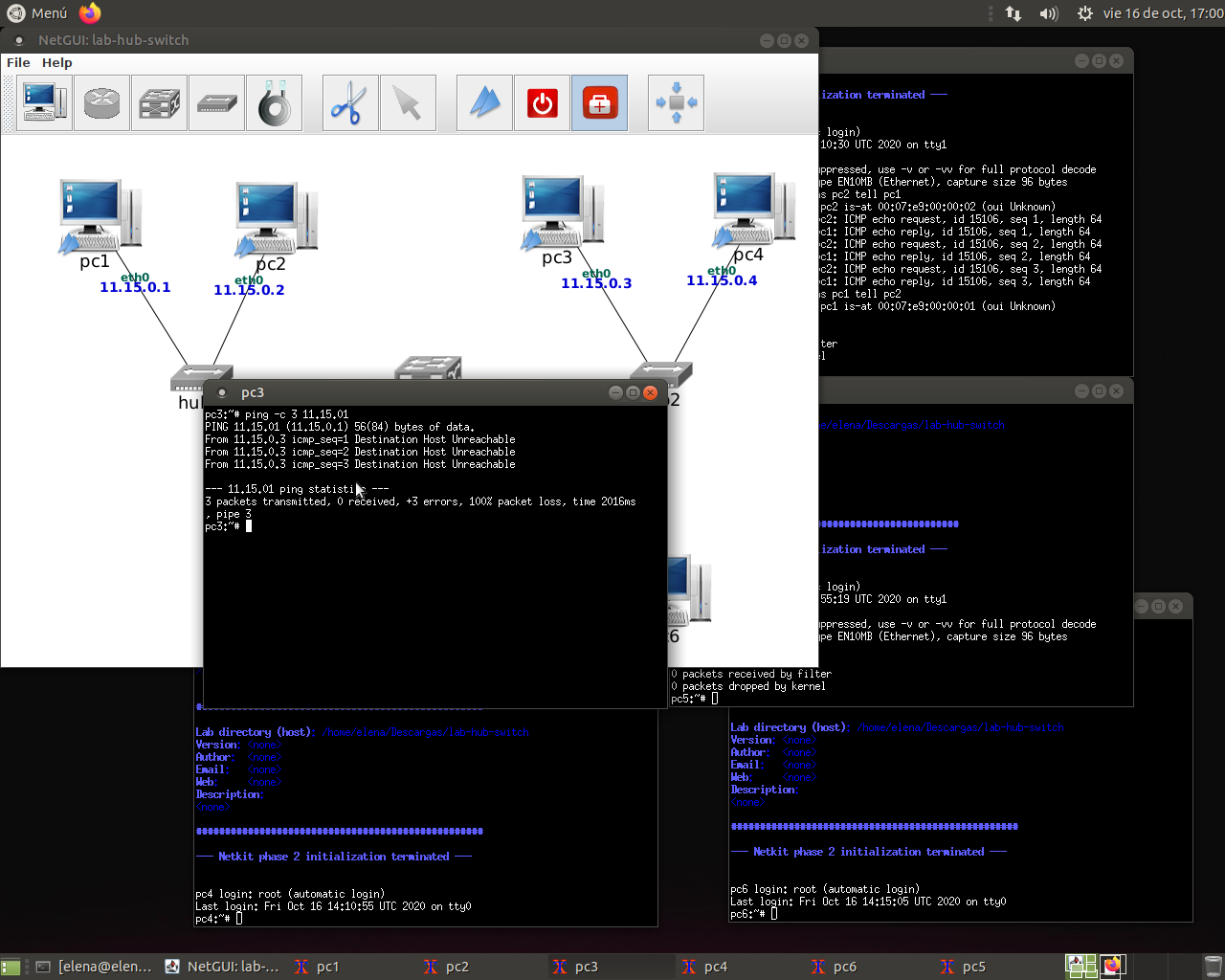
Copia en la memoria lo que muestra tcpdump en cada una de las máquinas.

Observamos que solo captura pc2.



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

Compruebo intentando hacer ping de pc3 a pc1.



**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 pc5 no hacen nada más.

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.

Ha ocurrido justo lo que pensaba

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?

Se manda el mensaje de pregunta arp a todos, diciendo, Who has 11.15.0.2, pero el mensaje de respuesta, solo lo manda, el que tiene esa dirección, osea pc2, los demás no tienen que recibir respuesta, porque no era para ellos la pregunta.

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

De nuevo por la misma razón. EL ping lo está haciendo pc1 a pc2. Los demás no tienen que recibir nada más que el arp de pregunta, y como no es para ellos, ni contestan ni hacen nada más.

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

La conversación no va con ellos.

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

Pc1 → 00:07:e9:00:00:01

Pc2 → 00:07:e9:00:00:02

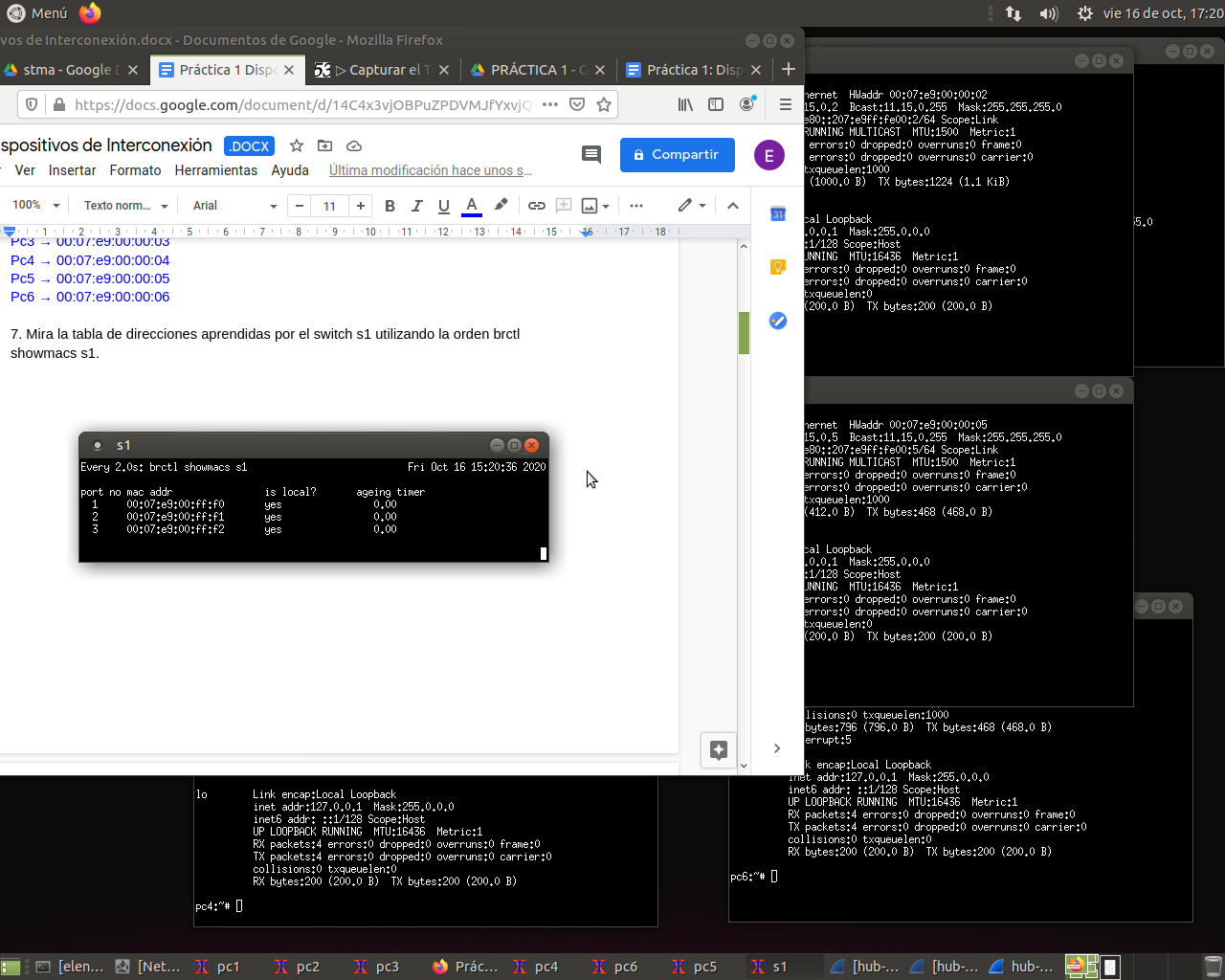
Pc3 → 00:07:e9:00:00:03

Pc4 → 00:07:e9:00:00:04

Pc5 → 00:07:e9:00:00:05

Pc6 → 00:07:e9:00:00:06

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

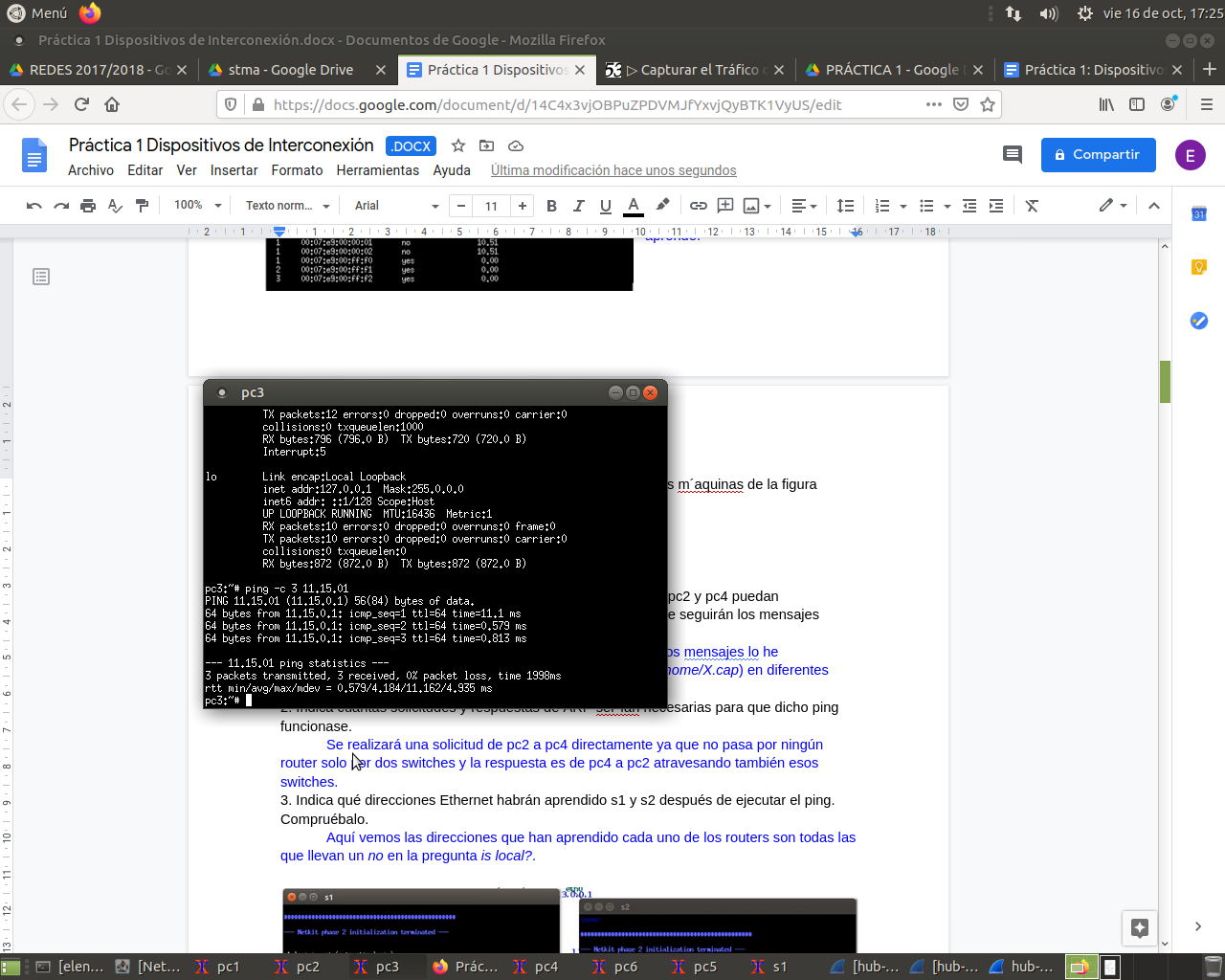
* Antes del ping pc1 a pc2
* Después del ping pc1 a pc2



Aparecen las direcciones de pc1 y pc2 porque al hacer el ping las aprende.

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

Realizamos de nuevo el ping pc3 a pc1.



**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 seguirán los mensajes, ya que la conectividad a través dle router no va a ser posible pos las direcciones ip. Asi que se podrán conecntar a través de los switches, que mandaran mensajes arp preguntando pot pc4.

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

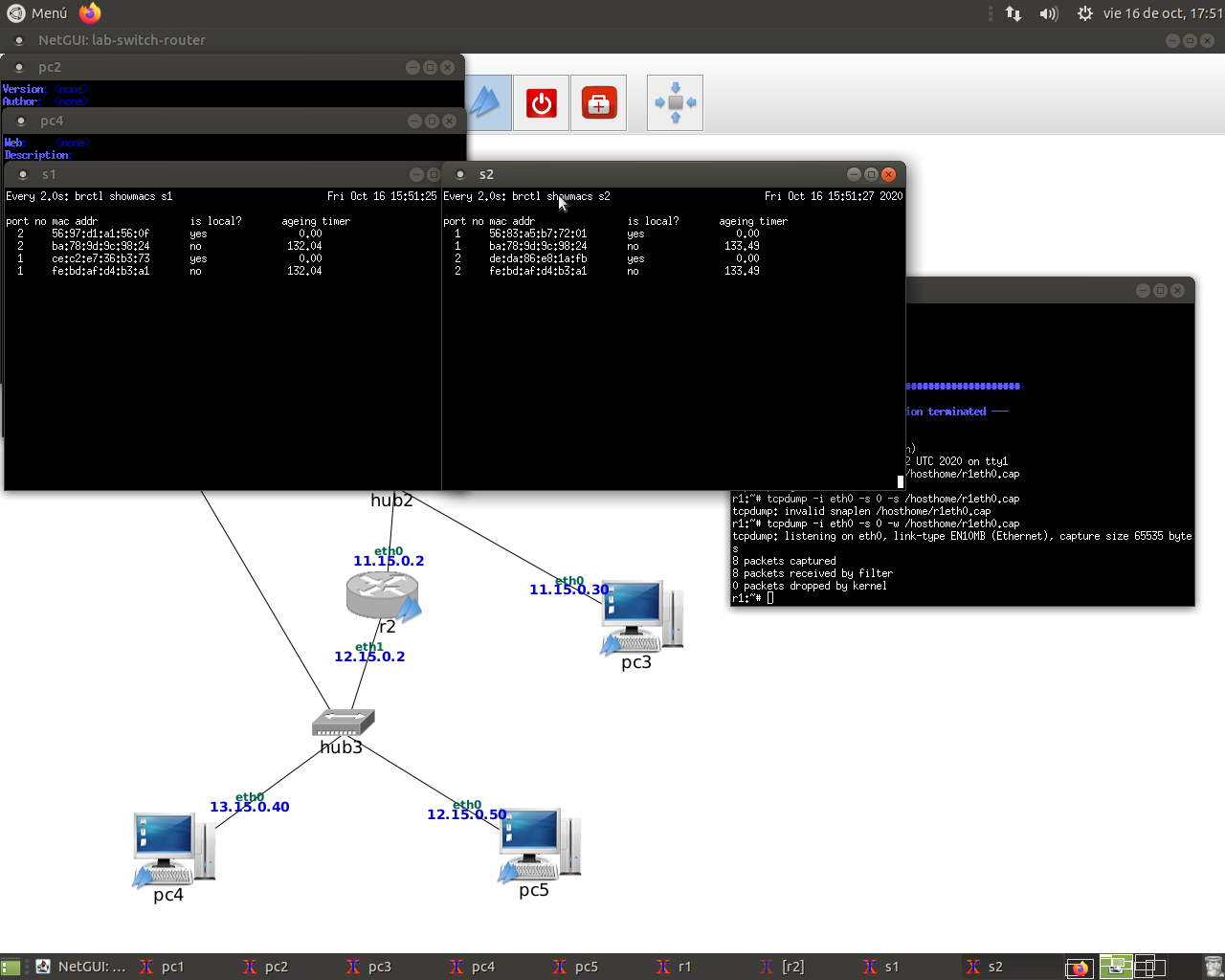
S1 y s2, generan solicitudes arp, para todos, preguntando quien tiene 13.15.0.20

y generan respuesta de arp solo pc4. Y luego pc4 genera solicitudes de arp para todo preguntando quien tiene 13.15.0.40 y responde con respuesta arp desde la interfaz de pc2 diciendo donde está para que se la aprendan y puedan enviar respuesta.

3. Para ver todo el tráfico generado deberás lanzar un tcpdump por cada hub de la figura. Justifica la respuesta.

4.Lanza Tcpdump En Las Máquinas Pc1(switch-router-01.cap),pc3(switch-router-02.cap) ypc5(switch-router-03.cap) para ayudarte a comprobar tus suposiciones

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

Direcciones aprendidas de s1 y s2, son las no locales. Que son las correspondientes a pc2 y pc4.

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

Los switch envían la solicitud arp a todos, aunque estos tres pc, no contestan porque no preguntan por ellos. Pero los mensajes icmp echo request son distintos, y sí los habrás recibido porque comparten interfaz.

**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?

Seguirá el camino pc1→r1 → pc3, no hace falta los switches para conectarse, a través del router se pueden conectar sin problemas.

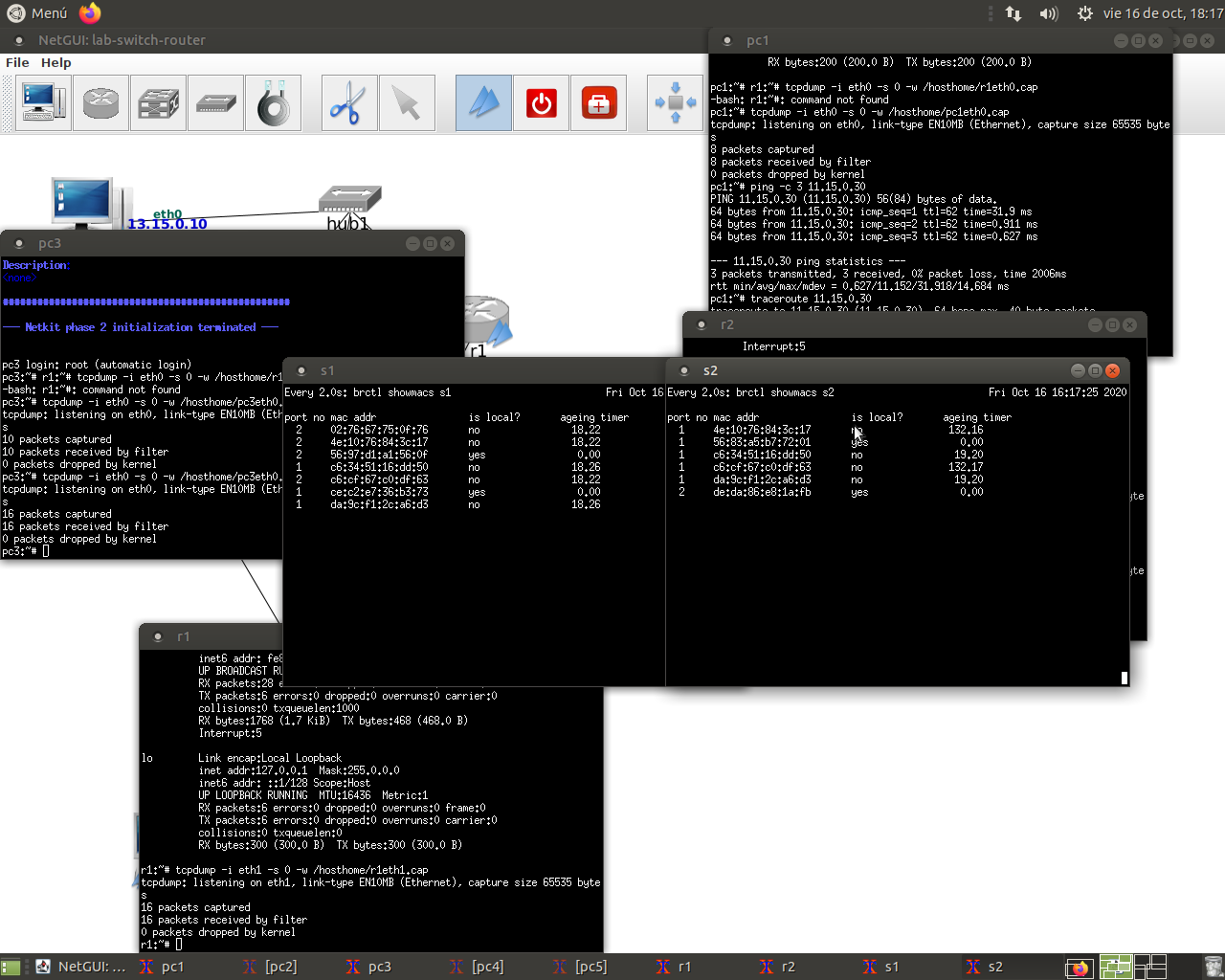
2. Indica cuantas solicitudes y respuestas de ARP serán necesarias para que dicho ping funcionase.

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. Lanza tcpdump en las maquinas r1(eth0)(switch-router-04.cap),pc2(switch-router-05.cap) y pc5(switch-router-06.cap) para ayudarte a comprobar tus suposiciones.

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

El camino de ida, es pc3-r1-pc1 pero el camino de vuelta es pc1-r1-r2-pc3. Luego las direcciones aprendidas de s1, son las de r1,r2 pc1 y pc3 y las de s2, r1, pc1 y pc3.



5. ¿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, esto es porque pc5 tiene una dirección ip distinta.

**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?

Sigue el camino pc2 →s1 → r1 → r2 → pc5 porque los routers no son suficientes para establecer conexión ya que no tienen información suficiente en sus tablas de encaminamiento para poder establecer la conexión.

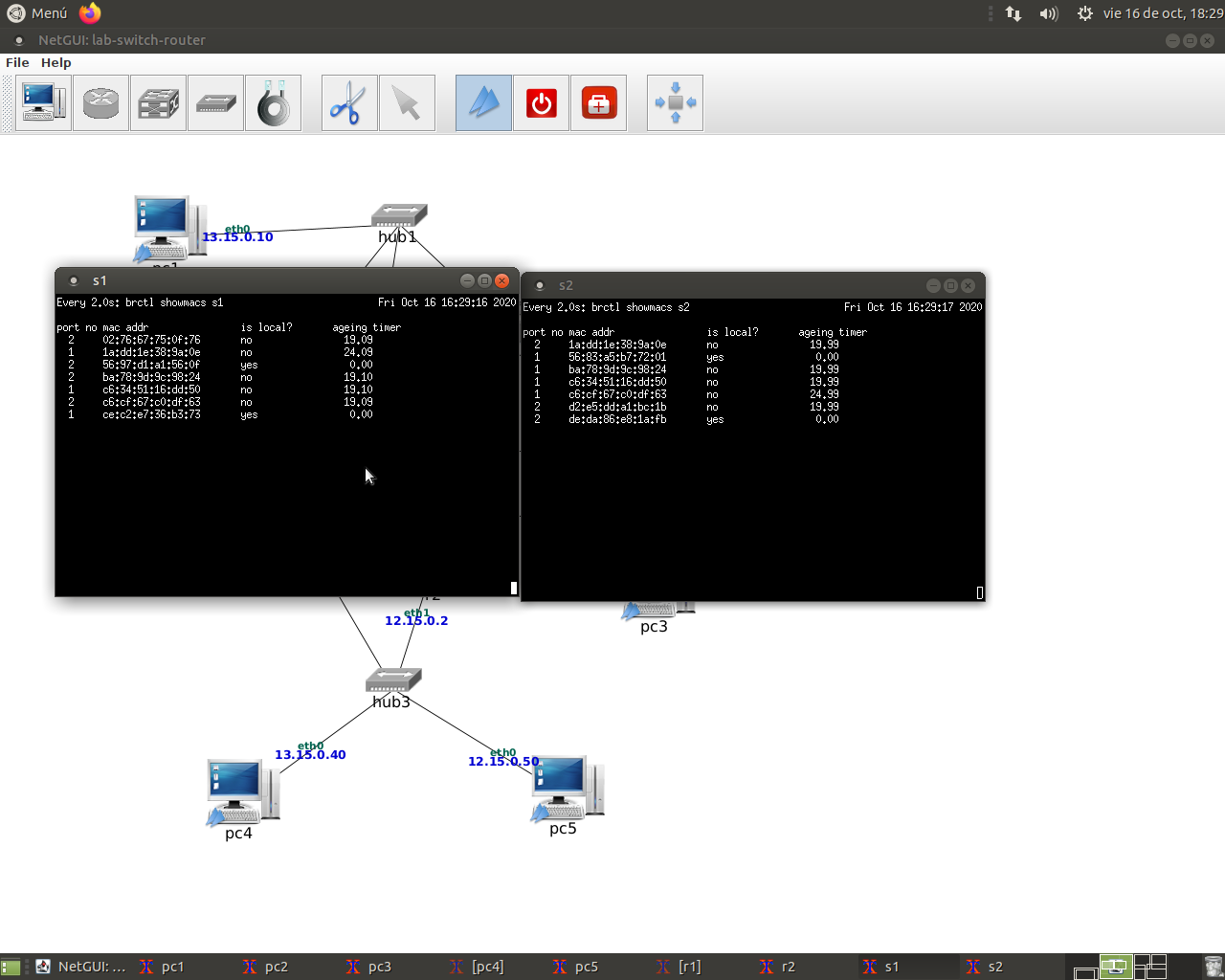
2. Indica cuántas solicitudes y respuestas de ARP serán necesarias para que dicho ping funcionase.

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. Lanza tcpdump en las maquinas pc1(switch-router-07.cap),pc3(switch-router-08.cap) y pc4(switch-router-09.cap) para ayudarte a comprobar tus suposiciones.

4. 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.



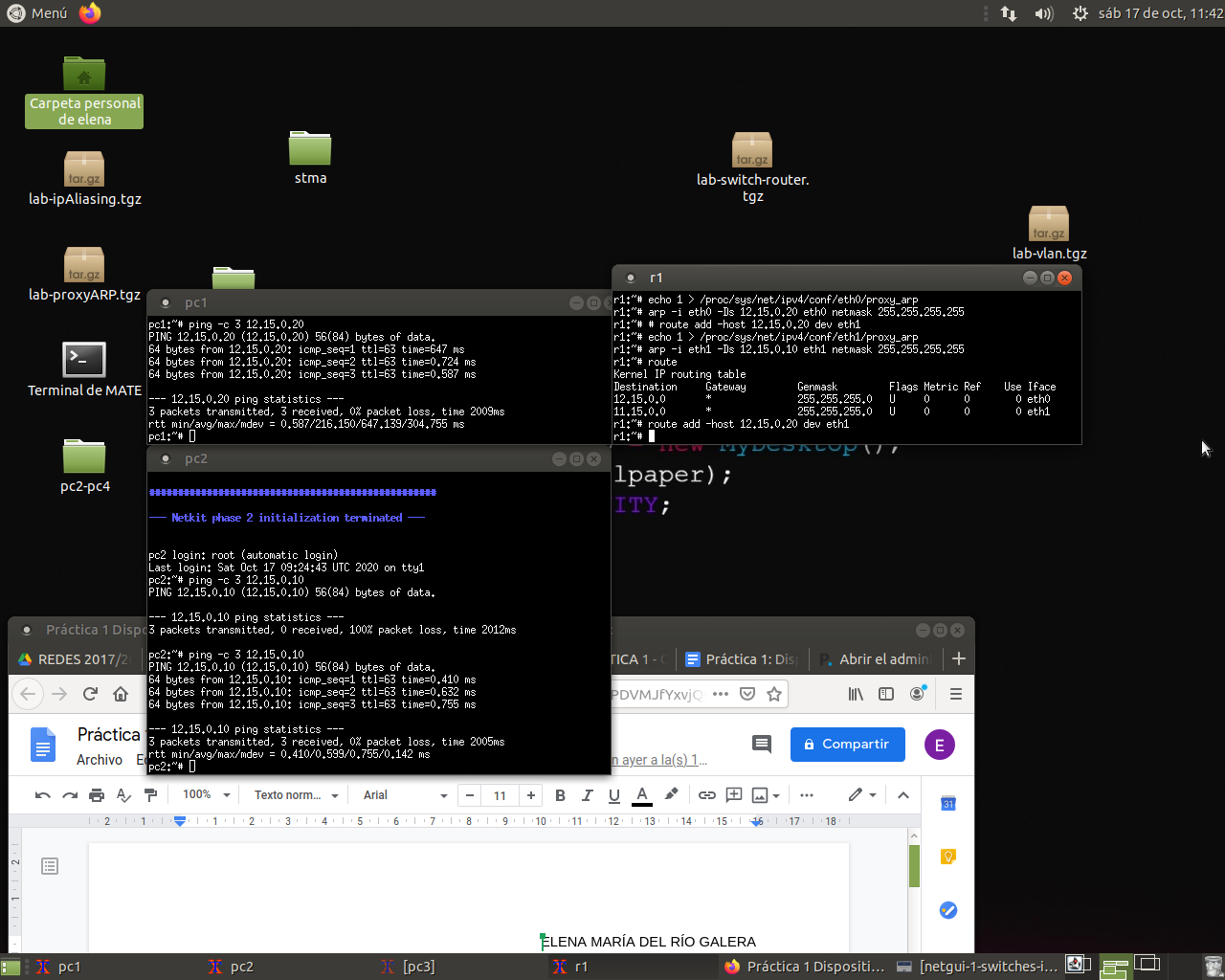
5. ¿Crees que habrá llegado alguno de los mensajes ICMP echo request a pc1, pc3 o pc4?

Sí. Porque están conectados por el hub en las mismas subredes.

**3.Proxy ARP**

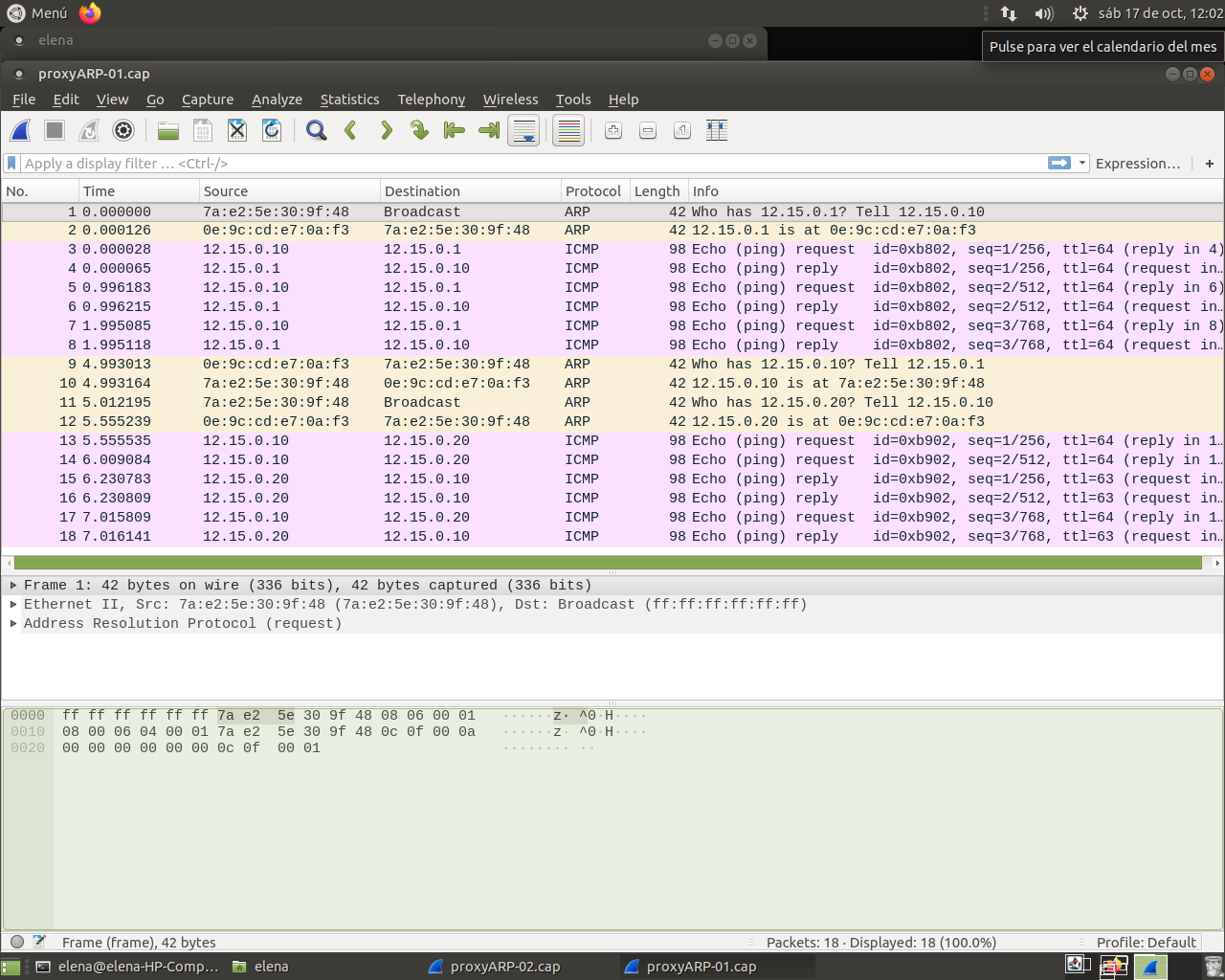
1. Activa proxy ARP en la configuración del router r1 para que las máquinas pc1 y pc2 tengan conectividad IP entre ellas en ambos sentidos. Explica qué modificaciones han sido necesarias y por qué.

He realizdo los cambios en r1, tuve un problema al escribir el comando royte, y no me funcionaba el ping, por eso consulto la tabla route y lo vuelvo a ejecutar, después de eso sin problemas funciona el ping en los dos sentidos. pc1-pc2 y pc2-pc1

****

2. Con las caches de ARP vacas, realiza una captura en la interfaz r1(eth0) (proxyARP-01.cap) y en pc3 (proxyARP-02.cap) y ejecuta un ping desde pc1 a la direccion IP de r1(eth0), enviando solo 3 paquetes, y despues un ping desde pc1 a pc2, enviando solo 3 paquetes. Interrumpe la captura y explicalas solicitudes de ARP que ves en el traco capturado en ambos cheros.

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 eth0( la dirección ethernet acabada en f3).

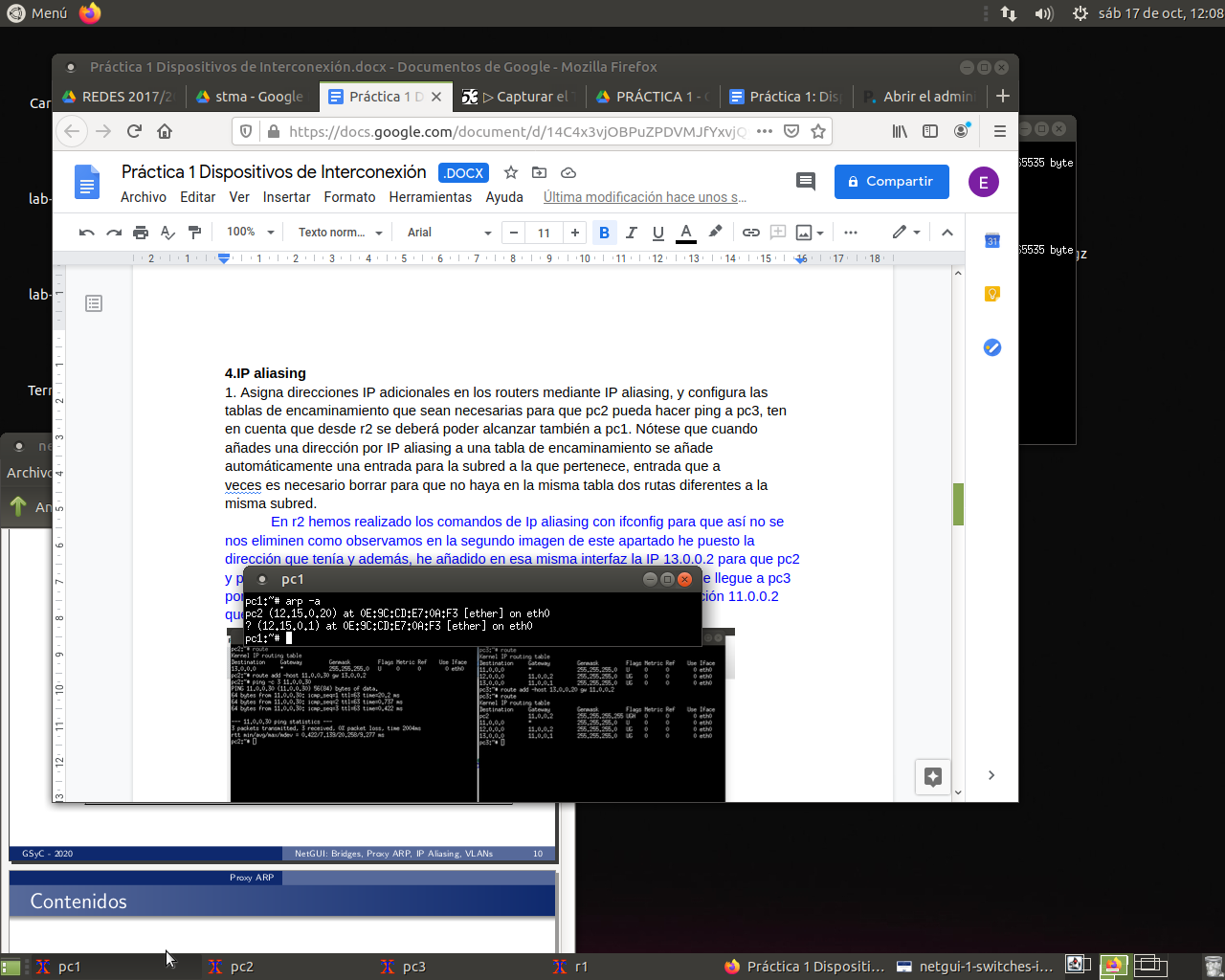
****

3. A partir de la captura y de las direcciones IP de r1, ¿cómo puedes saber que r1 esta realizando proxy ARP?

Utiliza ARP proxy porque para distintas solicitudes el router contesta con la misma dirección. Es decir, hacemos un ping, se generan, solicitudes de arp distintas preguntando primero por r1 eth0 y después por pc2, y la respuesta es la misma, que están en el mismo sitio r1(dirección ethernet acabada en f3). Nos etá *mintiendo.*

4. Si se ha borrado la cache de ARP de pc1 vuelve a ejecutar los 2 ping anteriores y consulta la cache de ARP de pc1, indica que observas, explicando a que maquina/s pertenece la informacion almacenada.

Vemos en la captura, que para pc2 con dirección 12.15.0.20 tiene asignada la dirección ethernet de r1 eth0, luego una prueba más de que se está utilizando proxy arp. Ya que también tiene la misma dirección de respuesta cuando se refiere a 12.15.0.1.

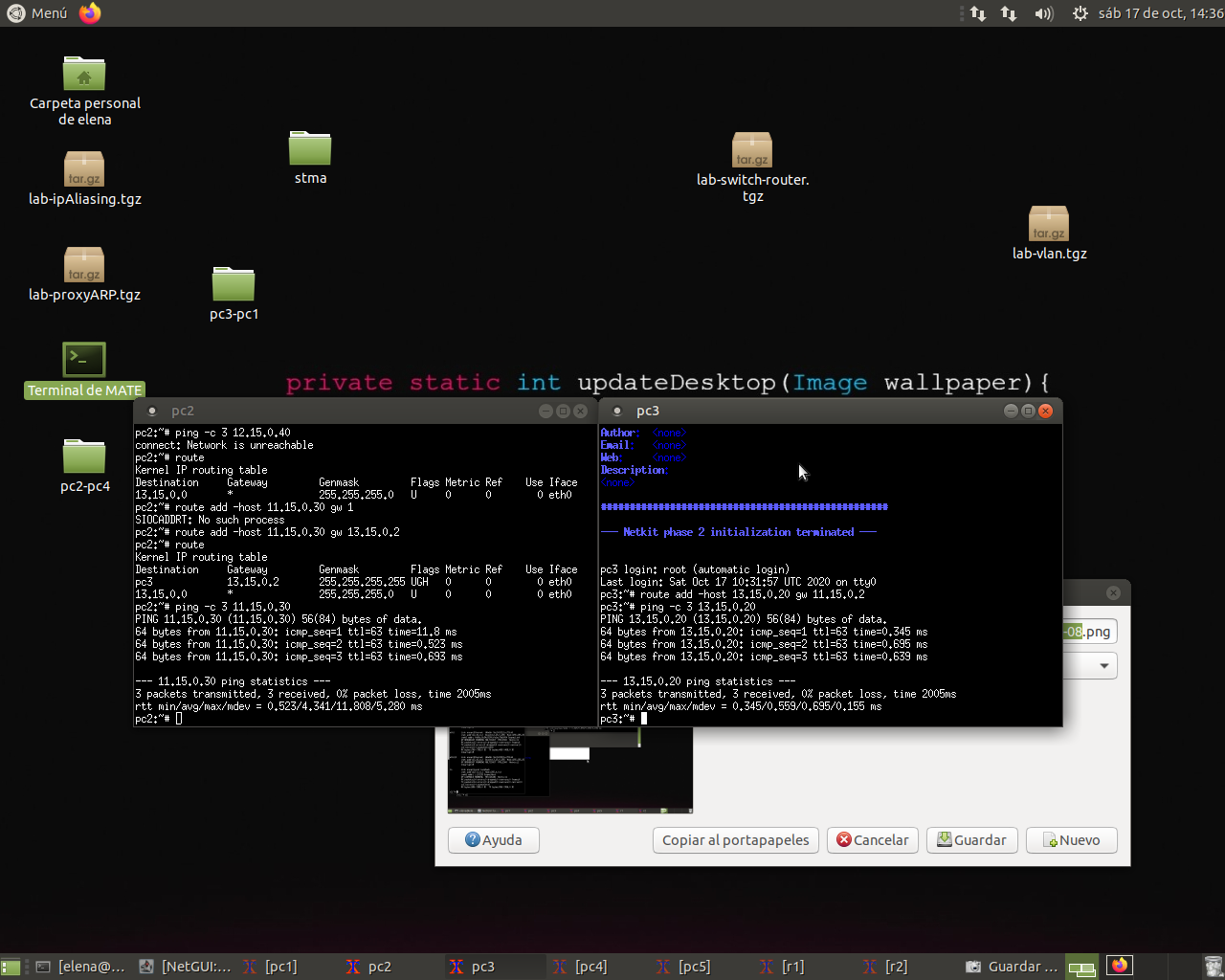
****

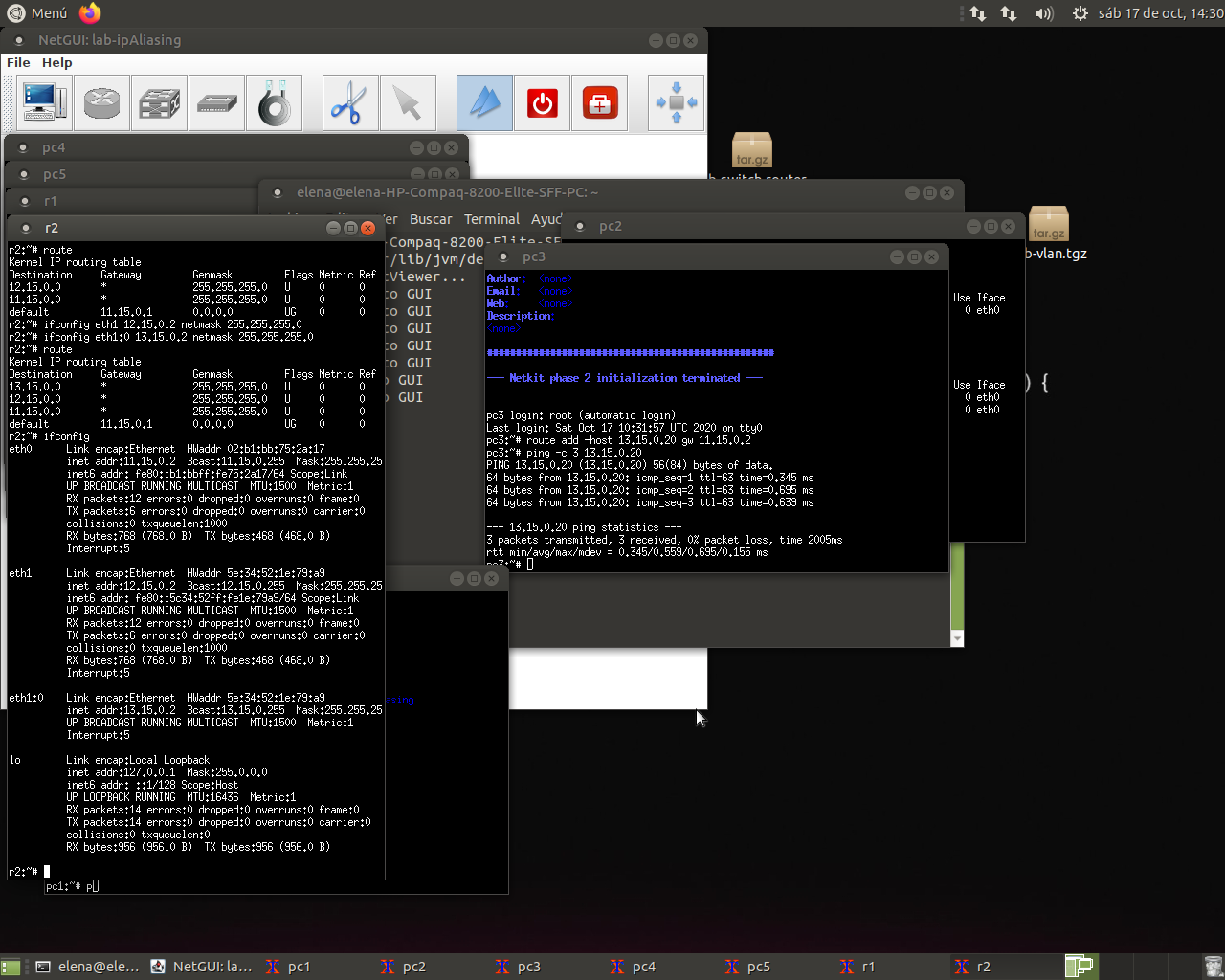
**4.IP aliasing**

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.

He configurado ip aliasing con if config en r2. he añadido la IP 13.15.0.2 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 r2.

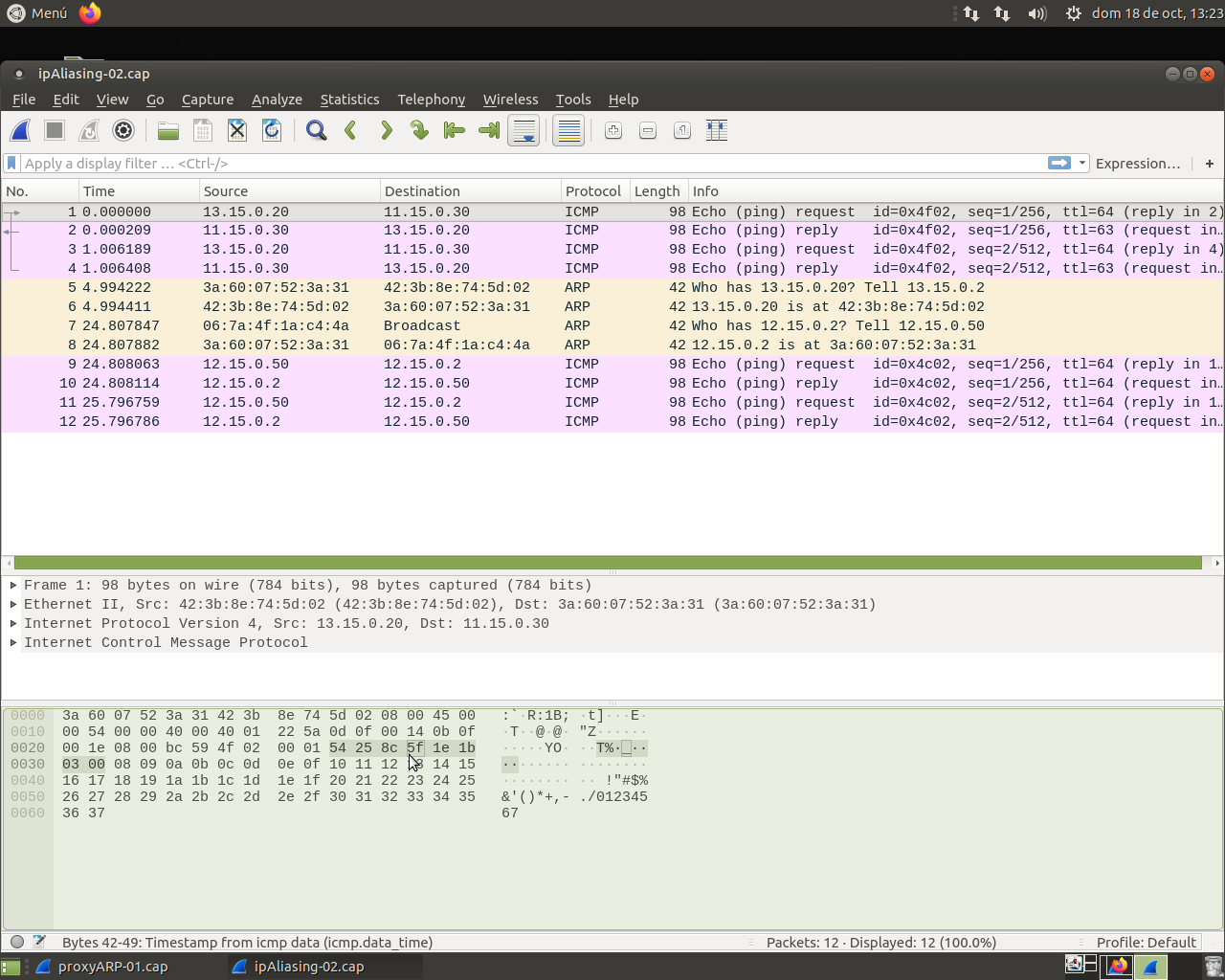




2. Realiza una captura en r2(eth1) (ipAliasing-01.cap) y ejecuta un ping desde pc2 a pc3 enviando 3 paquetes y despues ejecuta un ping desde pc5 a la direccion IP de r2(eth1). Interrumpe la captura y explica las solicitudes de ARP que observas.

Vemos (5 y 6), solicutud ARP preguntando r2 eth1 por pc2. Responde pc2.

Vemos (7 y 8) solicitud arp preguntando pc5 por la eth1 de r2. Responde r2.



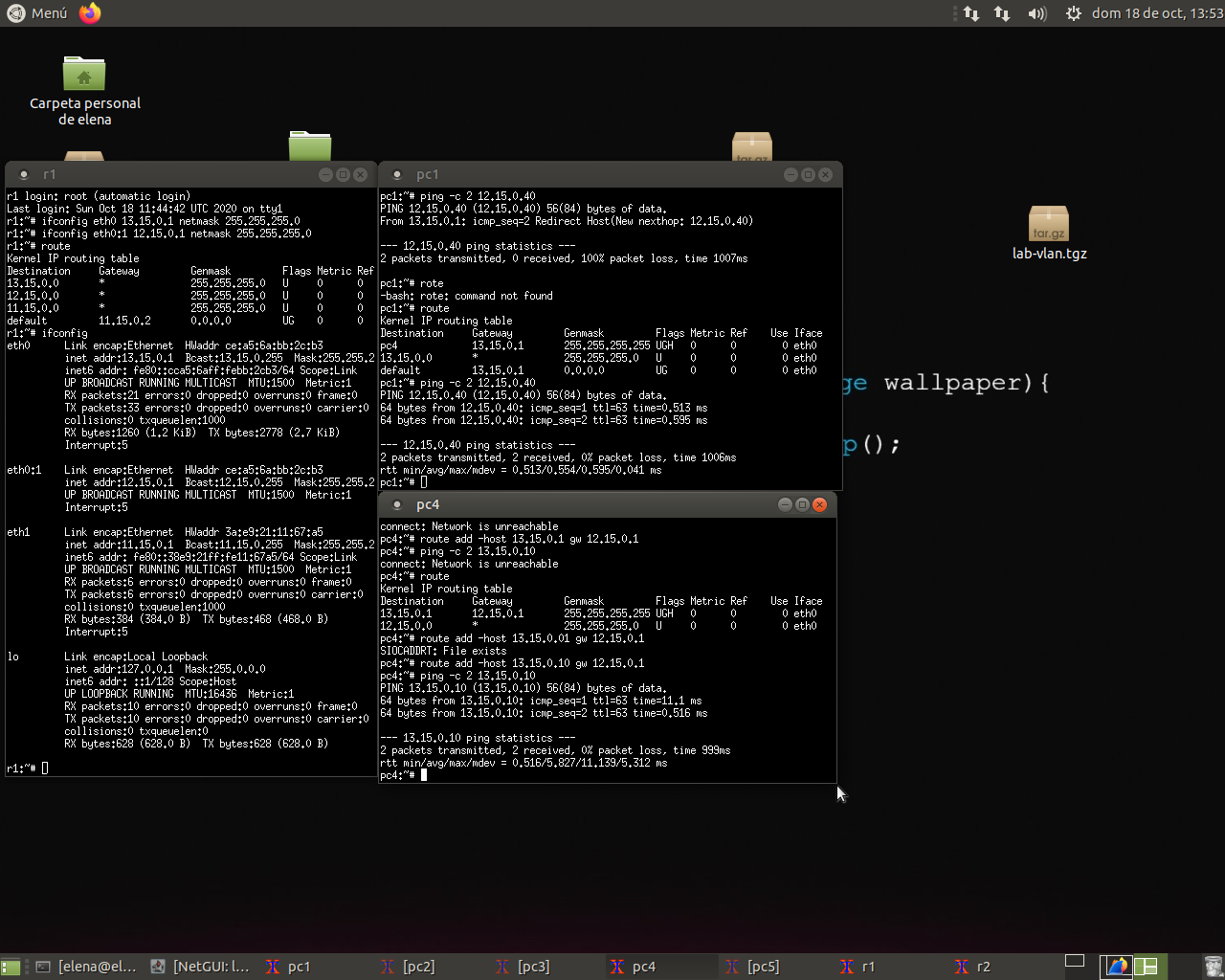
3. ¿Se puede saber solo mirando el chero de captura que en r2 no se ha congurado proxy ARP?

Sí, ya que cuando se usa proxy arp, el router, se hace pasar por la maquina y conesta por ella, por lo que para diferentes direcciones ip, se contesta con la misma . Y en este caso no es así, vemos que con ip aliasing lo que se hace es redirigir a la máquina configurando un gateway para cada dirección.

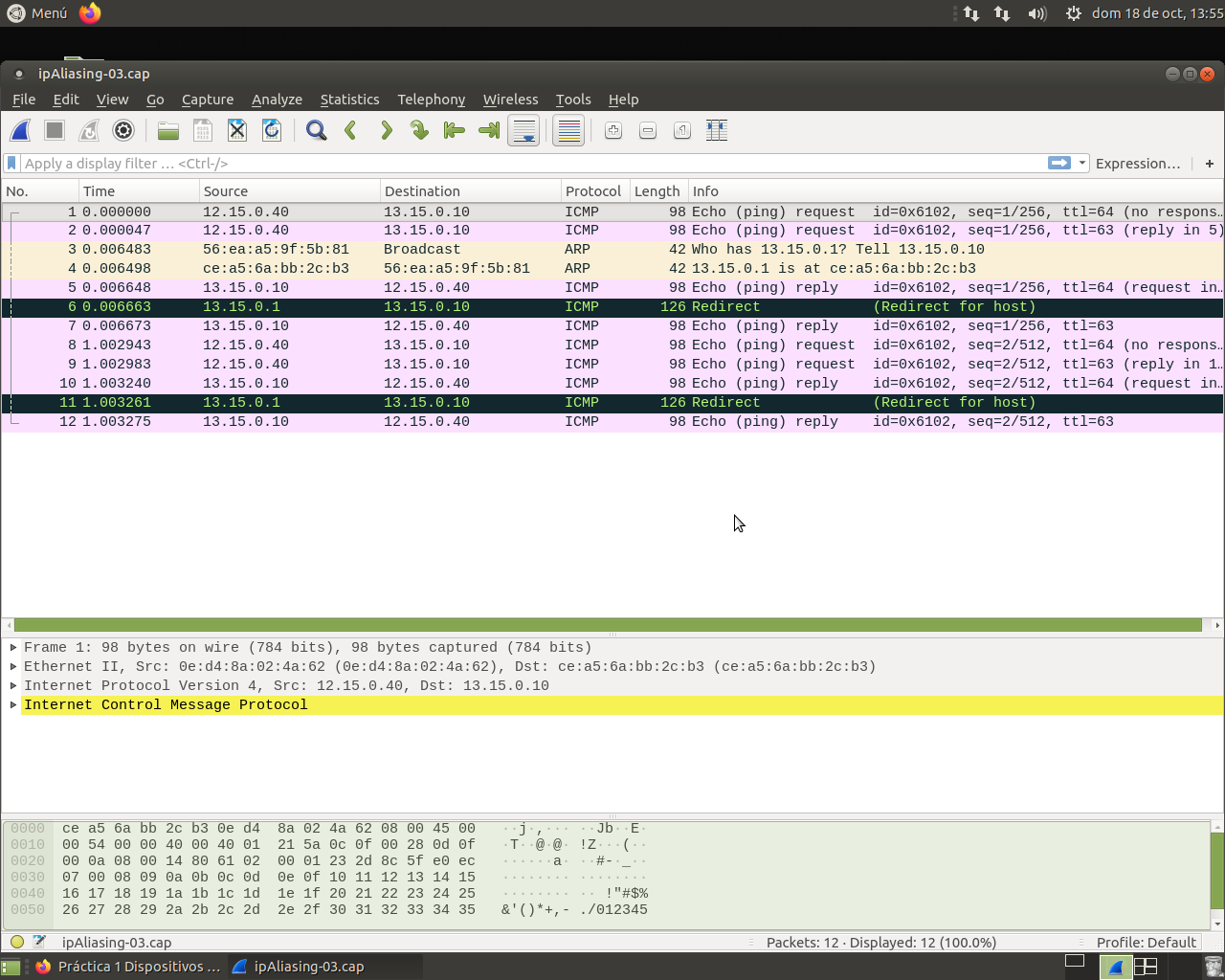
4. Con la configuración que has realizado previamente pueden comunicarse pc1 y pc5? ¿Por qué? Si tu respuesta es negativa, modifica la configuración para que pc5 y pc1 puedan intercambiar tráfico.

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.

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



6. Realiza una captura en r1(eth0) (ipAliasing-02.cap) para ver que paquetes se intercambian cuando pc4 hace ping a pc1. Explica los resultados en la memoria.



**5.VLANs**

1. Explica que máquinas se pueden comunicar entre ellas.

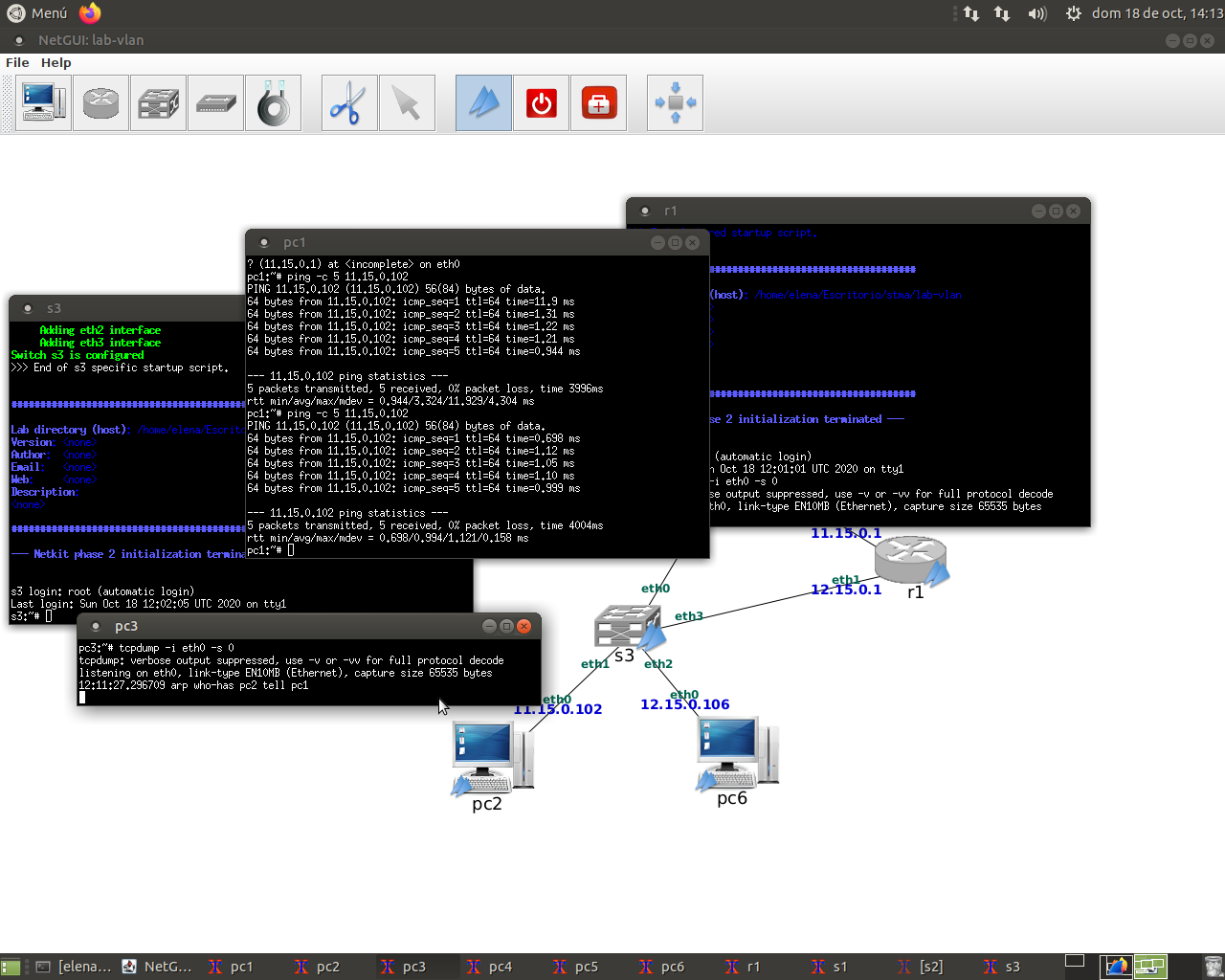
Compruébalo realizando ping.

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, podemos ver un ejemplo en pc3.



**5.1.Configuración de VLAN100.**

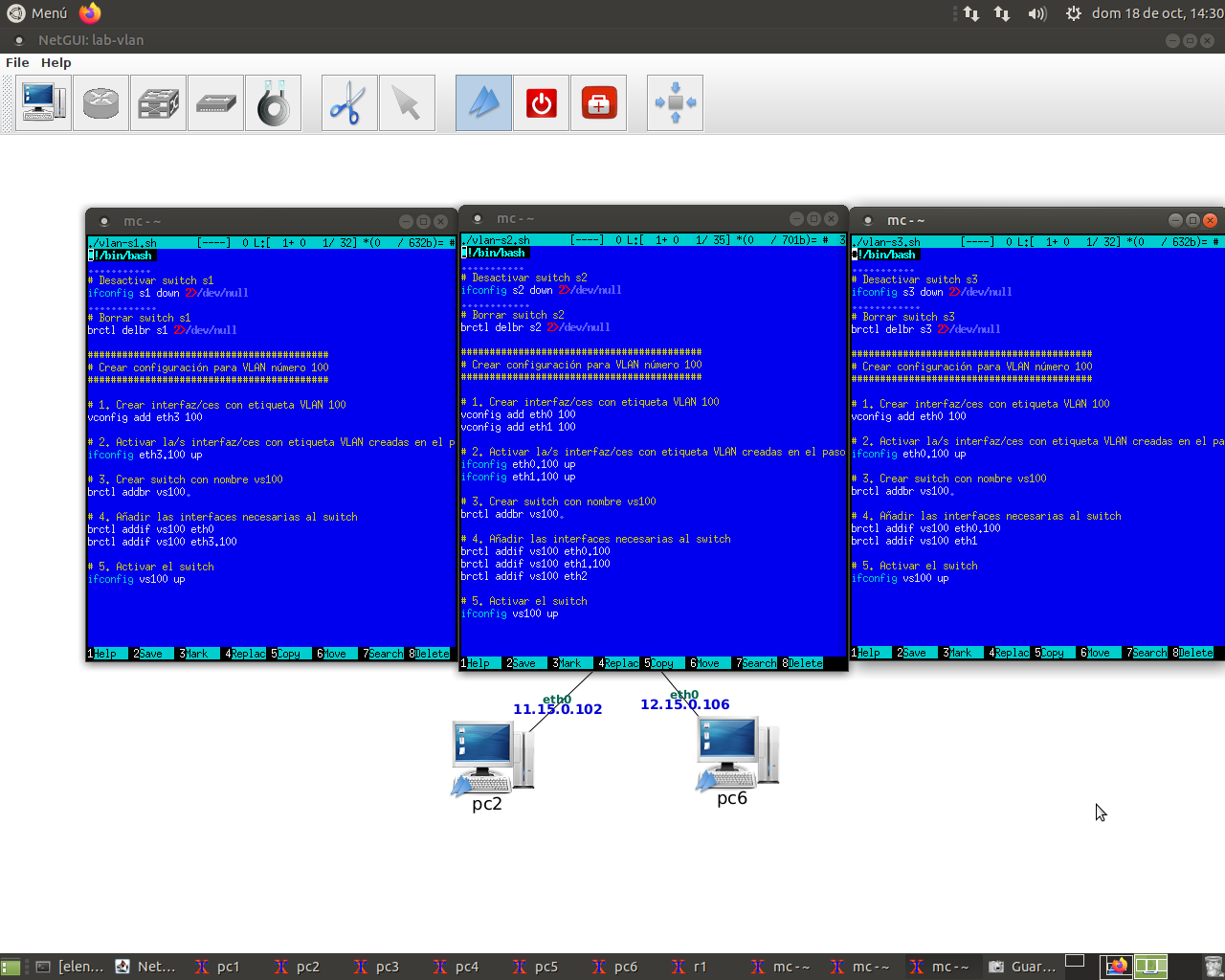
1. Estudia estos scripts para entender qué hace cada uno de ellos. Observa que la primera línea #!/bin/bash indica el intérprete que va a ejecutar este script, en este caso bash. El resto de líneas en el chero que comienzan por # son comentarios. Cada uno de los comandos que se desean ejecutar se escriben en líneas diferentes 4.

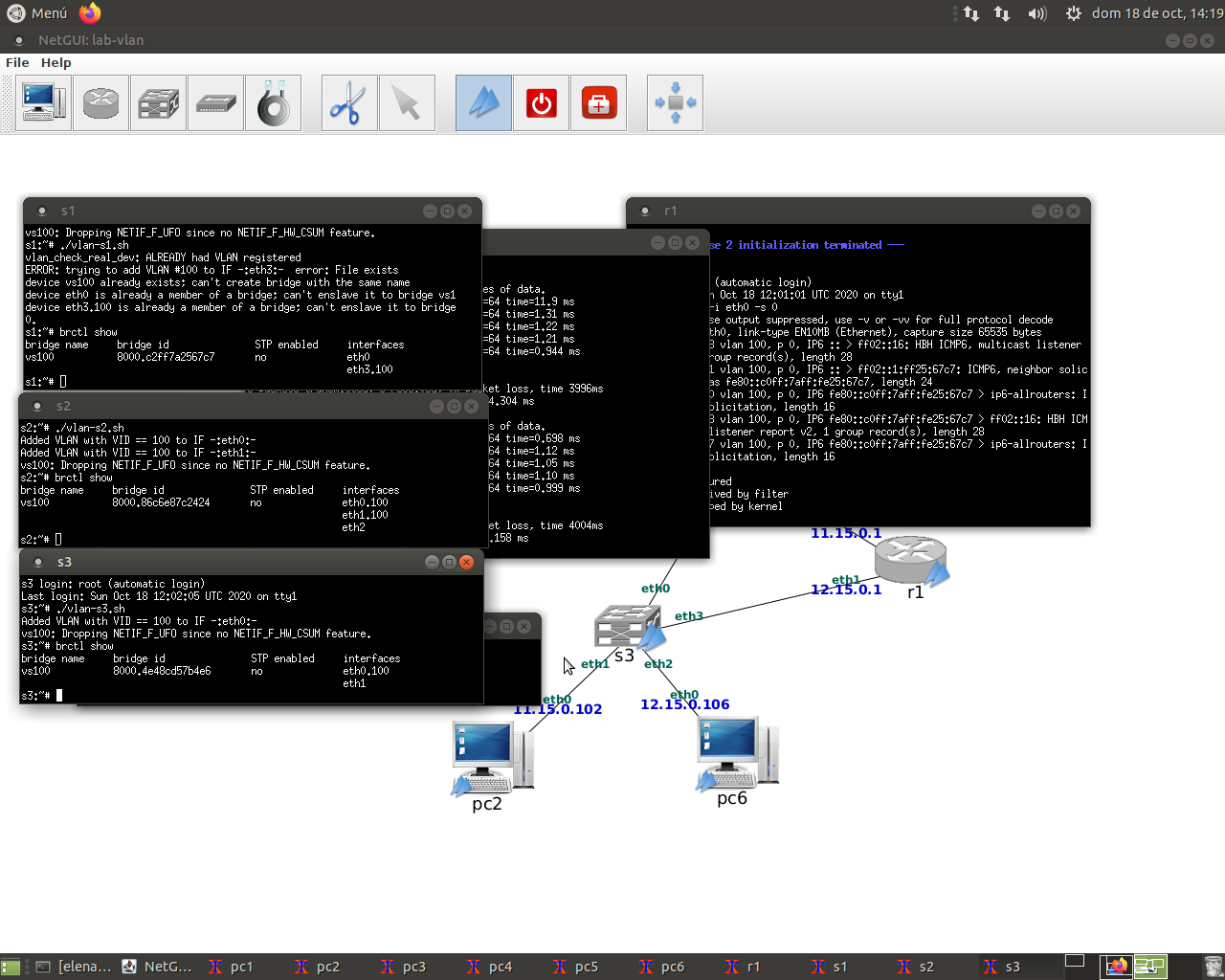
2. Ejecuta los scripts para aplicar la configuración. Debes ejecutar cada uno de esos scripts en su switch, por ejemplo en s1:

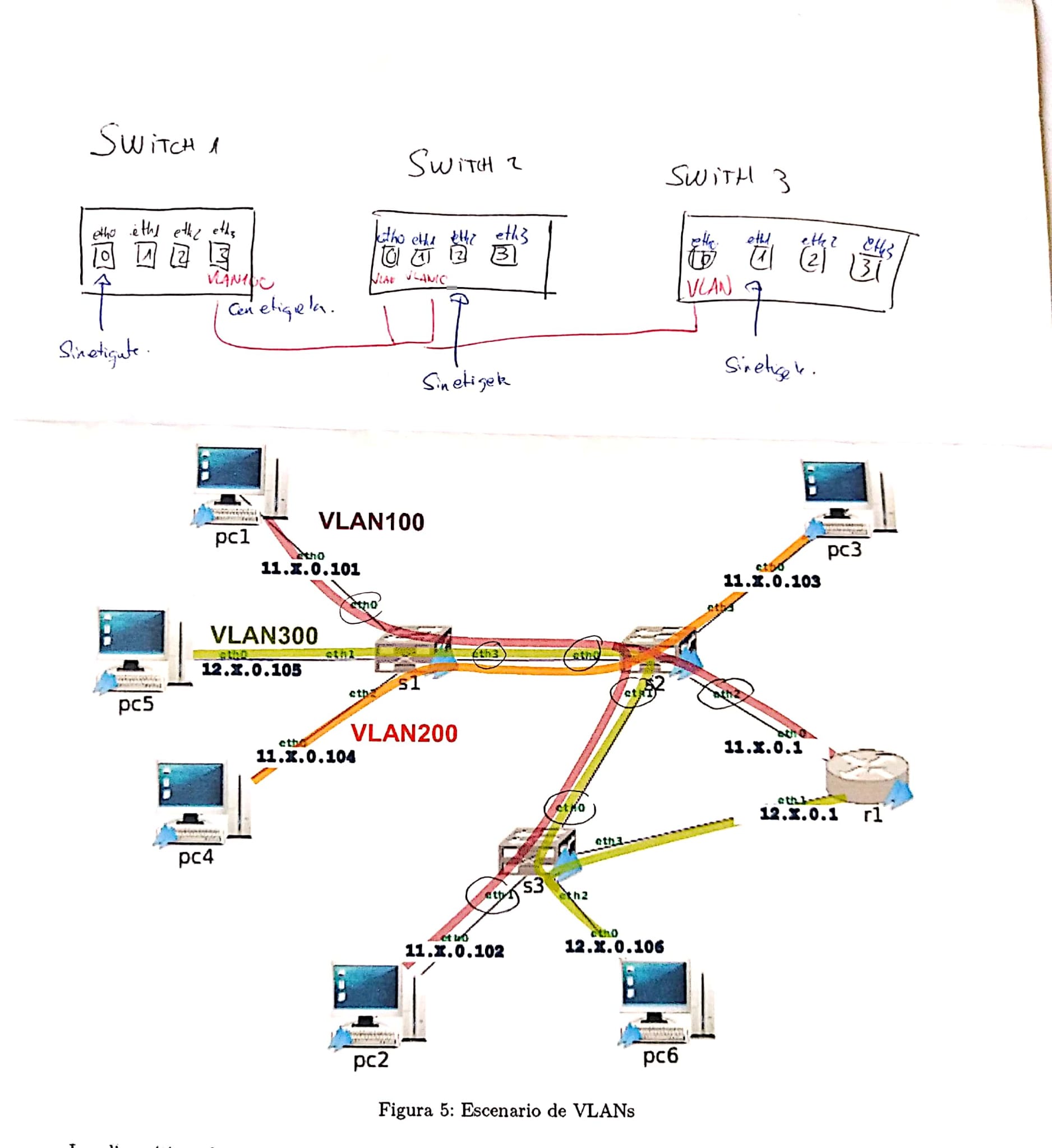
s1:~# ./vlan-s1.sh

Puedes comprobar la configuración que tiene en un switch escribiendo brctl show.

En la captura vemos lo que hemos hecho





3. Haz un dibujo de cada switch que muestre las interfaces que intervienen en la VLAN100, indicando si estas interfaces llevan o no etiqueta VLAN.

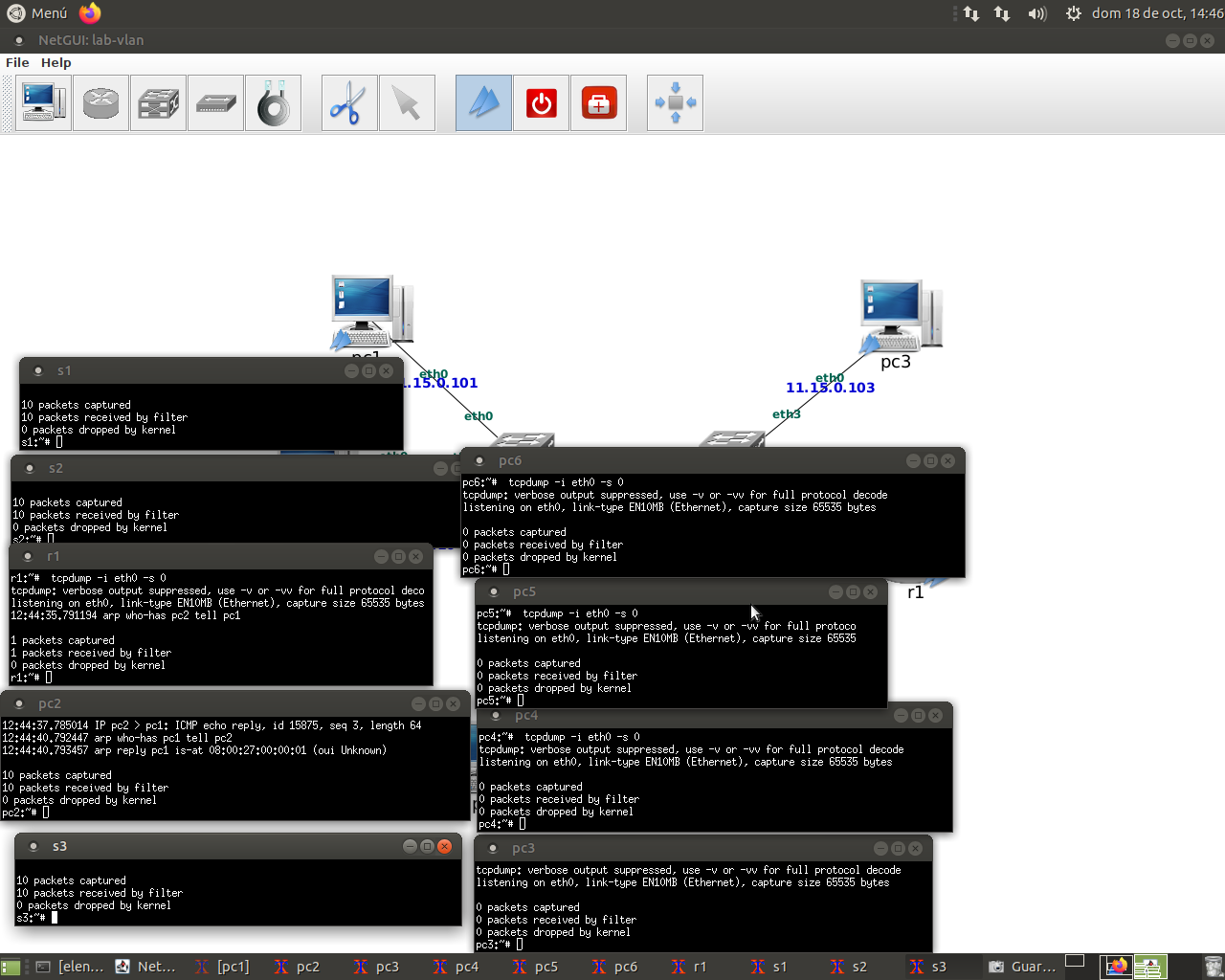
He hecho el dibujo fijandome en los scripts de cada switch y en la figura de vlan, he rodeado, los eth de vlan 100, con y sin etiqueta

4. Indica que maquinas se pueden comunicar entre ellas.

Solo se pueden conectar pc1, pc2 y r1 puesto que están en la misma VLAN.

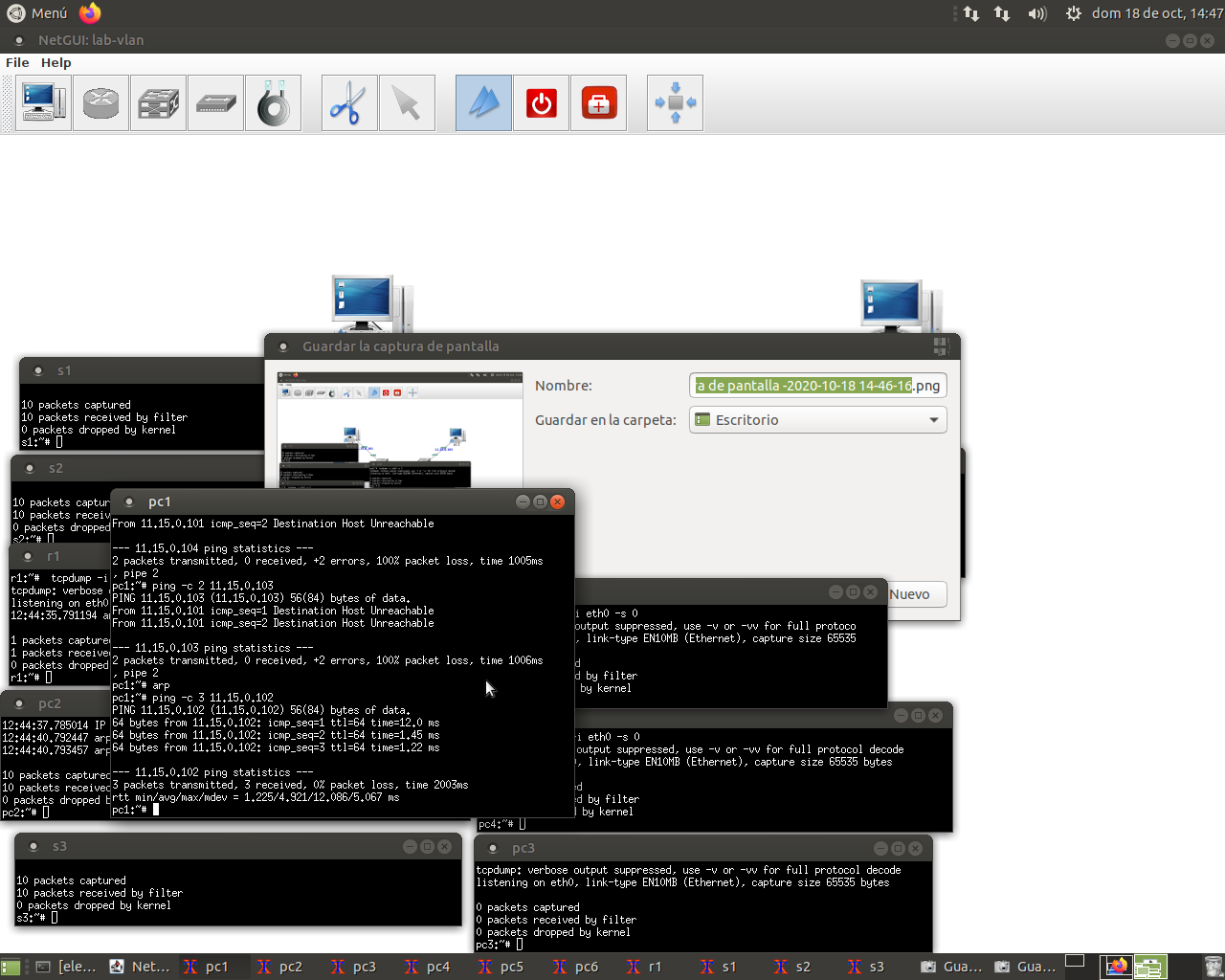
5. Suponiendo que la caché de ARP de pc1 esta vacía, indica donde se puede capturar un solicitud de ARP que la máquina pc1 envía preguntando por la dirección Ethernet de la máquina pc2.

Podemos capturar una solicitud de ARP en s1, s2 ,s3, pc2 o r1 que también están en la VLAN100.



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

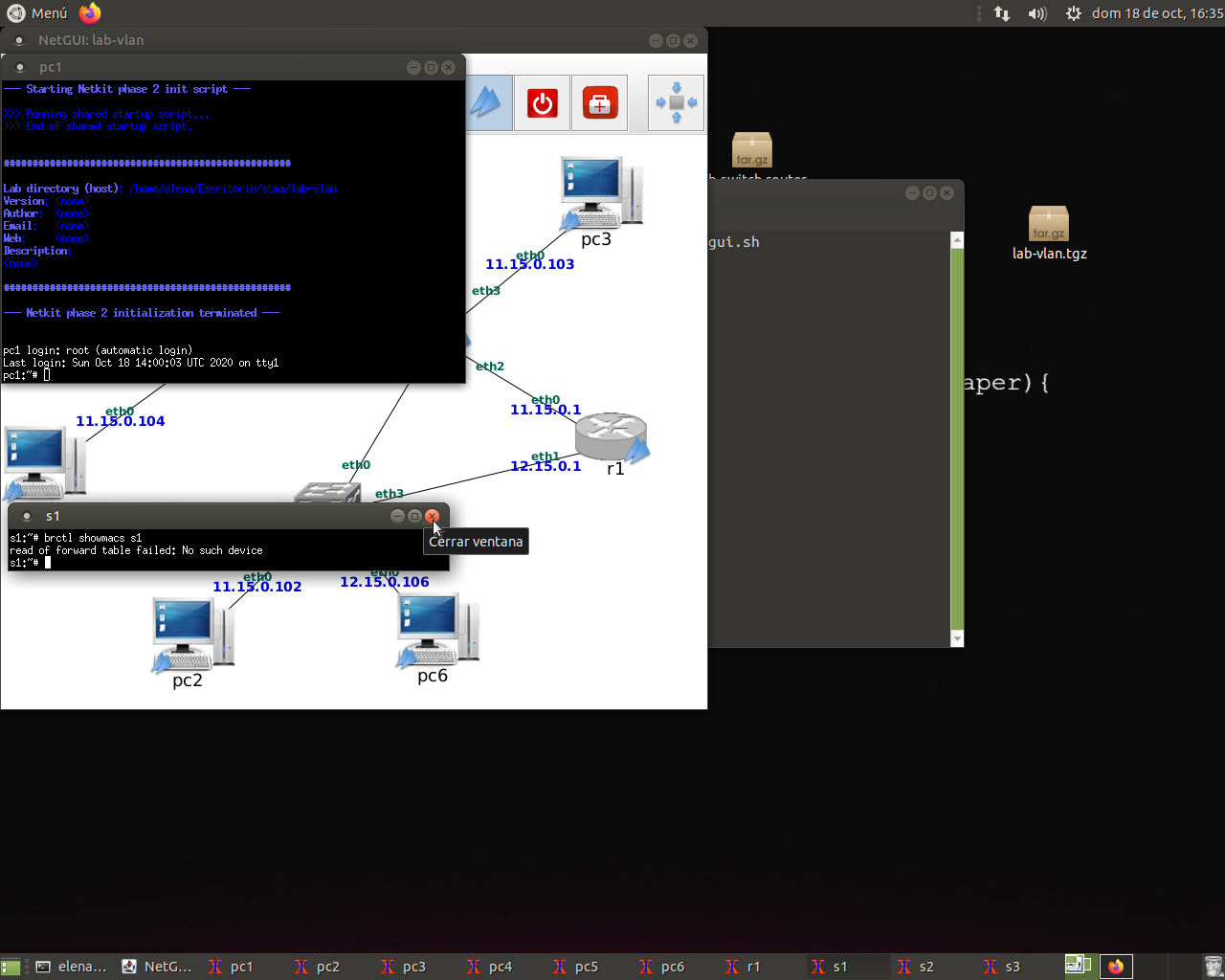
El ping funciona porque además de estar en la misma subred están en la misma VLAN porque sino no funcionaria aunque estuvieran en la misma subred.



7. 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.

8. Interrumpe las capturas. Observa las direcciones Ethernet aprendidas por s1, s2 y s3.

Con el comando brctl showmacs sx, no me deja ver la tabla de direcciones aprendidas.COmo tiene configurado vlans, no existe la tabla de direcciones aprendidas. Seguidamente me di cuenta que las direcciones aprendidas debía consultarlas de vl100. Ya sabemos que las direcciones aprendidas son las que pone no local.





9. 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?

S1, S2 Y S3 tienen dicha etiqueta. Aunque seguramente sea introducida por s1, que es por el primepr que pasa el ping desde pc1.

b) ¿Qué switch elimina dicha etiqueta?

La captura del s2 es la que me sale diferente y no aparece vlan, luego será este switch el que lo elimine.

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. En las capturas de pc2 y pc1 no vemos el capmpo vlan.

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

Por que la interfaz que estamos capturando, aunque pertenece a vlan100, no interviene en esta conexion, está conectada a r1. Luego solo vemos la solicitud arp, como no va con el la cosa, la ignora, y no se captura más trafico.

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)?

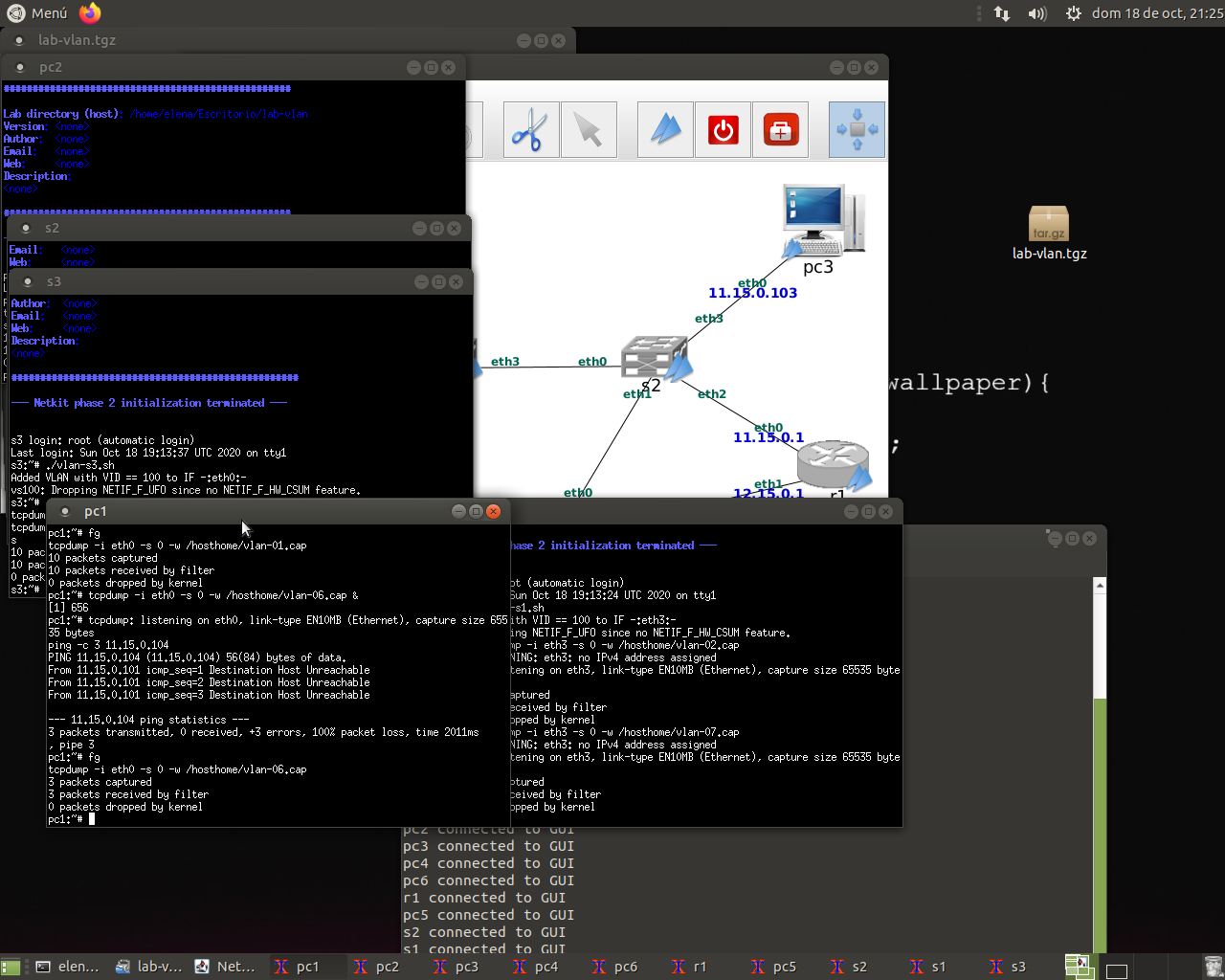
Es practicamente igual, la unica diferencia es que en el switch ya aparece la etiqueta vlan

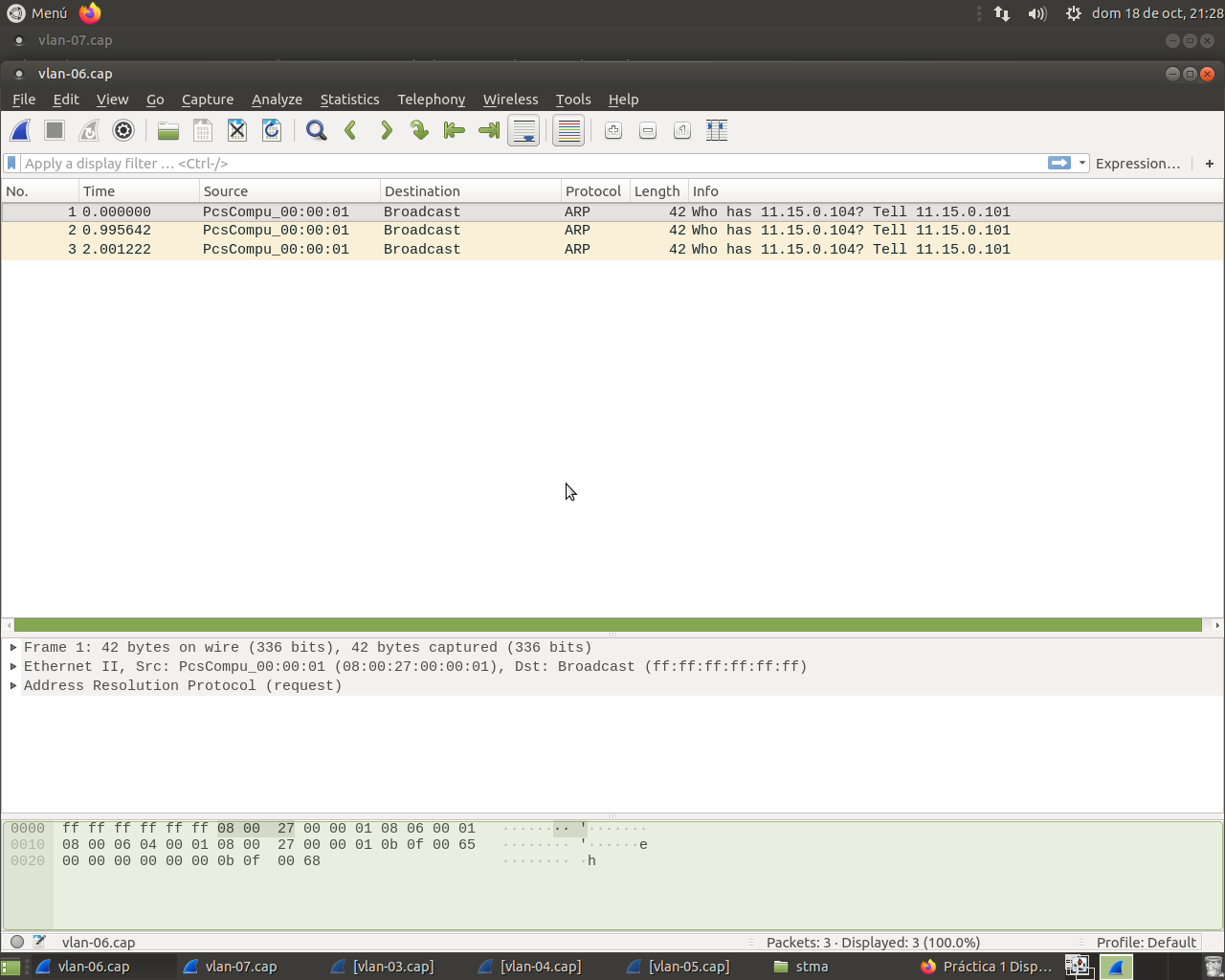
f ) ¿En qué se diferencia el mensaje ICMP Echo request que se captura en pc1(eth0) del mismo mensaje que se captura en s1(eth3)?

De nuevo como en el aparatado anteriorl, la unica diferencia es que en el switch ya aparece la etiqueta vlan

10. 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.

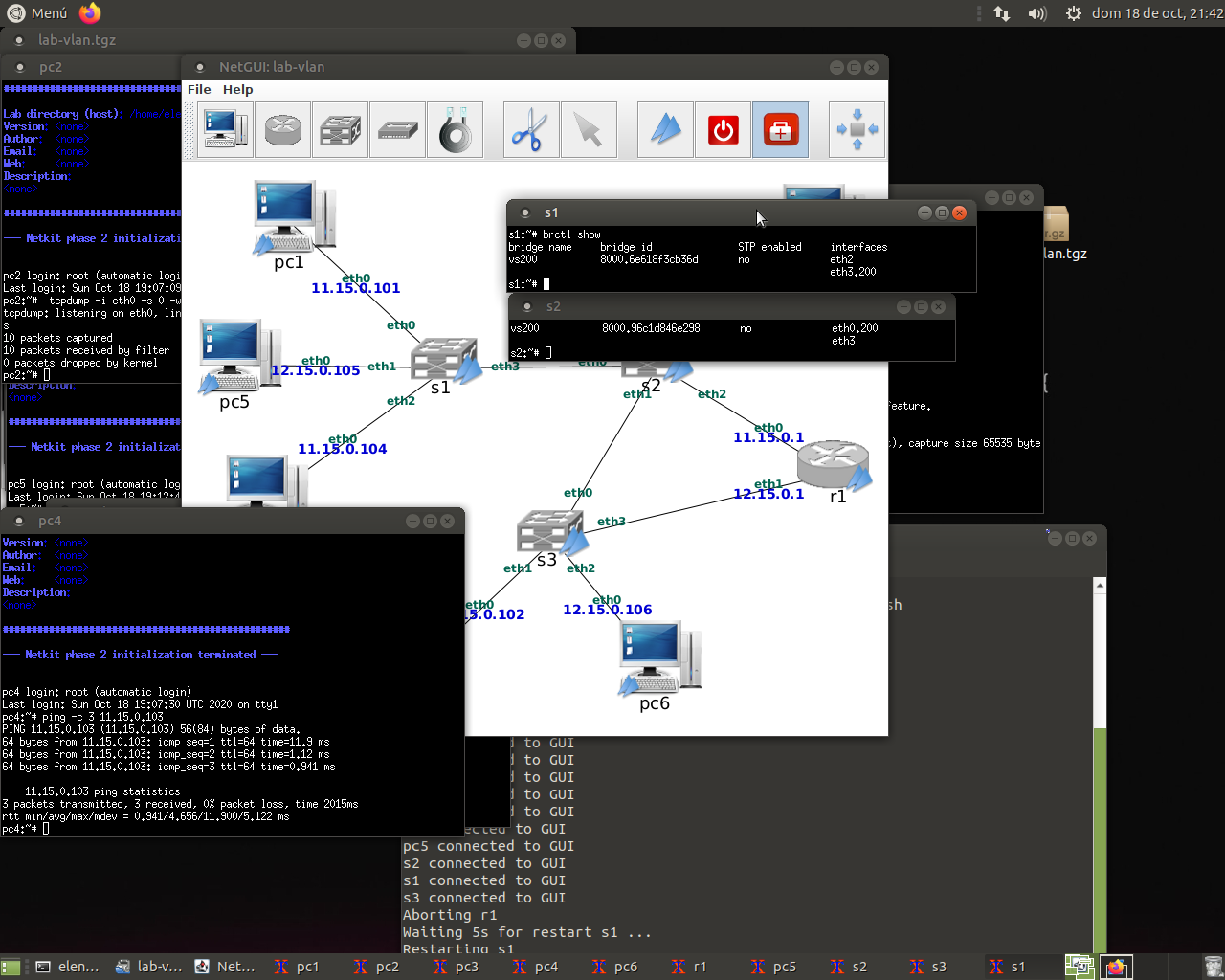
Es indiferente que esten en la misma subred porque el escenario está confuigurado para funcionar con vlan. como pc4 no está conectado, en las capturas solo llegamos a ver solicitudes arp de broadcast.



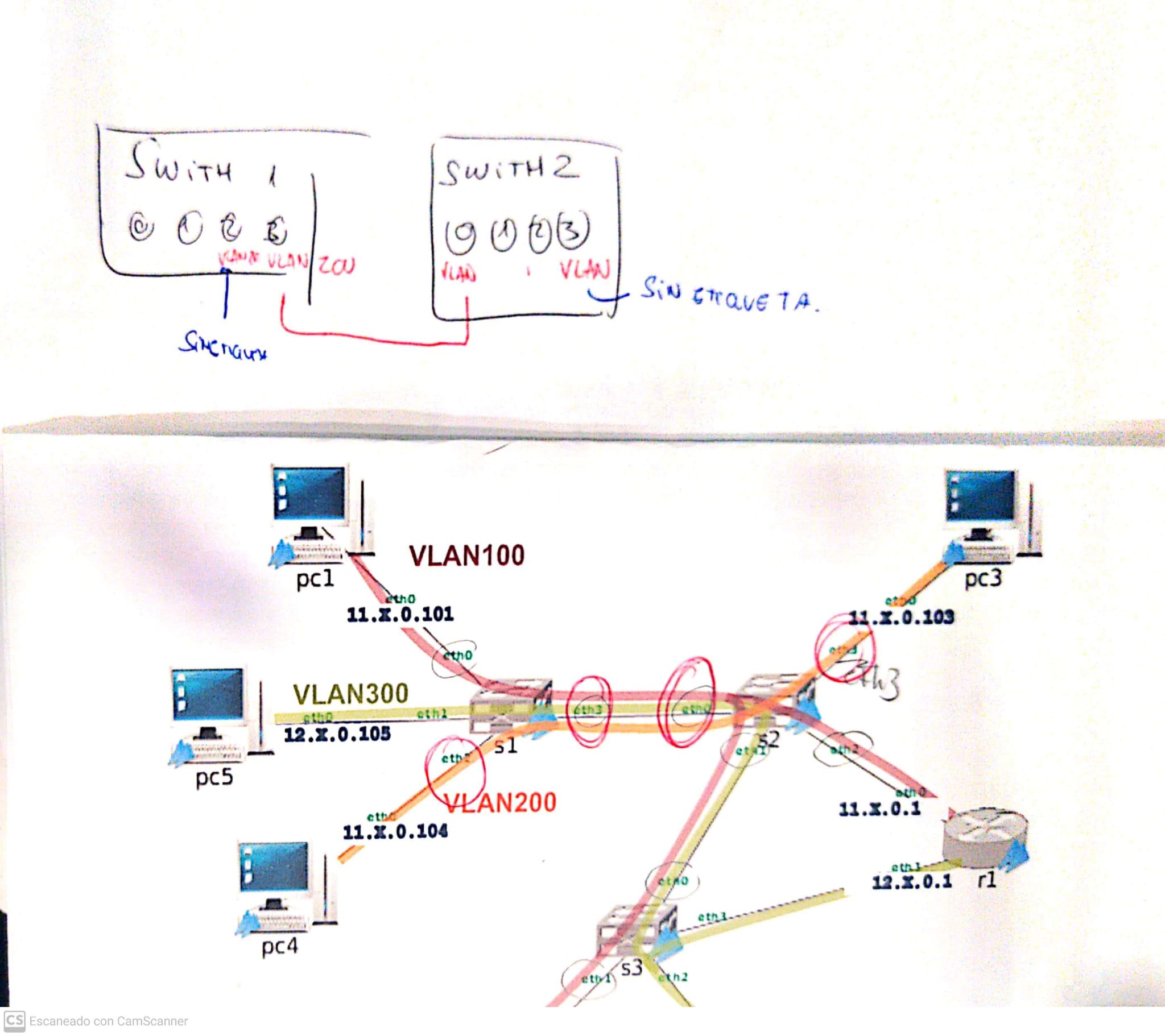


**5.2. Configuración de VLAN200.**

He configurado vlan 200 en los ficheros de configuracion con el comando mcedit ./vlan-s1.sh



1. Haz un dibujo de cada switch que muestre las interfaces que intervienen en la VLAN200, indicando si estas interfaces llevan o no etiqueta VLAN.

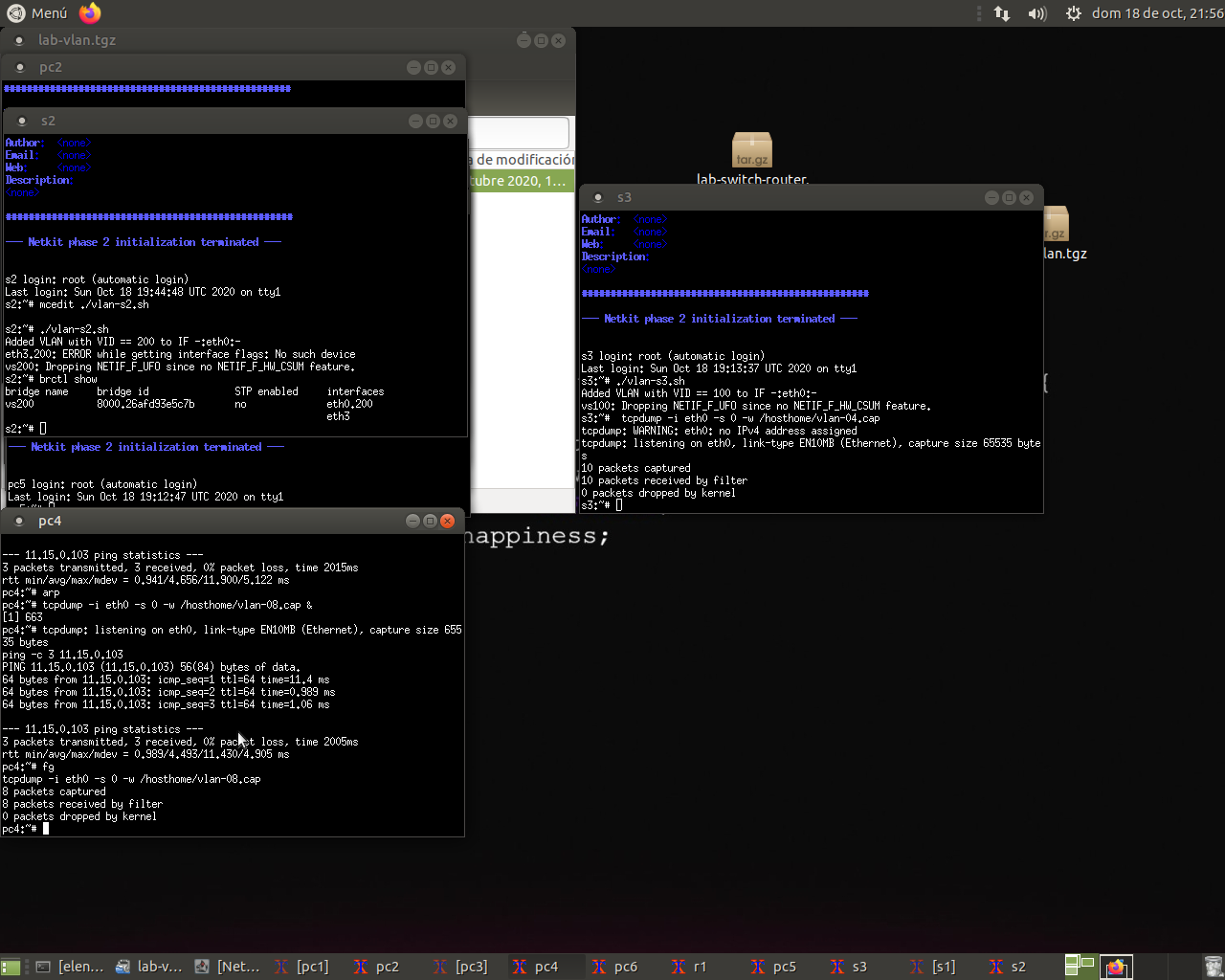


2. Indica que máquinas se pueden comunicar entre ellas con la configuración de VLAN200.

Solo las que están dentro de esa VLAN200, es decir,pc4 y pc3

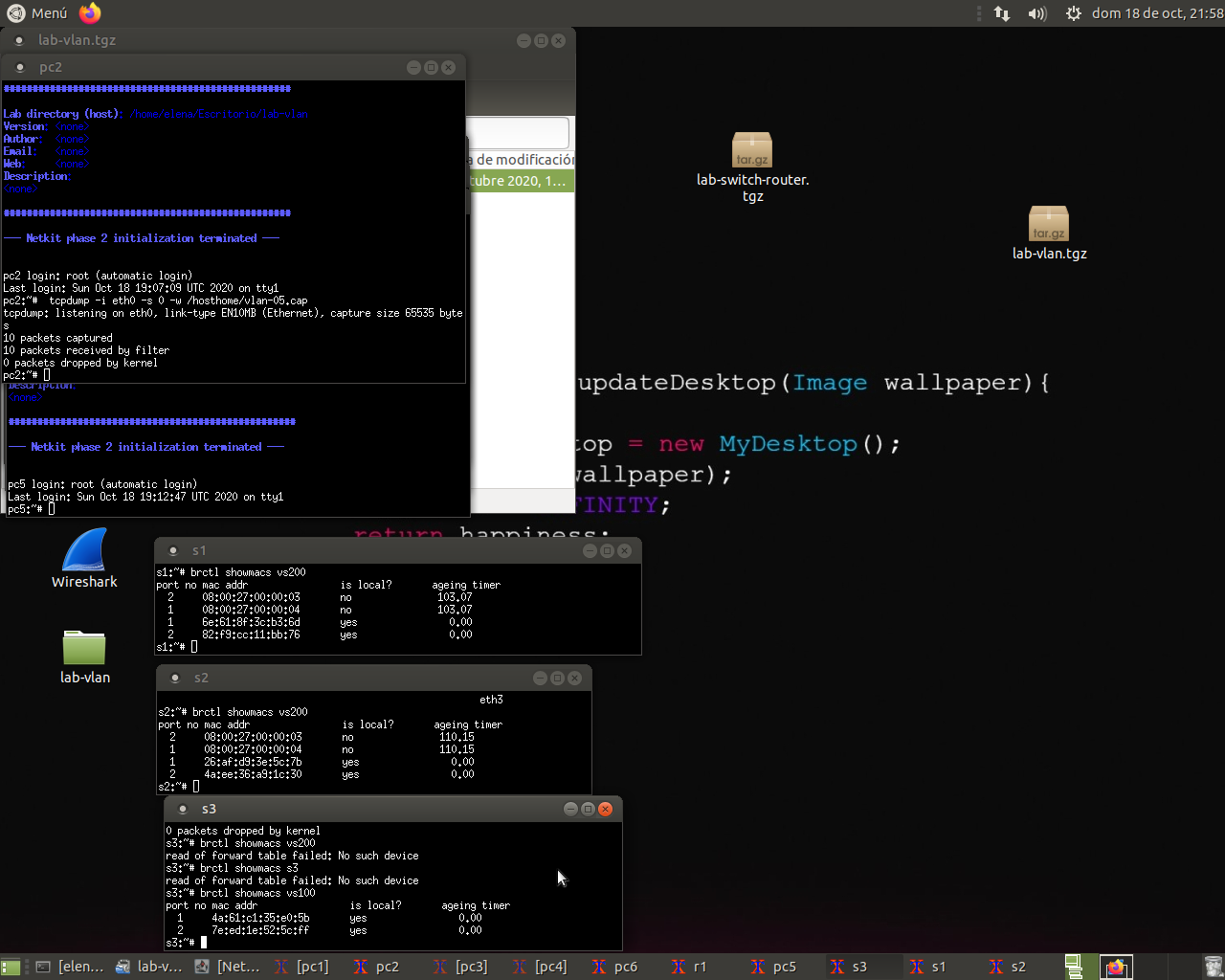
3. Asegurate de que la cache de ARP de pc4 esta vaca, borrala si es necesario. Arranca tcpdump en las siguientes interfaces: pc4(eth0) (vlan-08.cap), s1(eth3) (vlan-09.cap), pc3(eth0) (vlan-10.cap) y pc1(eth0) (vlan-11.cap) guardando esta vez el traco capturado en un chero. Realiza un ping desde pc4 a pc3.

El ping funciona porque están en la misma VLAN200.



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

S3 no aprenderá ninguna porque no esta en vs200. Y s1 y s2 aprenden las de pc3 y pc4



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.

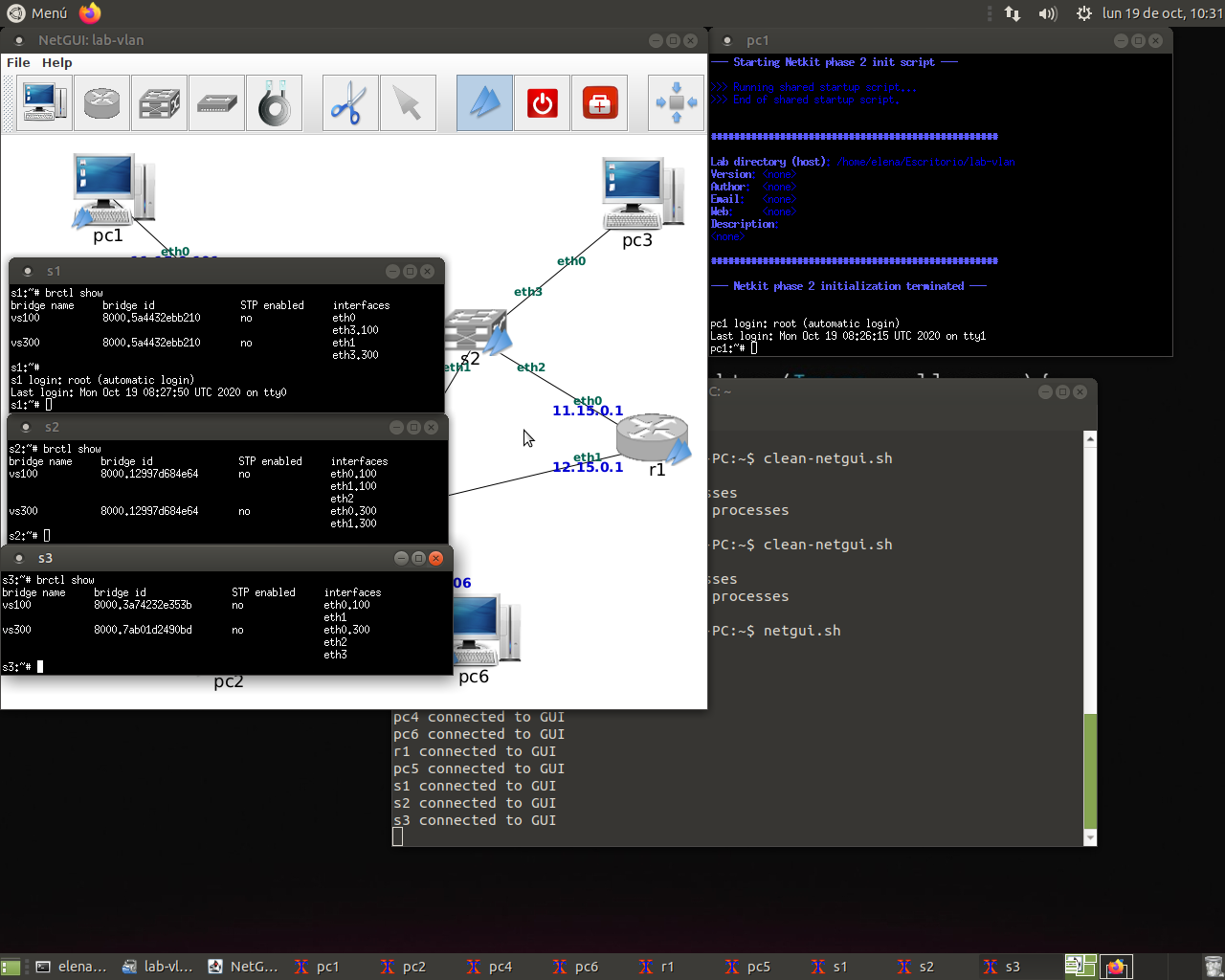
5. Indica que ocurre ahora cuando se hace un ping desde pc1 a pc4, teniendo en cuenta que ambas máquinas se encuentran en la misma subred, conectadas al mismo switch y las interfaces de dicho switch tienen configurada una VLAN. Compruebalo realizando una captura en pc1 (vlan-12.cap) y otra en pc4 (vlan-13.cap).

Explica el resultado.

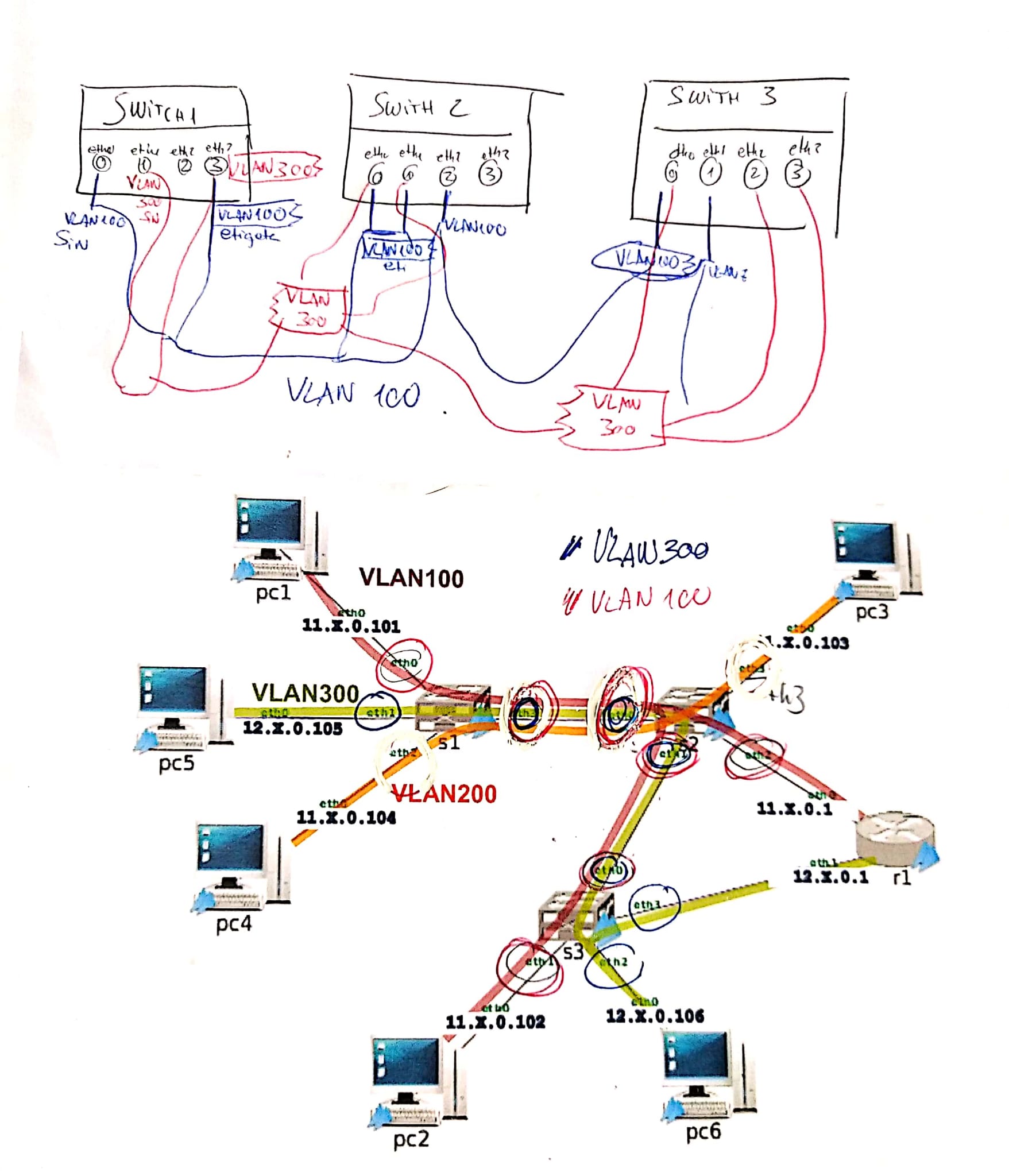
Es indiferente que esten en la misma subred porque el escenario está configurado para funcionar con vlan. pc4 está conectado, en la vlan 200 y pc1 no, por lo que no es posible conectar. en las capturas solo llegamos a ver solicitudes arp de broadcast.

**5.3.Configuración de VLAN300.**

En este apartado se analiza el comportamiento de 2 VLANs que estan conectadas a través de un router. Esta configuración se proporciona en unos scripts que ya se encuentran en el escenario: vlan100y300-s1.sh, vlan100y300-s2.sh y vlan100y300-s3.sh, en s1, s2 y s3 respectivamente.

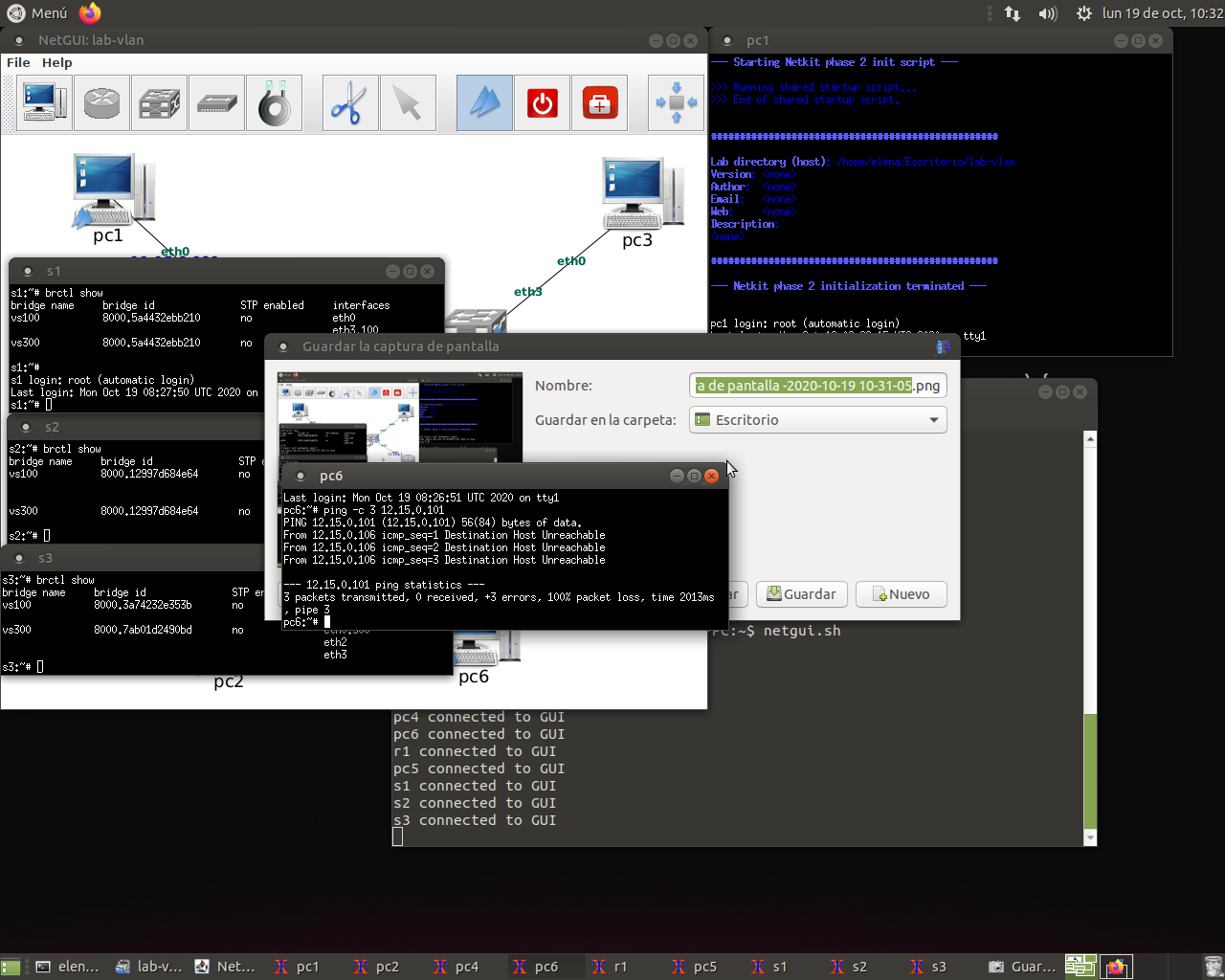


1. Haz un dibujo de cada switch que muestre las interfaces que intervienen en la VLAN200, indicando si estas interfaces llevan o no etiqueta VLAN.



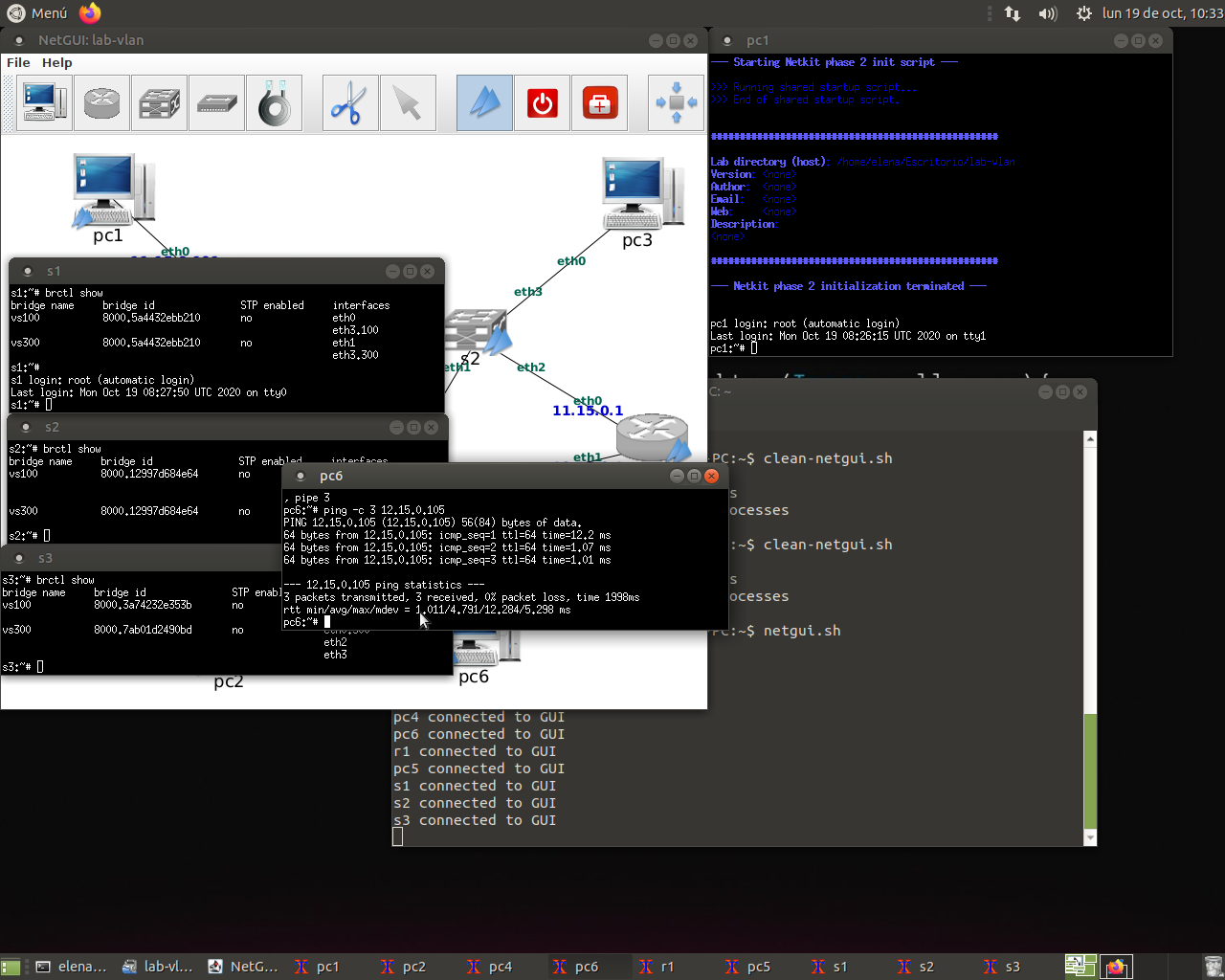
2. Realiza un ping desde pc6 a pc1. ¿Qué crees que está ocurriendo?

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.



3. 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.



4. 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 (en todas sus interfaces), en r1 (todas interfaces), en s2 (eth0,eth1 y eth2), en s1 (todos sus interfaces), en pc2, pc5, pc6 y pc1. Las etiquetas vlan solo la tendrán los switches. El id de la etiqueda 100 o 300 dependerá de las máquinas que se quieran comunicar.

5. Asegúrate de que las cachés de ARP del pc 6y1 están vacías, borrarlas si es necesario. Arranca Tcpdump Las siguientes interfaces:pc6(eth0)(vlan-14.cap),s3(eth1)(vlan-15.cap),r1(eth0)(vlan-16.cap),s2(eth0)(vlan-17.cap) y pc1(eth0)(vlan-18.cap), guardando esta vez el trafico capturado en un fichero. Realiza un ping desde pc6ap c1. Supon en que interfaces aparecera el trafico 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.