Prácticas con NetGUI

Práctica 2: IP, ARP, ICMP

Arquitectura de Redes de Ordenadores

Arquitectura de Internet

GSyC

Departamento de Teoría de la Señal y Comunicaciones y

Sistemas Telemáticos y Computación

Marzo de 2017

Resumen

En esta práctica se aprende a configurar las tablas de encaminamiento de las máquinas utilizando dos métodos distintos: interactivamente mediante el uso del mandato route y estáticamente utilizando ficheros de configuración.

IMPORTANTE: Toma nota de todo lo que hagas en un cuaderno de laboratorio, ya sea en papel o en electrónico. En él debería constar, para cada apartado de esta y de las siguientes prácticas, 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 para dejar constancia de lo que vas aprendiendo en cada práctica. Este cuaderno de laboratorio te será muy útil para repasar lo aprendido.

Introducción

Descarga de la página de la asignatura el fichero lab-p2.tgz, que contiene un escenario de red. Si al pulsar sobre el enlace aparece una ventana de diálogo, elige “Guardar archivo”. Guárdalo, por ejemplo, en la carpeta de Descargas.

En una ventana de terminal, cámbiate con la orden cd al directorio dentro del cuál quieras guardar el escenario de red. Por ejemplo:

cd Practicas

Escribe en la ventana de terminal la siguiente orden para descomprimir el escenario de red:

tar -xvzf ~/Descargas/lab-p2.tgz

El resultado de la ejecución de este comando creará una nueva carpeta que recibirá el nombre lab-p2, en la cual podrás encontrar los ficheros del escenario. La nueva carpeta lab-p2 se creará dentro de la carpeta desde la que se ejecute la orden anterior (en el ejemplo anterior se creará dentro de la carpeta Practicas).

Entre los ficheros del escenario se incluye el script reset-lab, que devuelve el escenario a su estado inicial cuando se ejecuta. Para ejecutar el script hay que estar en la carpeta del escenario, y desde allí escribir en una ventana de terminal de la máquina real:

./reset-lab

Si se desea simplemente devolver algunas máquinas a su estado inicial, pero no todas, es decir, si por ejemplo se desea devolver al estado inicial solo pc1 y r1, se escribirá:

./reset-lab pc1 r1

Tras descomprimir el escenario éste se encuentra en su estado inicial, por lo que no es necesario ejecutar reset-lab al principio.

NOTA: Para realizar esta práctica tendrás que consultar la documentación adicional sobre los comandos para modificar la tabla de encaminamiento, y sobre los comandos arp, ping y traceroute.

1

1. Configuración de tablas de encaminamiento con route

Lanza ahora NetGUI. En el menú, elige File ! Open y selecciona la carpeta lab-p2 en la que está el escenario. Verás aparecer la red de la figura 1.

Arranca únicamente las siguientes máquinas: pc1, pc4, r3 y pc2.

Este escenario realiza una configuración asignando direcciones IP a todas las interfaces de las máquinas, excepto a pc1. Esta configuración inicial está almacenada en el fichero /etc/network/interfaces de cada una de las máquinas, tal y como se ha visto en la práctica anterior.

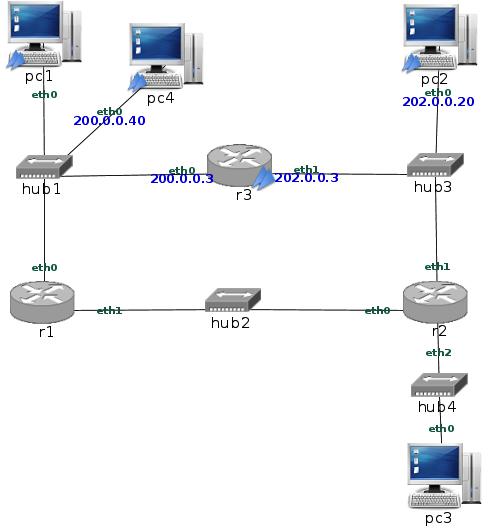
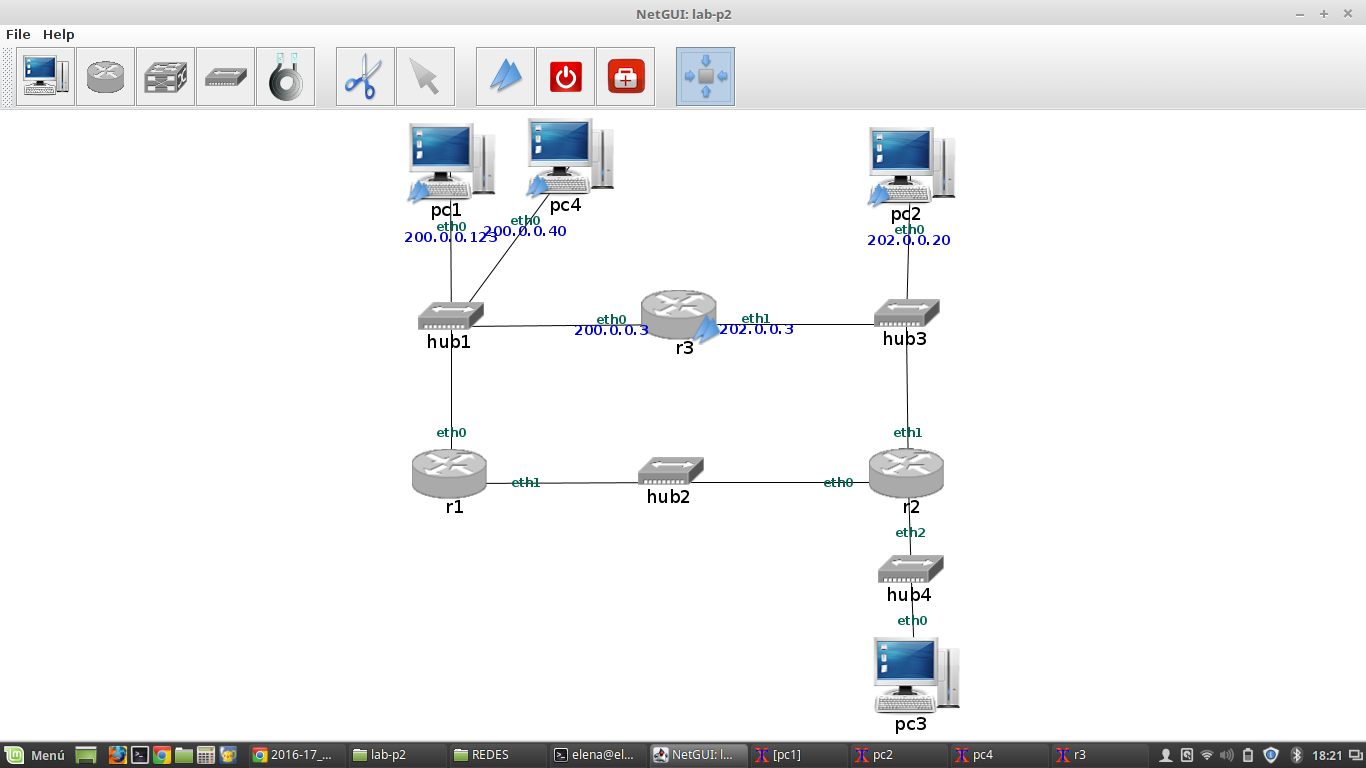


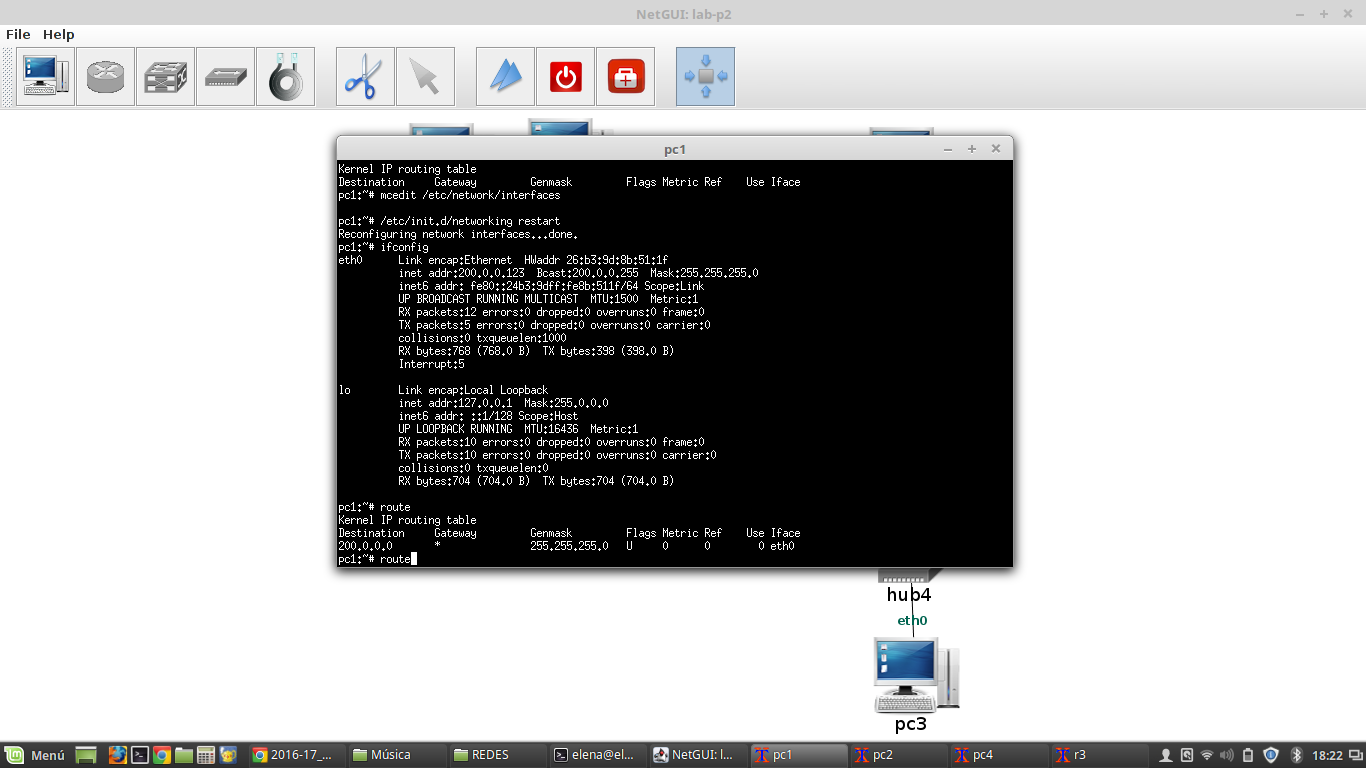
Figura 1: Sólo se arrancan: pc1, pc2, pc4 y r3

Teniendo en cuenta que sólo están estas máquinas arrancadas, responde a las siguientes cuestiones:

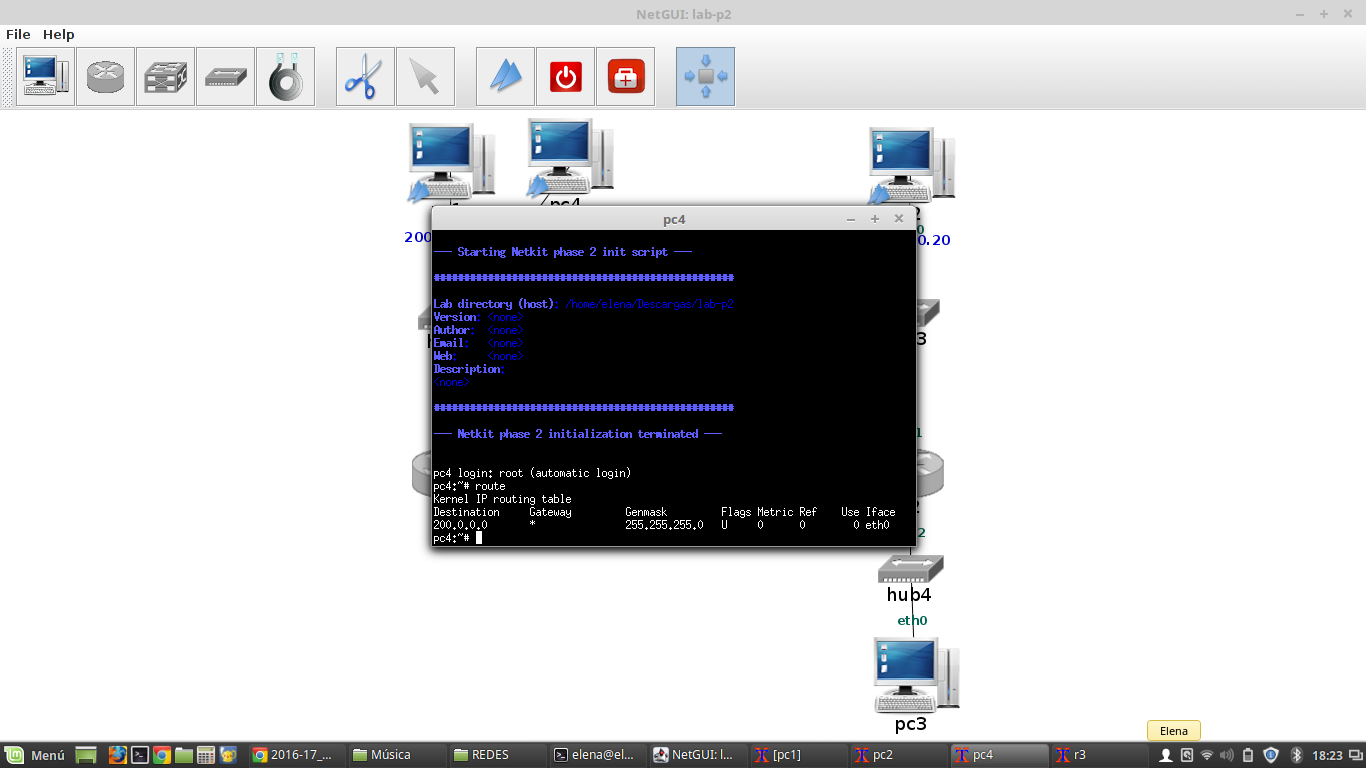
1. **Escribe en pc1 la orden ping 127.0.0.1. ¿Obtienes mensajes de respuesta? ¿Quién está enviando esos men-sajes de respuesta? Con la orden route puedes consultar la tabla de encaminamiento. Comprueba la tabla de encaminamiento de pc1 para ayudarte a entender lo que está pasando.**

Sí obtiene mensajes de respuesta de 127.0.0.1 pero al ejecutar route vemos la tabla de encaminamiento vacía porque el pc1 no tiene direccion ip asignada.

1. **Modifica el fichero /etc/network/interfaces de pc1 para que pc1 tenga una dirección IP acorde a la subred a la que está conectado Reinicia la red en pc1 para que se aplique la configuración que has escrito en el fichero /etc/network/interfaces.**
2. **Comprueba con route cómo en pc1, tras asignar la dirección IP a su interfaz de red, se ha añadido auto-máticamente una entrada en la tabla de encaminamiento. Con esta tabla de encaminamiento en pc1, ¿a qué otras direcciones IP crees que pc1 podrá enviar datagramas IP?**

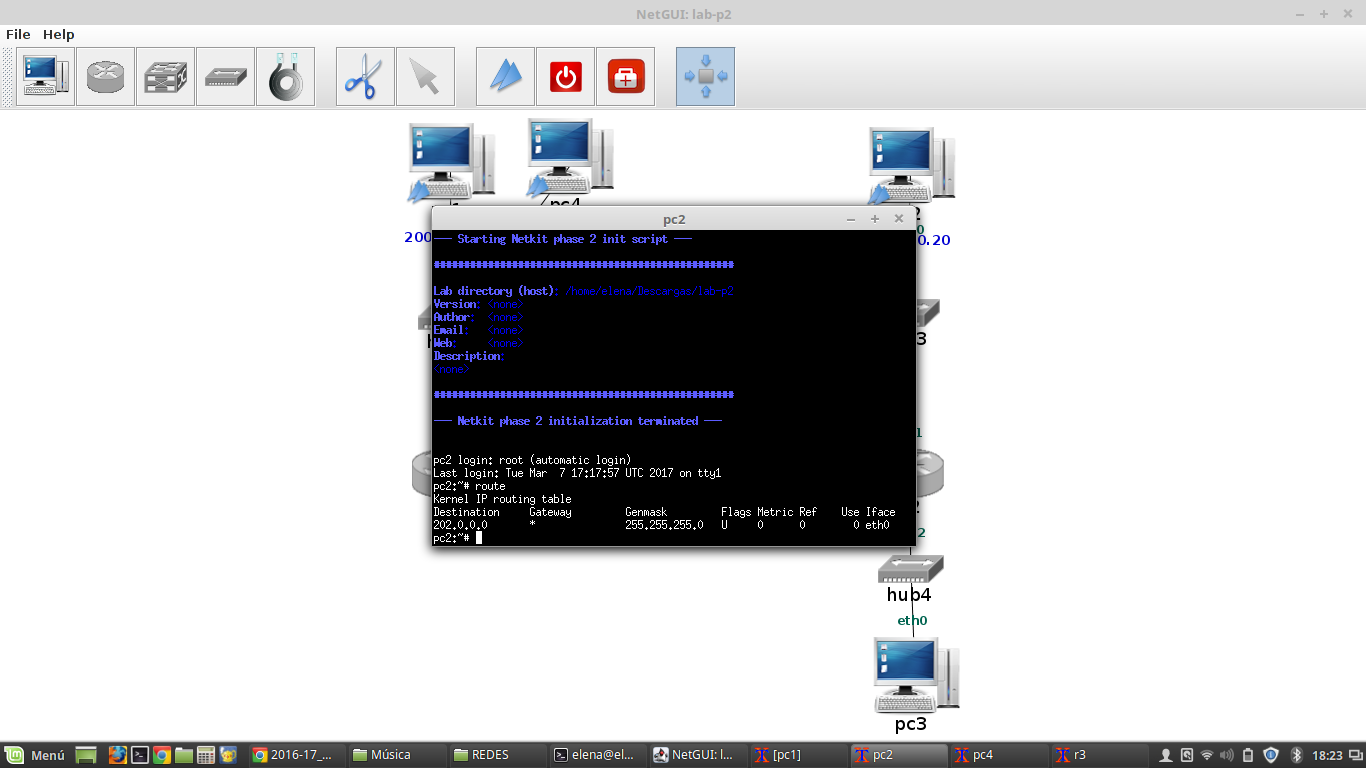
A las que se encuentran dentro de la misma subred, y dentro de la misma tienen asignada dirección ip con la misma cabecera, en este caso 200.0.0.

1. **Dado que el resto de las máquinas tienen ya configurada una dirección IP, podrás suponer fácilmente cuál es el contenido de su tabla de encaminamiento:**

**¿Cuál crees que será la tabla de encaminamiento de pc4?. Compruébalo consultando su tabla. Con esta tabla de encaminamiento, ¿a que otras direcciones IP crees que pc4 podrá enviar datagramas IP?**

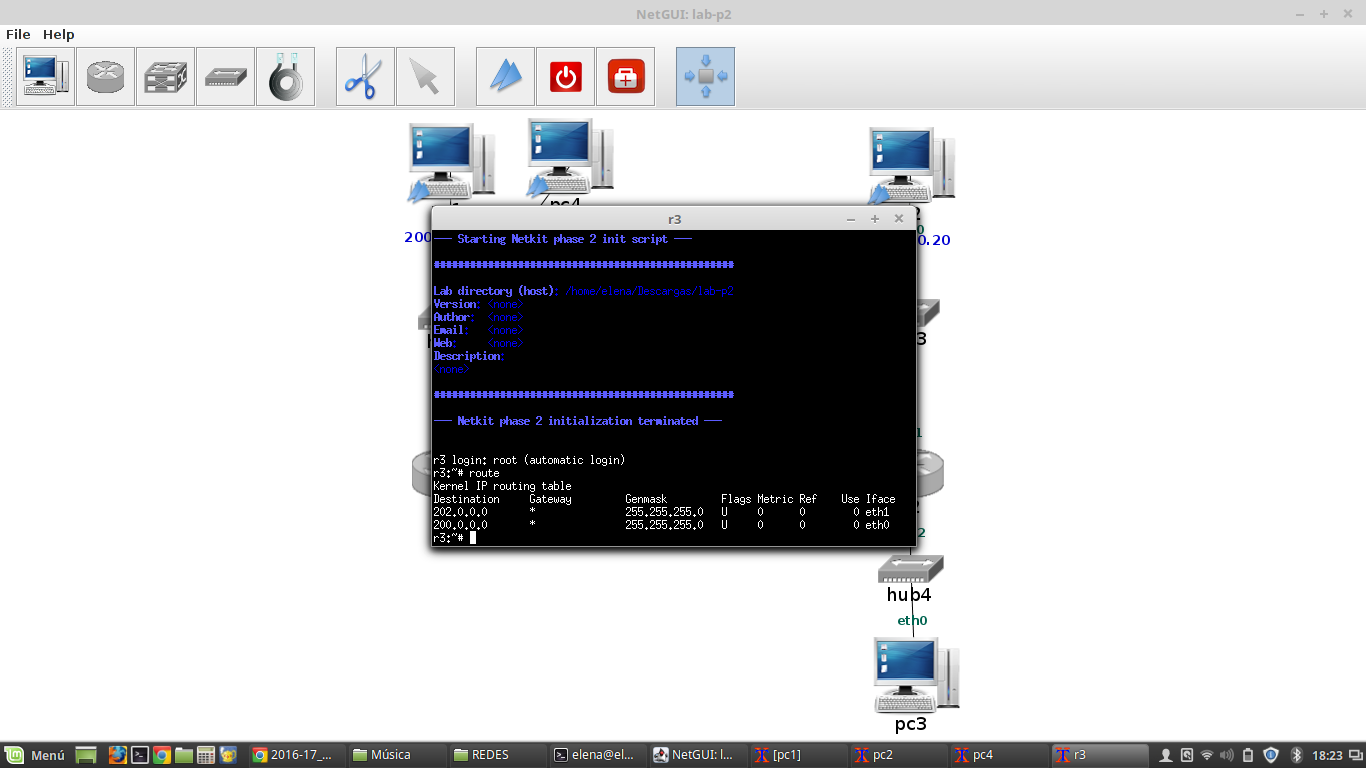
Con esta tabla de encaminamiento puede mandar datagramas ip a las máquinas que tengan la misma cabecera 200.0.0., que en este caso serían pc1, y r3

**¿Cuál crees que será la tabla de encaminamiento de pc2?. Compruébalo consultando su tabla. Con esta tabla de encaminamiento, ¿a que otras direcciones IP crees que pc2 podrá enviar datagramas IP?**



Con esta tabla de encaminamiento pc2 puede enviar datagramas ip a r3 unicamente que de las máquinas encendidas es de su misma subred y tiene la misma cabecera 202.0.0.

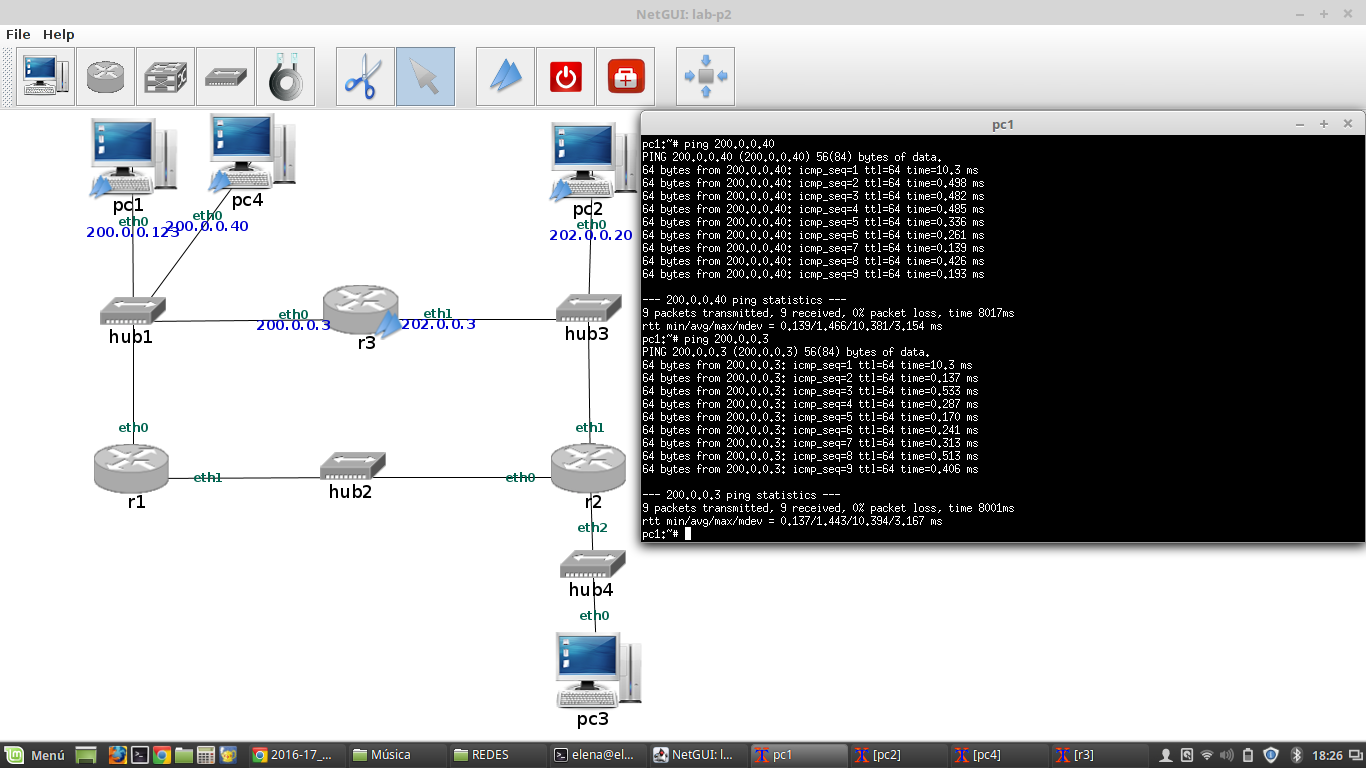
**¿Cuál crees que será la tabla de encaminamiento de r3?. Compruébalo consultando su tabla. Con esta tabla de encaminamiento, ¿crees que r3 puede enviar datagramas IP a pc1 y pc4? ¿Y a pc2.**



Con esta tabla de encaminamiento podrá enviar datagramas ip con la interfaz eth1 a las máquinas dentro de su misma subred con su misma cabecera en la dirección ip, 202.0.0. y puede enviar a pc2.

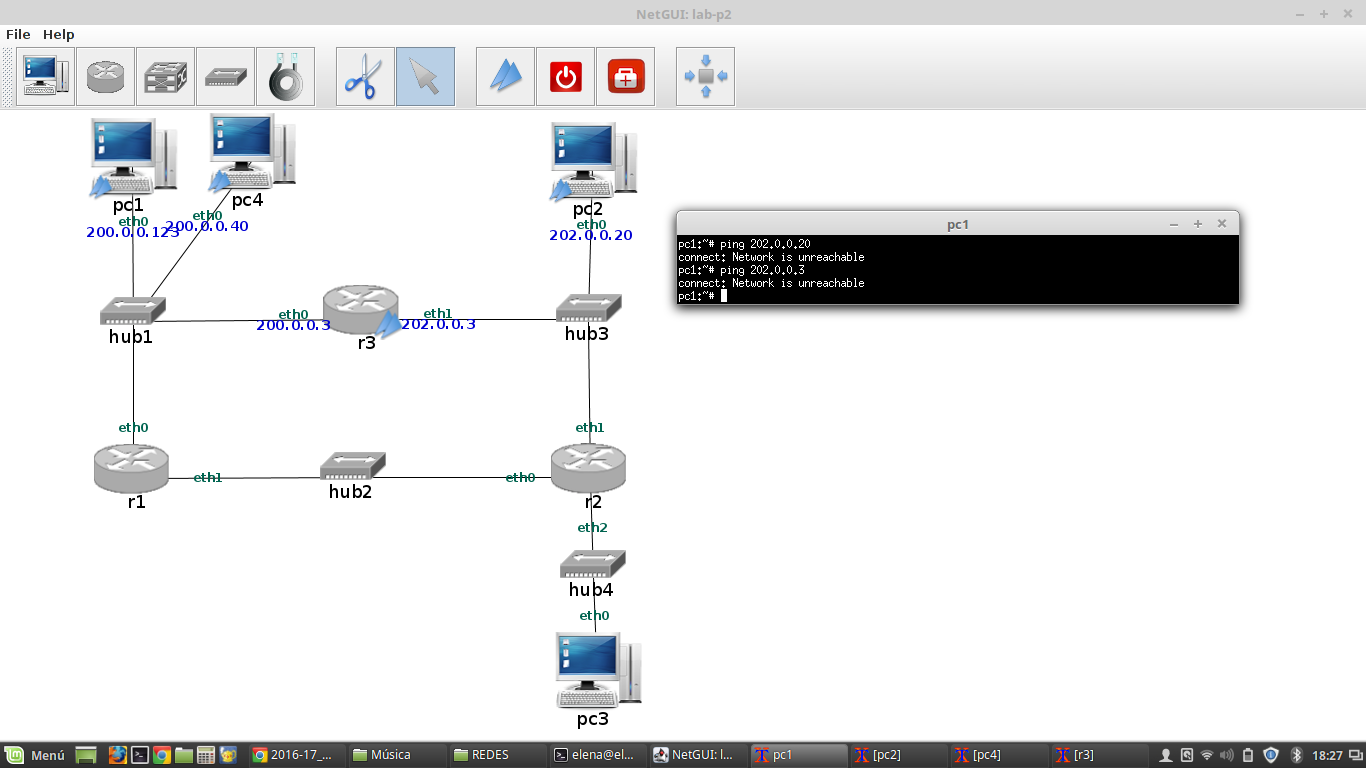
Con la interfaz eth0 puede enviar datagramas ip dentro de su misma subred que en este caso la cabecera es 200.0.0. y puede enviar a pc1 y pc4.

1. **Haz ping desde pc1 a pc4 y haz ping desde pc1 a la dirección r3(eth0). Ten en cuenta que no puedes utilizar los nombres pc1, pc4, etc. en el ping, sino que debes usar las direcciones IP correspondientes. ¿Funcionan estos ping? ¿Qué entradas de las tablas de encaminamiento se consultan en cada caso?**

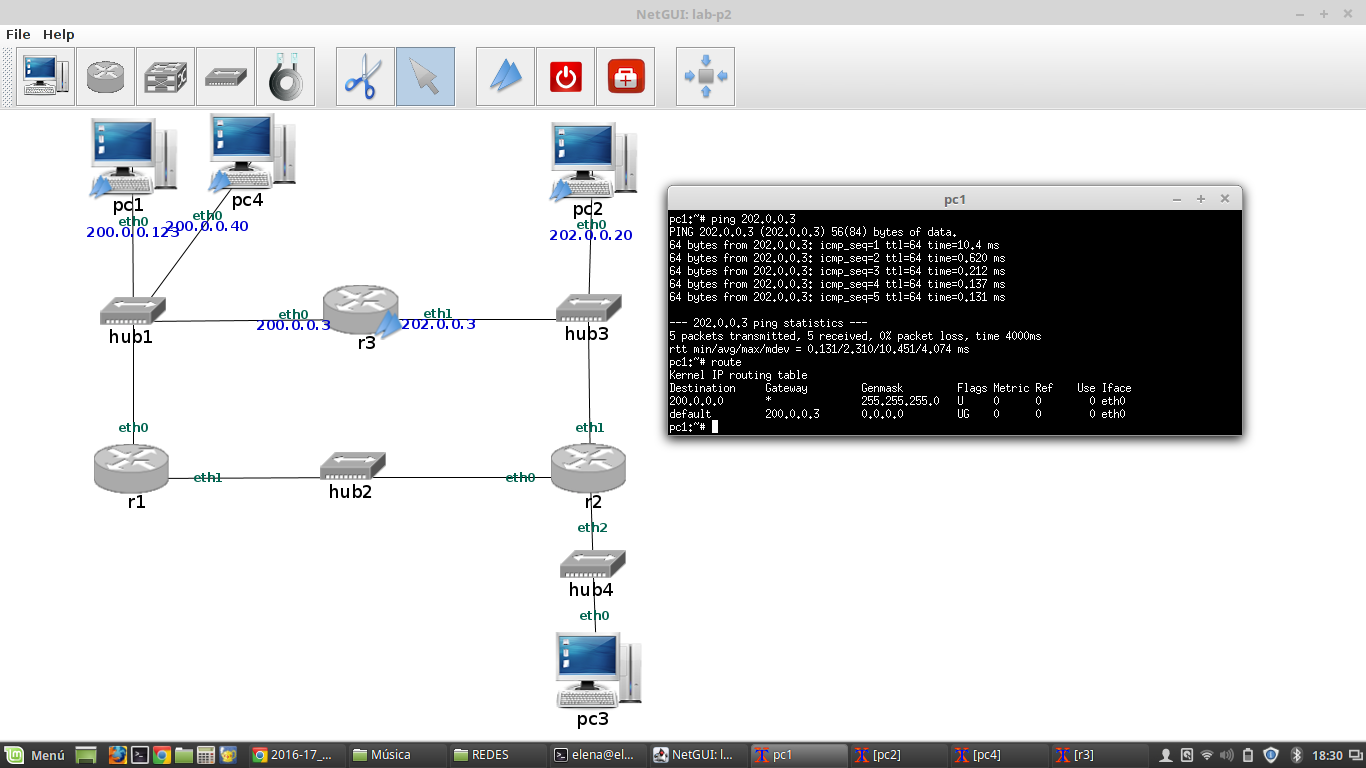
Sí porque pc4, r3 con interfaz eth0 y pc1 pertenece a la misma subred y tienen la misma cabecera en la dirección ip 200.0.0.

Se está utilizando la enteada 200.0.0.0 de la tabla de encaminamiento de r3.

**6. Haz un ping de pc1 a pc2 y haz un ping de pc1 a la dirección r3(eth1). ¿Funcionan estos ping? ¿Por qué?**

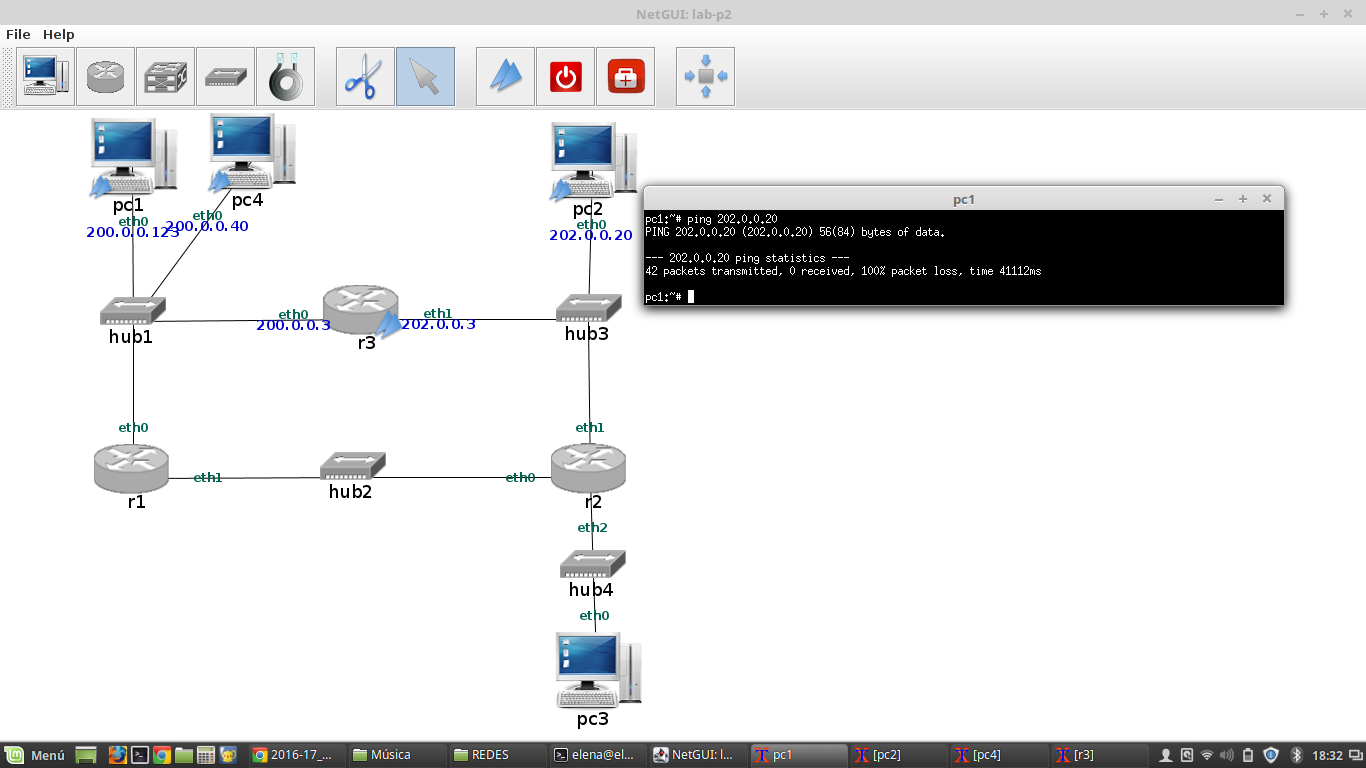
No funcionan porque pc1 no puede encaminar a 202.0.0.20 directamente necesitaría la ayuda de una interfaz vecina que es 200.0.0.3 y hay que configurarlo mediante *route*.

1. **Añade una ruta con el comando route en pc1 para que los datagramas IP que no sean para su propia subred los envíe a través del router r3.**
2. **Haz ahora ping desde pc1 a r3(eth1). ¿Funciona este ping? ¿Qué entradas de las tablas de encaminamiento se consultan?**



Funciona, porque con route hemos configurado que por defecto lo encamine a 200.0.0.3. Por lo tanto usamos la parte de la tabla de encaminamiento que hemos creado en el apartado anterior, la entrada por defecto o lo que es lo mismo *default.*

1. **Haz un ping de pc1 a pc2. ¿Por qué no funciona este ping?**



Porque he configurado una ruta de ida, pero no he configurado una ruta en pc2 de vuelta.

1. **En función del contenido actual de las tablas de encaminamiento de las máquinas y del router, explica qué máquinas podrán comunicarse entre sí.**

**Según lo configurado ahora:**

Pc1 se comunica con pc2 y r3

Pc2 se comunica con r3

Pc4 se comunica con r3

R3 se comunica con pc1 pc2 y pc4

**Pc1**

**Route**

**Destination 200.0.0.0**

**Default 200.0.0.3**

**Pc2**

**Route**

**Destination 202.0.0.0**

**Pc4**

**Route**

**Destination 200.0.0.0**

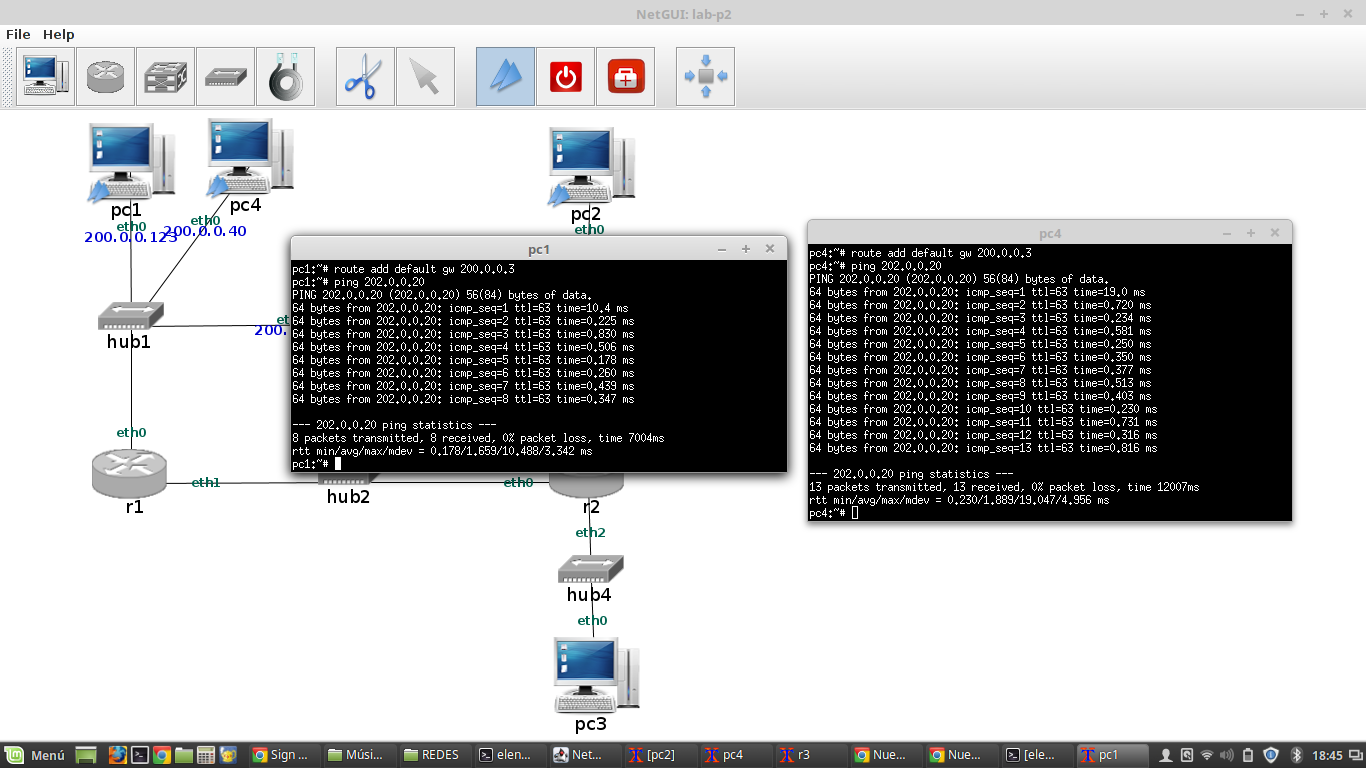
**R3**

**Route**

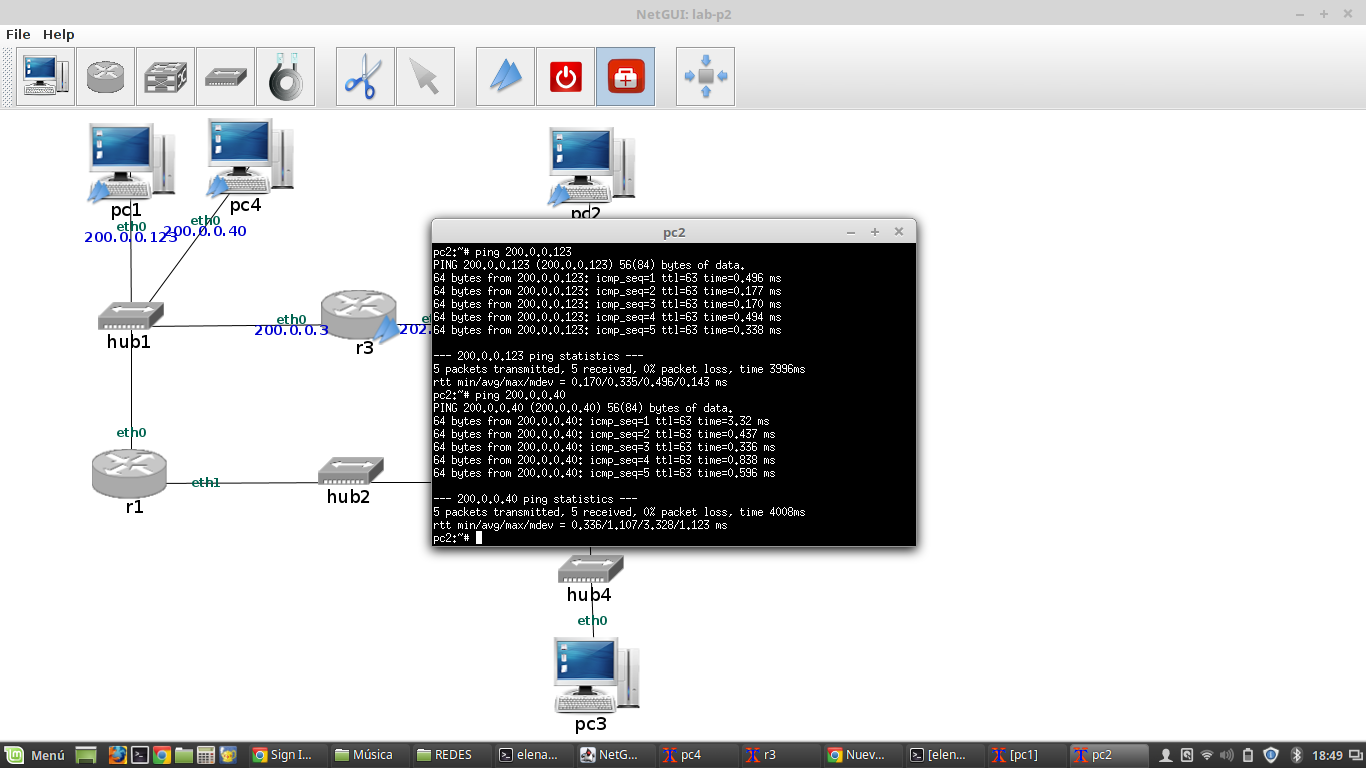
**Destination 200.0.0.0 eth0**

**Destination 202.0.0.0 eth1**

1. **Añade las rutas que consideres necesarias utilizando el comado route para que funcione un ping de pc1 a pc2 y de pc4 a pc2. Ten en cuenta que podrás utilizar, rutas de máquina, rutas de subred o ruta por defecto.**



1. **Indica si crees que con la configuración que has realizado funcionará un ping de pc2 a pc1 y de pc2 a pc4. Compruébalo.**



Funcionará porque para que editar es necesario editar de ida y de vuelta, por eso funciona.

* 1. **Capturas de tráfico**

**Antes de comenzar a realizar los siguientes ejercicios, espera al menos 10 minutos después de haber ejecutado el último ping del apartado anterior.**

1. **Consulta el estado de las cachés de ARP en los pcs y en el router. Explica su contenido.**
2. **Arranca en pc4 un tcpdump para capturar tráfico en su interfaz eth0, guardando la captura en un fichero (tal y como lo hiciste en la práctica 0).**
3. **Ejecuta en pc1 un ping a pc4 que envíe sólo 1 paquete ICMP Echo Request (ping -c 1 <máquinaDestino>).**
4. **Interrumpe la captura en pc4 (Ctrl+C).**
5. **Comprueba el estado de las cachés de ARP en pc1, pc4, pc2 y r3. Explica su contenido.**
6. **Arranca en un terminal de la máquina real la aplicación wireshark para cargar el fichero de captura que has obtenido. Observa los siguientes campos en los mensajes de la captura:**

**Mensaje de solicitud de ARP que envía pc1 a pc4.**

* **Dirección Ethernet destino**
* **Dirección Ethernet origen**
* **Tipo en la cabecera Ethernet**
* **Contenido del mensaje de solicitud de ARP: localiza el campo que contiene la dirección IP de la máquina sobre la que se está preguntando su dirección Ethernet.**

**Mensaje de respuesta de ARP que envía pc4 a pc1.**

* **Dirección Ethernet destino**
* **Dirección Ethernet origen**
* **Tipo en la cabecera Ethernet**
* **Contenido del mensaje de respuesta de ARP: localiza el campo que contiene la dirección Ethernet solicitada.**

**Datagrama IP que envía pc1 a pc4.**

* **Dirección Ethernet destino**
* **Dirección Ethernet origen**
* **Tipo en la cabecera Ethernet**
* **Dirección IP origen**
* **Dirección IP destino**
* **Campo TTL**

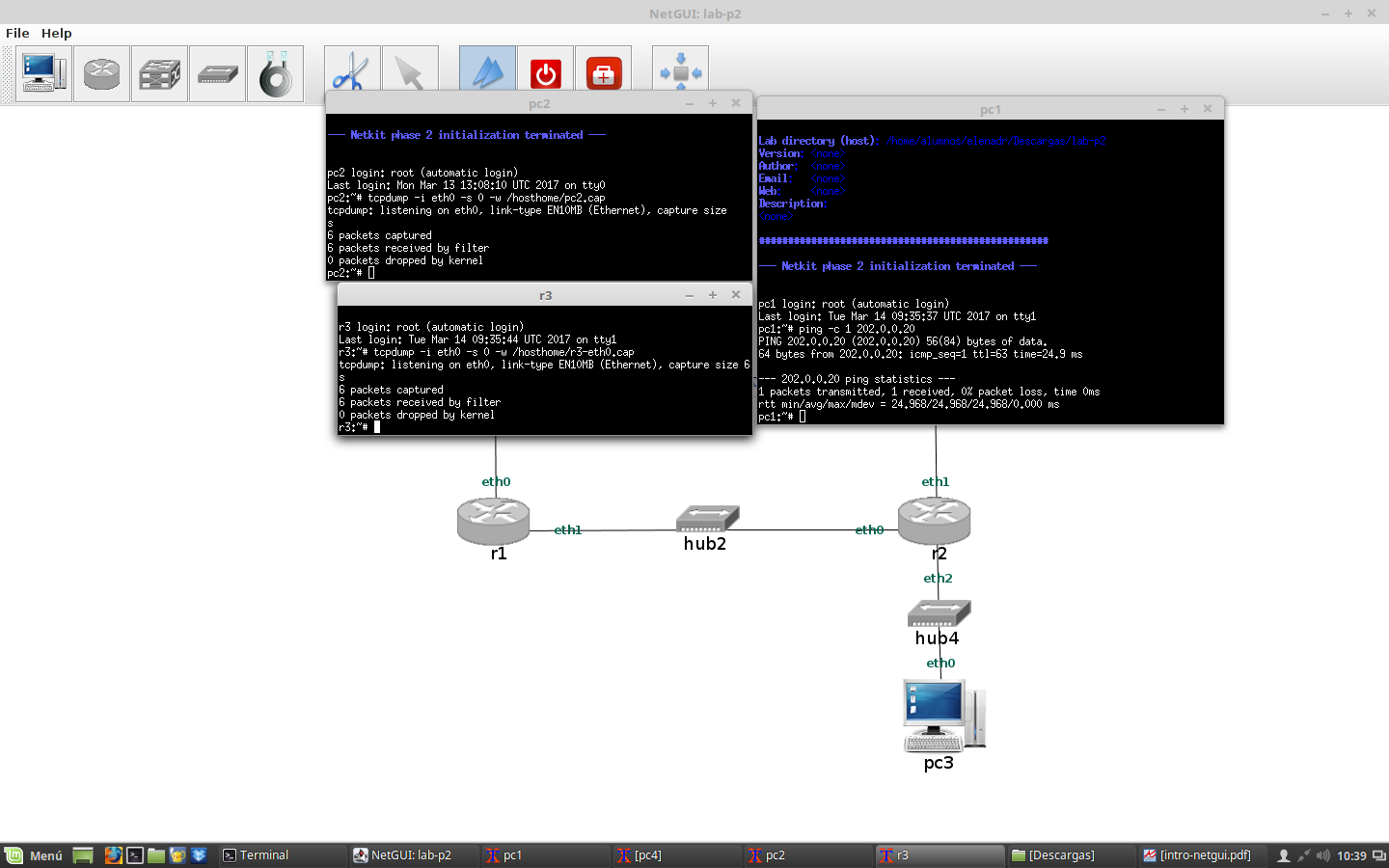
**Datagrama IP que envía pc4 a pc1.**

* + **Dirección Ethernet destino**
  + **Dirección Ethernet origen**
  + **Tipo en la cabecera Ethernet**
  + **Dirección IP origen**
  + **Dirección IP destino**
  + **Campo TTL**

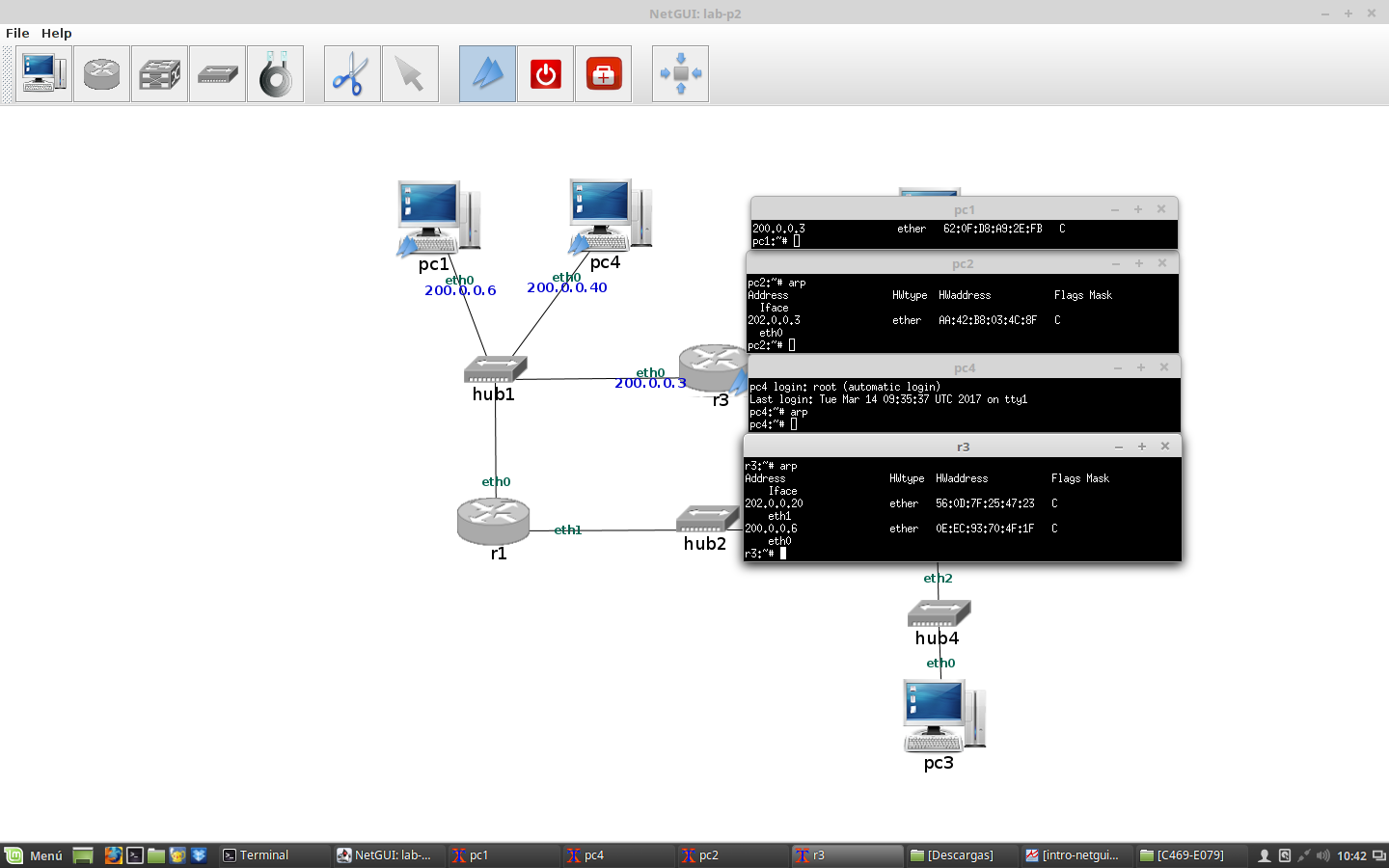
1. **Espera a que la caché de ARP de pc1 esté vacía. Ahora vamos a analizar el tráfico desde pc1 a pc2. ¿Cuántas capturas de tráfico crees que son necesarias para ver todos los paquetes que se generan en el escenario cuando se comunican pc1 y pc2?**

Por lo menos una.

1. **Arranca un tcpdump en r3(eth0) y en pc2 para ver todos los paquetes que se generan cuando pc1 y pc2 se comunican, guardando las capturas de tráfico en dos ficheros diferentes.**
2. **Ejecuta en pc1 un ping a pc2 que envíe sólo 1 paquete (ping -c 1 <máquinaDestino>).**
3. **Interrumpe las capturas (Ctrl+C).**

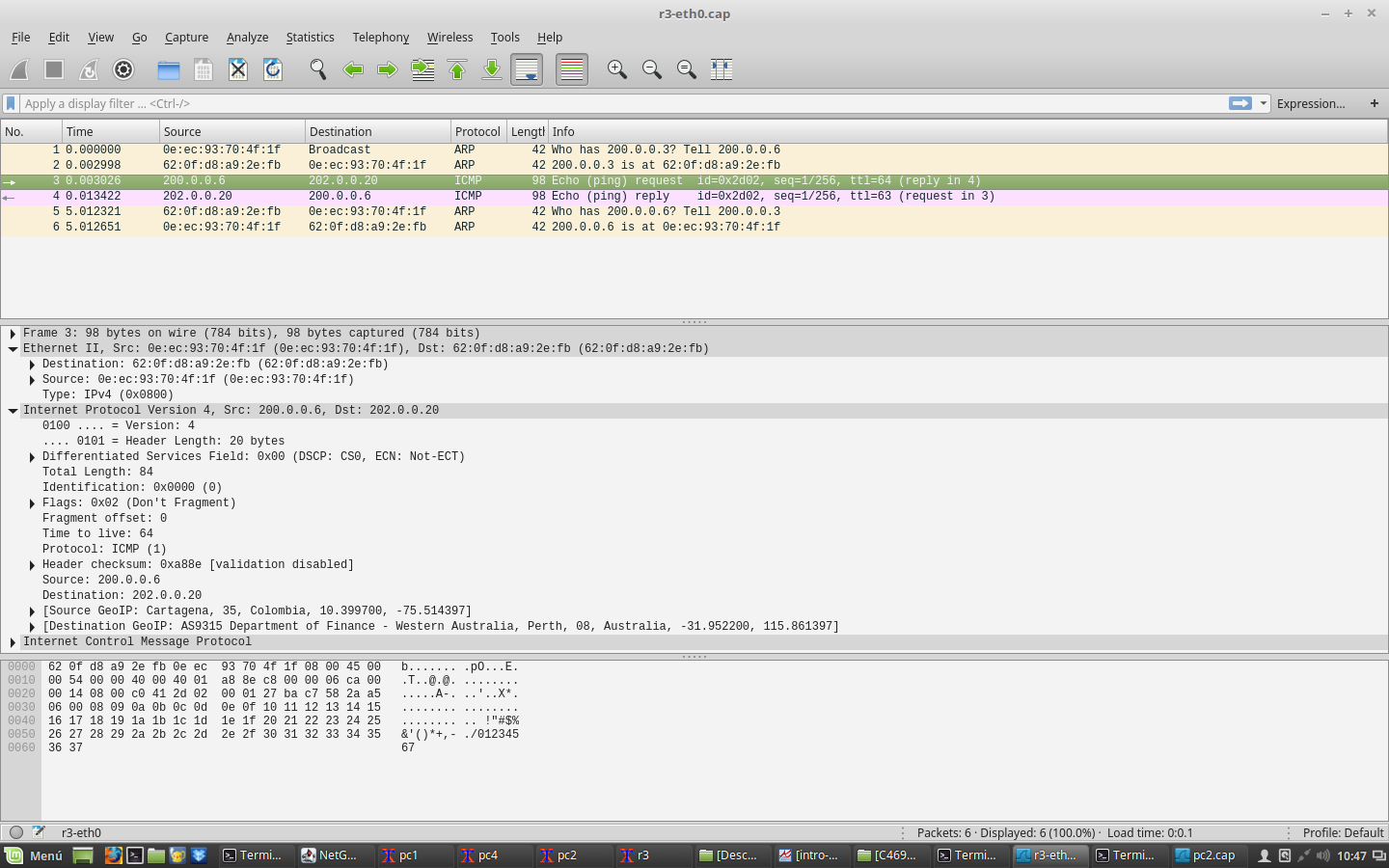
****

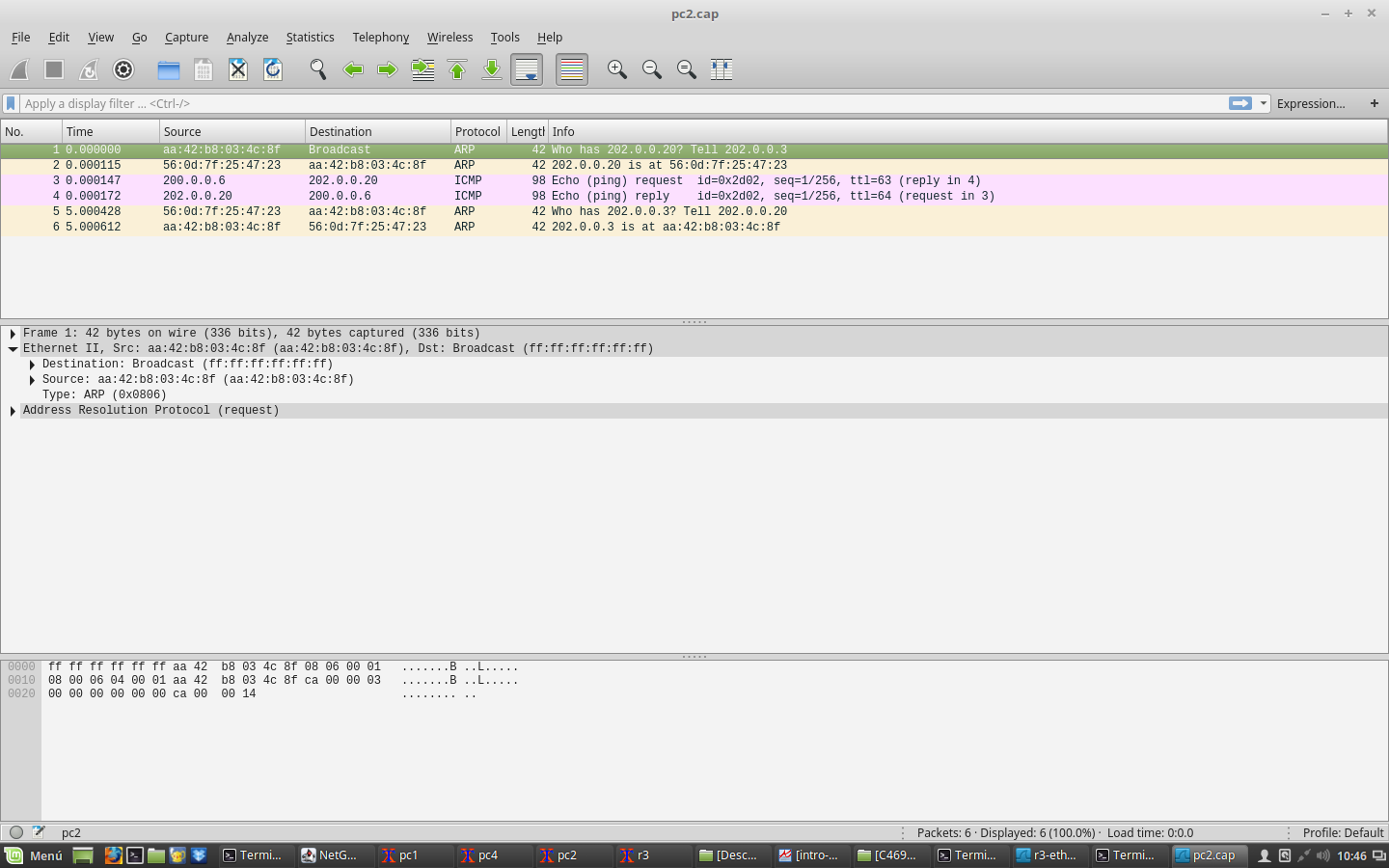
1. **Comprueba el estado de las cachés de ARP en pc1, pc2, pc4 y r3. Explica su contenido.**

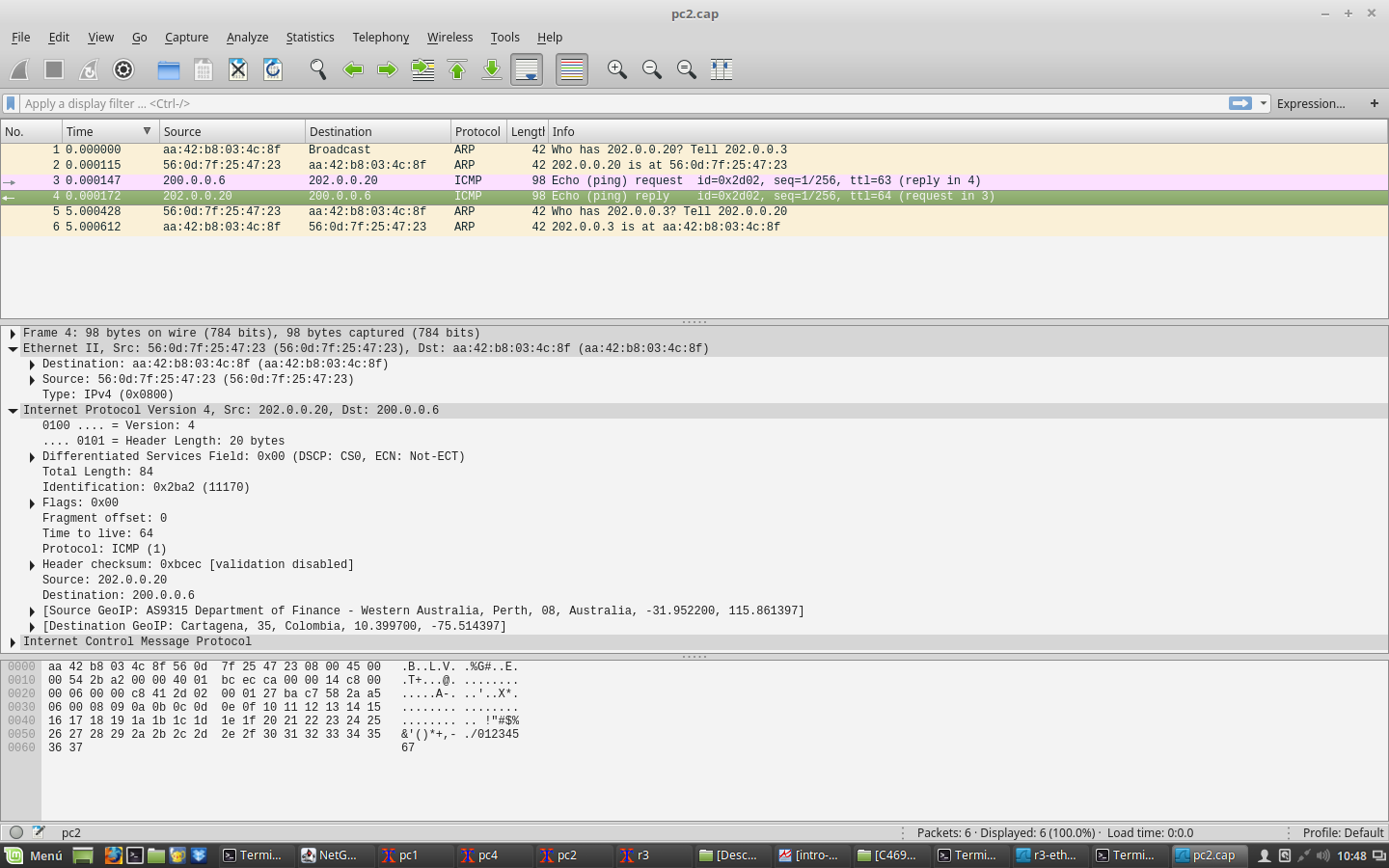
****

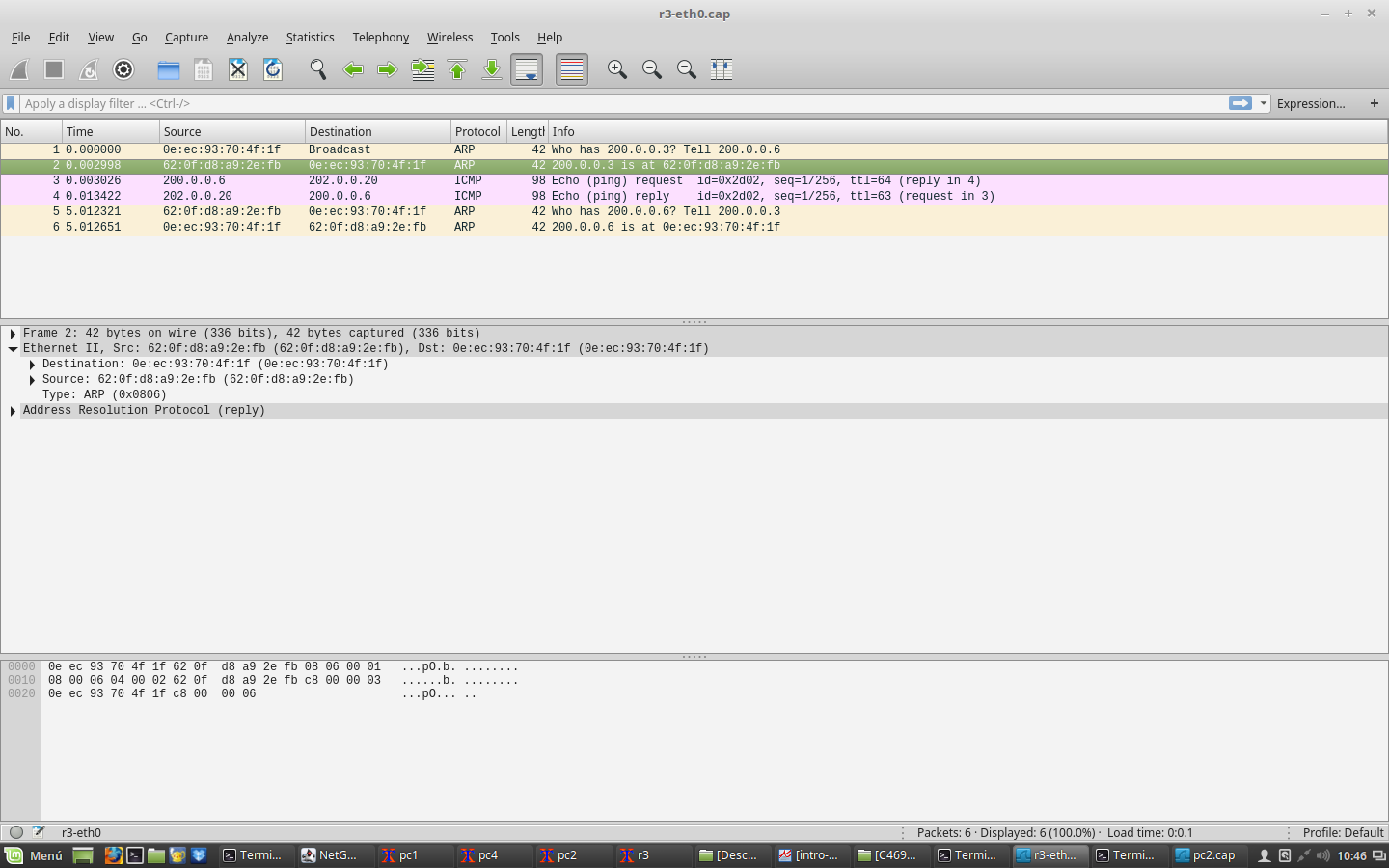
1. **Arranca en un terminal de la máquina real la aplicación wireshark para cargar el/los fichero/s de captura que has obtenido. Observa las capturas y construye una tabla por cada uno de los paquetes que se han capturado indicando el tipo y su contenido atendiendo a los siguientes campos:**

|  |  |
| --- | --- |
| **Mensajes ARP** | **Dirección Ethernet destino** |
|  | **Dirección Ethernet origen** |
|  | **Tipo en la cabecera Ethernet** |
|  | **Contenido del mensaje Ethernet** |
| **Datagramas IP** | **Dirección Ethernet destino** |
|  | **Dirección Ethernet origen** |
|  | **Tipo en la cabecera Ethernet** |
|  | **Dirección IP origen** |
|  | **Dirección IP destino** |
|  | **Campo TTL** |

****

****

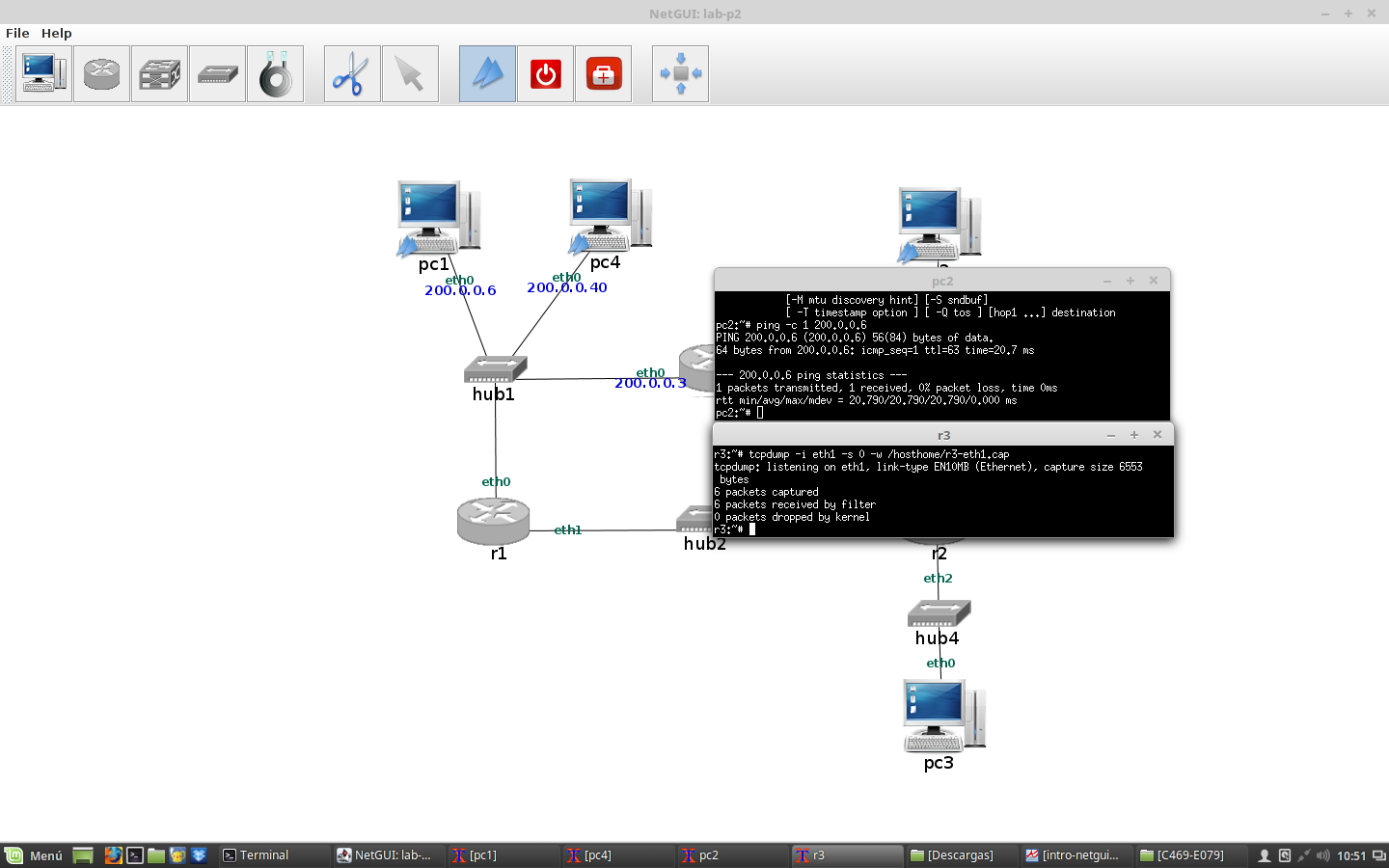
****

****

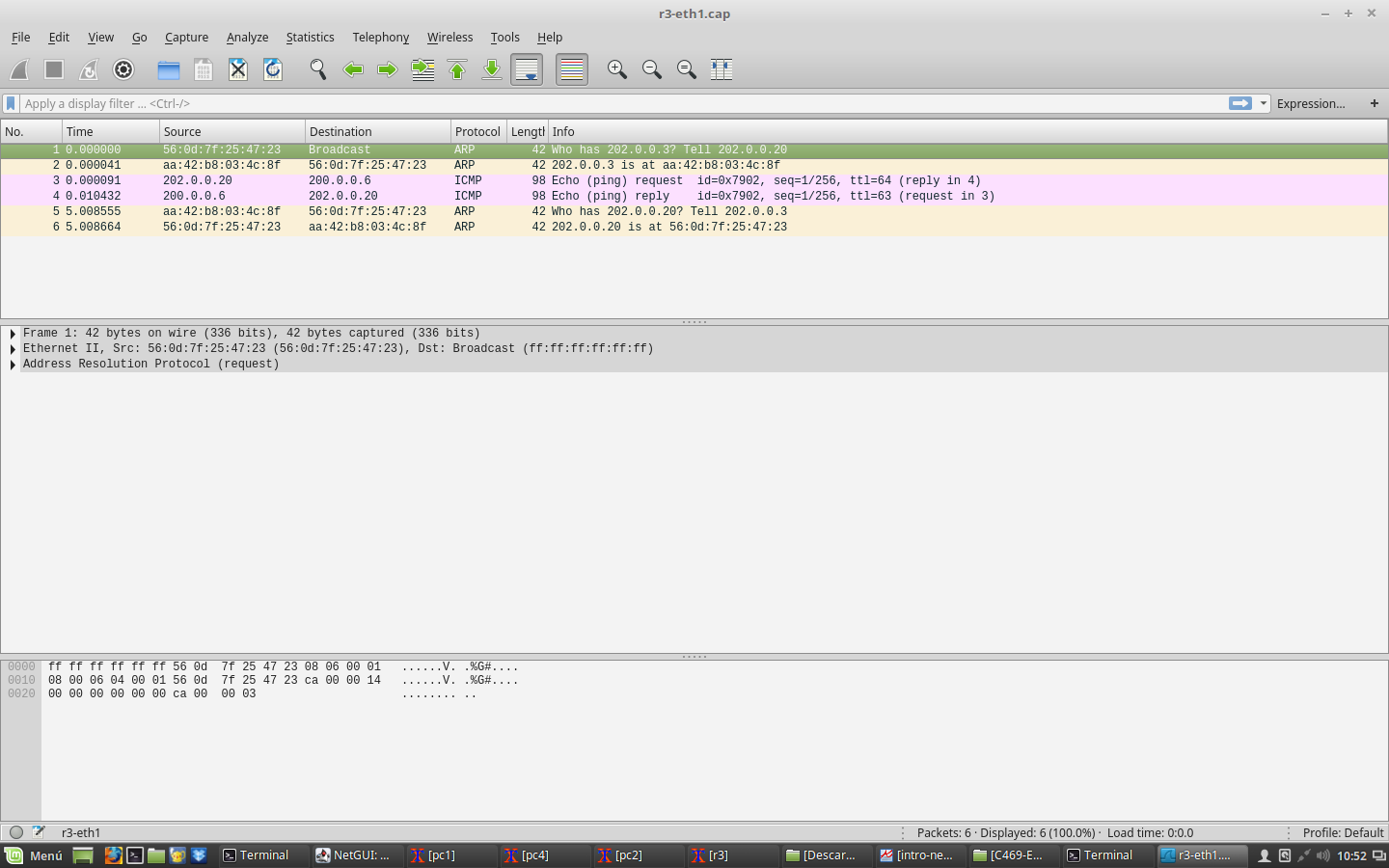
* 1. **Observa cómo un datagrama IP viaja por cada una de las subredes hacia el destino en tramas Ethernet diferentes. ¿Qué únicos campos de la cabecera IP cambian al atravesar diferentes subredes?**

Cambian el TTL.

* 1. **Espera a que la caché de ARP de pc2 esté vacía. Arranca en r3 un tcpdump para capturar tráfico en su interfaz eth1, guardando la captura en otro fichero diferente.**
  2. **Ejecuta en pc2 un ping a pc1 de forma que envíe sólo 1 paquete ICMP Echo Request (ping -c 1 <máquinaDestino>). A continuación ejecuta en pc2 un ping a pc4 de forma que envíe sólo 1 paquete ICMP Echo Request.**
  3. **Interrumpe la captura en r3(eth1) (Ctrl+C).**

****

* 1. **¿Cuántos mensajes ARP crees que se habrán capturado en el fichero? Compruébalo cargando el fichero de captura en el wireshark.**

****

1. Configuración de tablas de encaminamiento mediante ficheros

de configuración

Arranca el resto de las máquinas y routers de la figura y obtendrás un diagrama similar a la figura 2. Ten en cuenta que en pc1 ya tendrás configurada una dirección IP, mantén esta configuración.

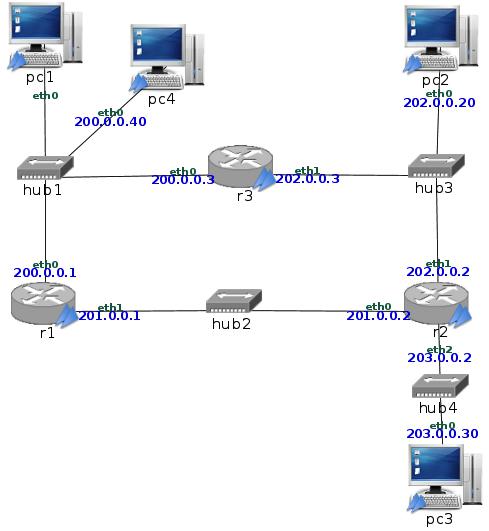


Figura 2: Todas las máquinas arrancadas

4

1. **¿Cuántas subredes observas en la figura? Escribe la dirección de cada una de estas subredes junto con su máscara.**

Hay cuatro subredes, y las direcciones son:

* network 200.0.0.0

netmask 255.255.255.0

* network 201.0.0.0

netmask 255.255.255.0

* network 202.0.0.0

netmask 255.255.255.0

* network 203.0.0.0

netmask 255.255.255.0

1. **Reinicia las máquinas pc1, pc2 y pc4.**
2. **Consulta las tablas de encaminamiento en todas las máquinas y routers, comprobarás que las rutas que configuraste en el apartado anterior han desaparecido. Los pcs y routers sólo tienen ruta a las subredes a las que están directamente conectados. Por tanto sólo se podrán comunicar con las máquinas con las que son vecinas.**

1. **Con la configuración actual, indica qué máquinas se pueden comunicar entre sí, especificando sus direcciones IP.**

Pc1 200.0.0.9 se comunica con:

pc4 200.0.0.40

r1(eth0) 200.0.0.1

r3 (eth0)200.0.0.3

pc2 202.0.0.20 se comunia con:

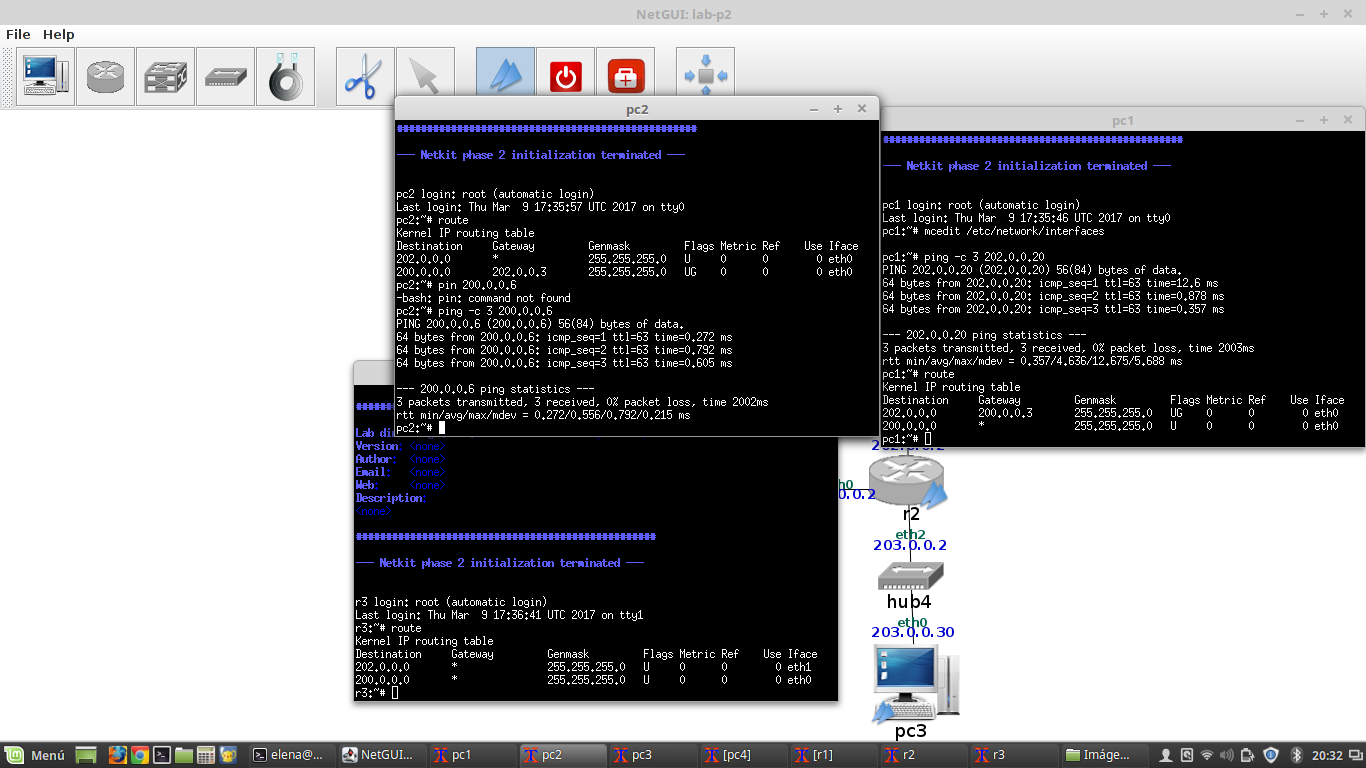
r3 (eth1) 202.0.0.

1. **Modifica el fichero /etc/network/interfaces en los ordenadores y en los routers de la red de forma que funcionen las siguientes rutas. Podrás utilizar rutas de máquina, de subred o rutas por defecto:**

**a) Conectividad entre pc1 y pc2 en los dos sentidos, a través de las siguientes rutas:**

**pc1)r3)pc2 pc2)r3)pc1**

**Ejecuta en pc1 la orden ping -c 3 <dirIPpc2> para comprobar si hay conectividad entre las máquinas. Para verificar que el camino es el descrito previamente, deberás ejecutar route en pc1 y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar pc2. Esta entrada debería indicar que el siguiente salto es r3. A continuación en r3 deberás ejecutar route y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar pc2. Esta entrada debería indicar que r3 no necesita ningún router adicional para alcanzar pc2.**

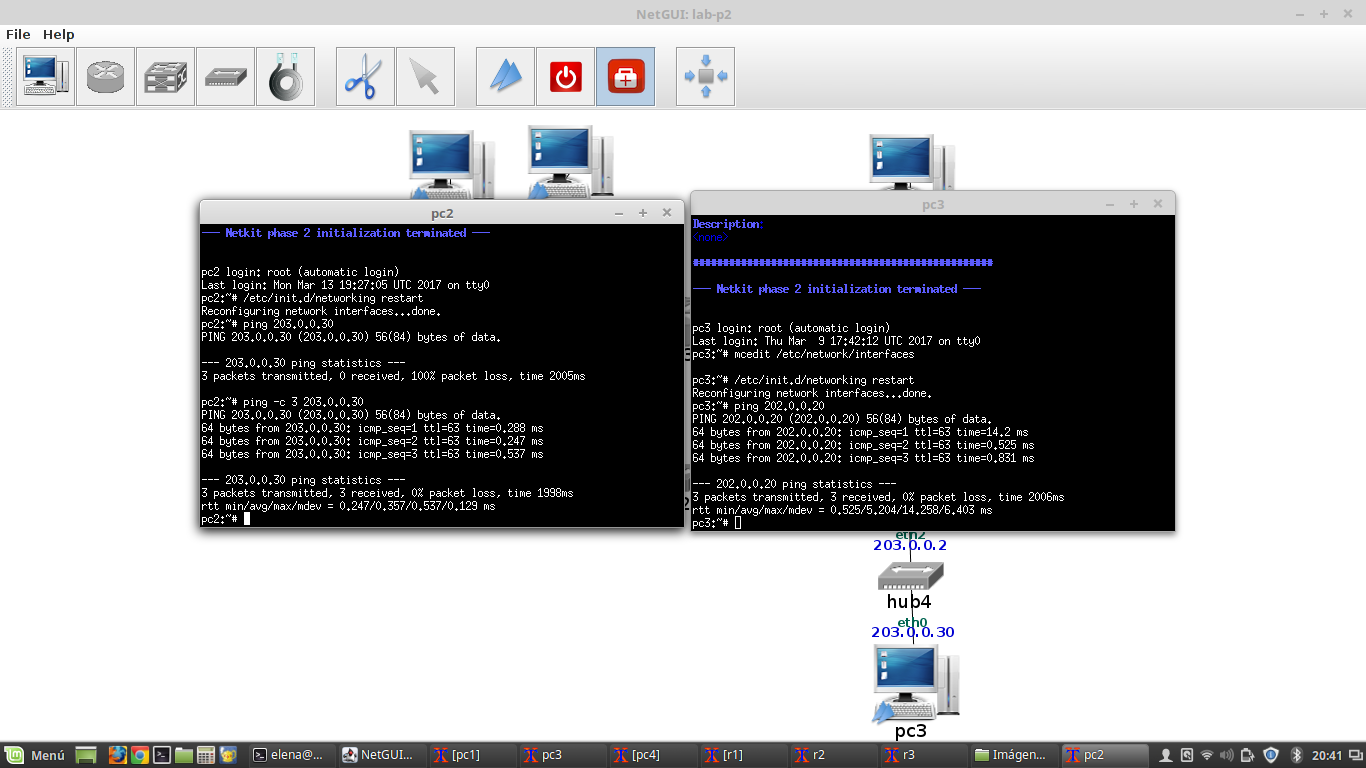
****

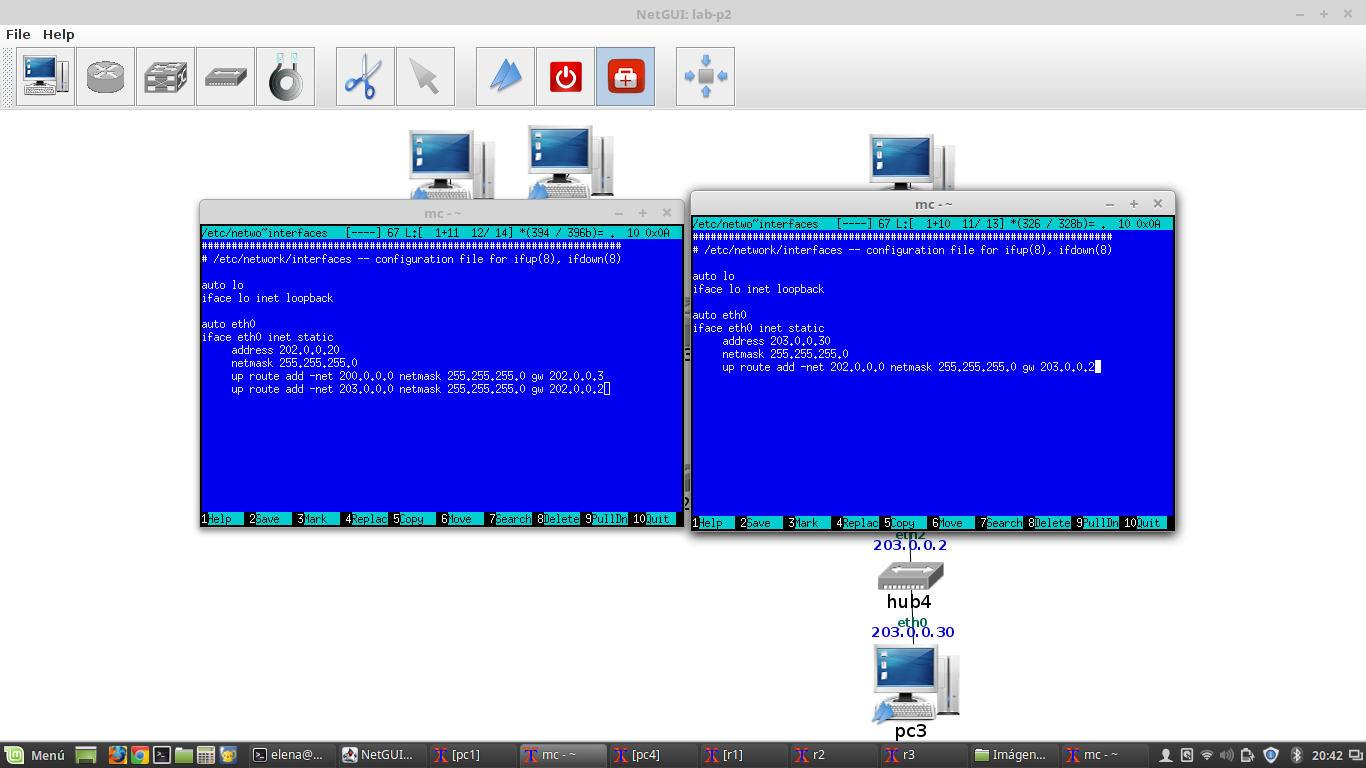
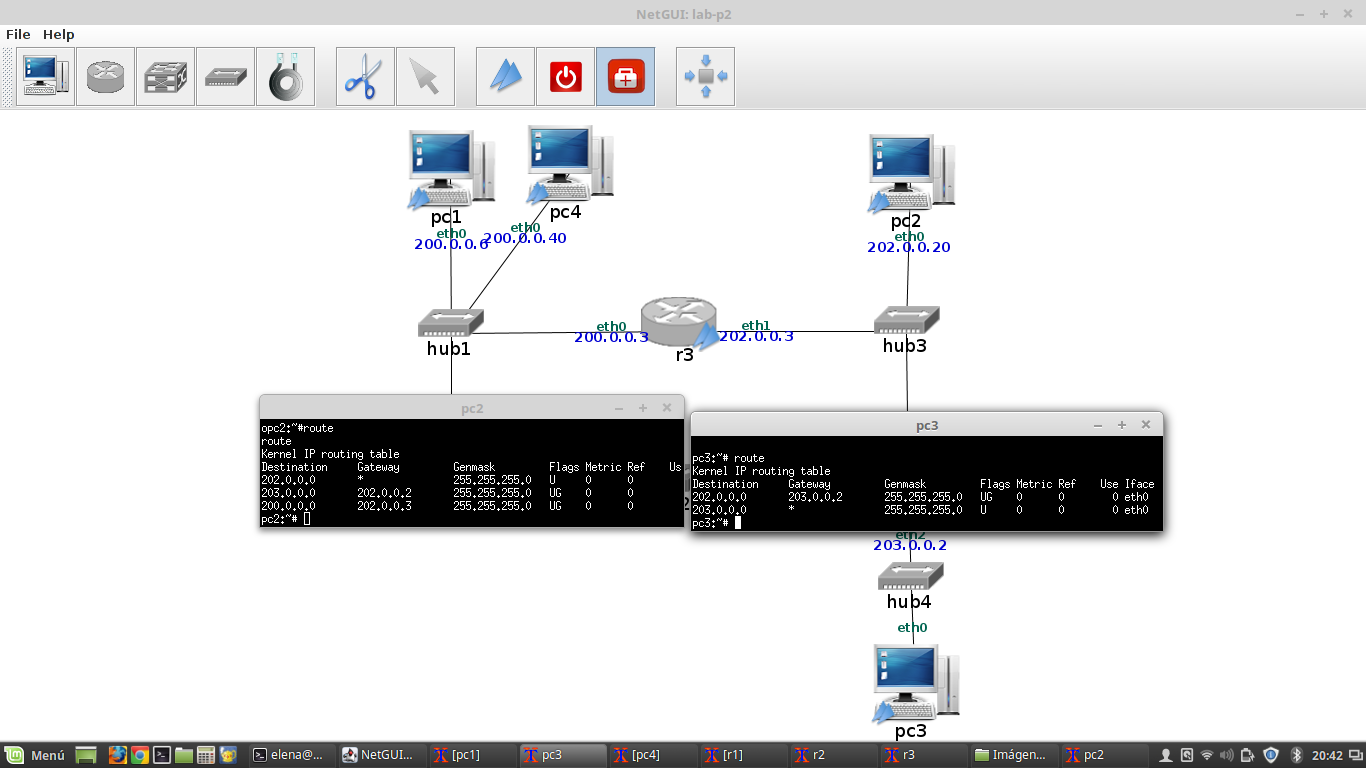
**b) Conectividad entre pc2 y pc3 en los dos sentidos, a través de la siguientes rutas:**

**pc2)r2)pc3**

**pc3)r2)pc2**

**Ejecuta en pc2 la orden ping -c 3 <dirIPpc3> para comprobar si hay conectividad entre las máquinas. Para verificar que el camino es el descrito previamente, deberás ejecutar route en pc2 y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar pc3. Esta entrada debería indicar que el siguiente salto es r2. A continuación en r2 deberás ejecutar route y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar pc3. Esta entrada debería indicar que r2 no necesita ningún router adicional para alcanzar pc3.**

**De forma análoga deberás consultar las tablas de encaminamiento en el sentido pc3)r2)pc2.**

****

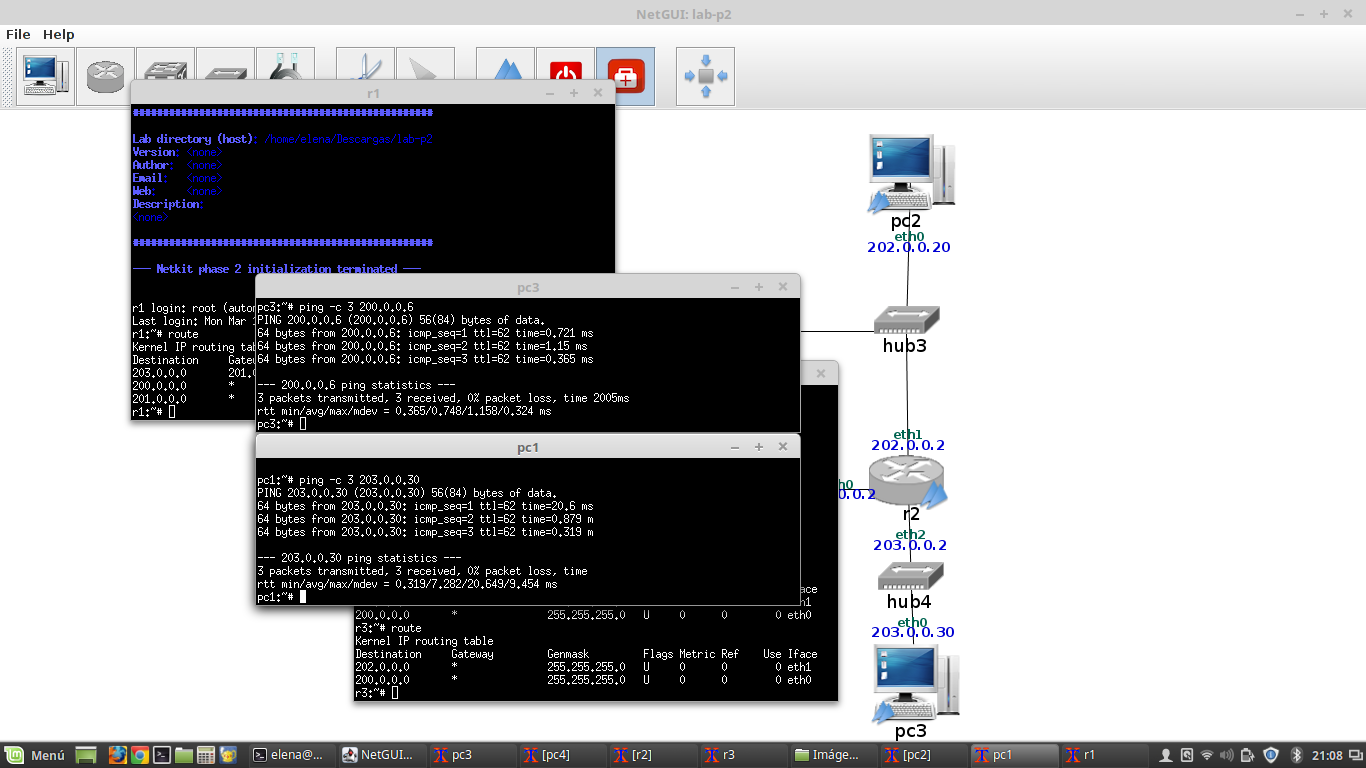
**c) Conectividad entre pc1 y pc3 en los dos sentidos, a través de las siguientes rutas:**

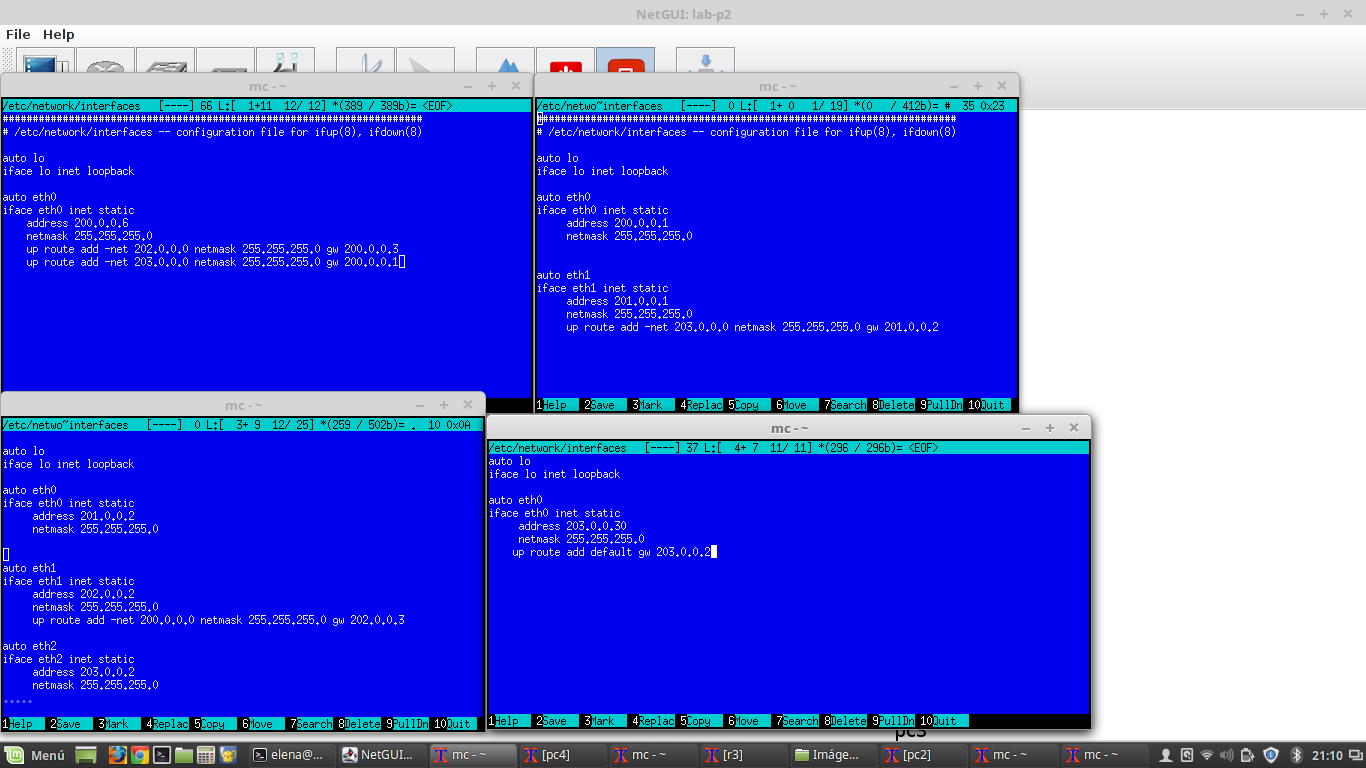
**pc1)r1)r2)pc3**

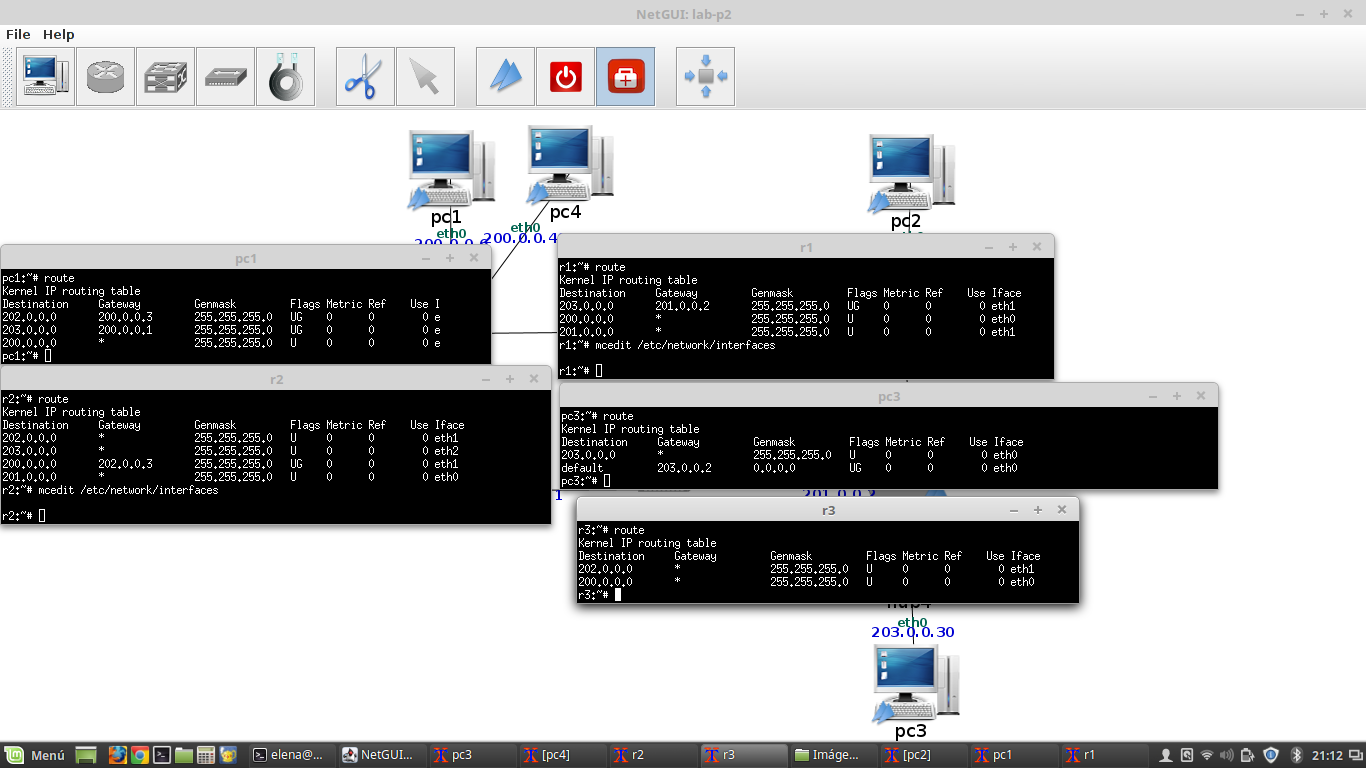
**pc3)r2)r3)pc1**

**Ejecuta en pc1 la orden ping -c 3 <dirIPpc3> para comprobar si hay conectividad entre las máquinas. Para verificar que el camino es el descrito previamente, deberás ejecutar route**

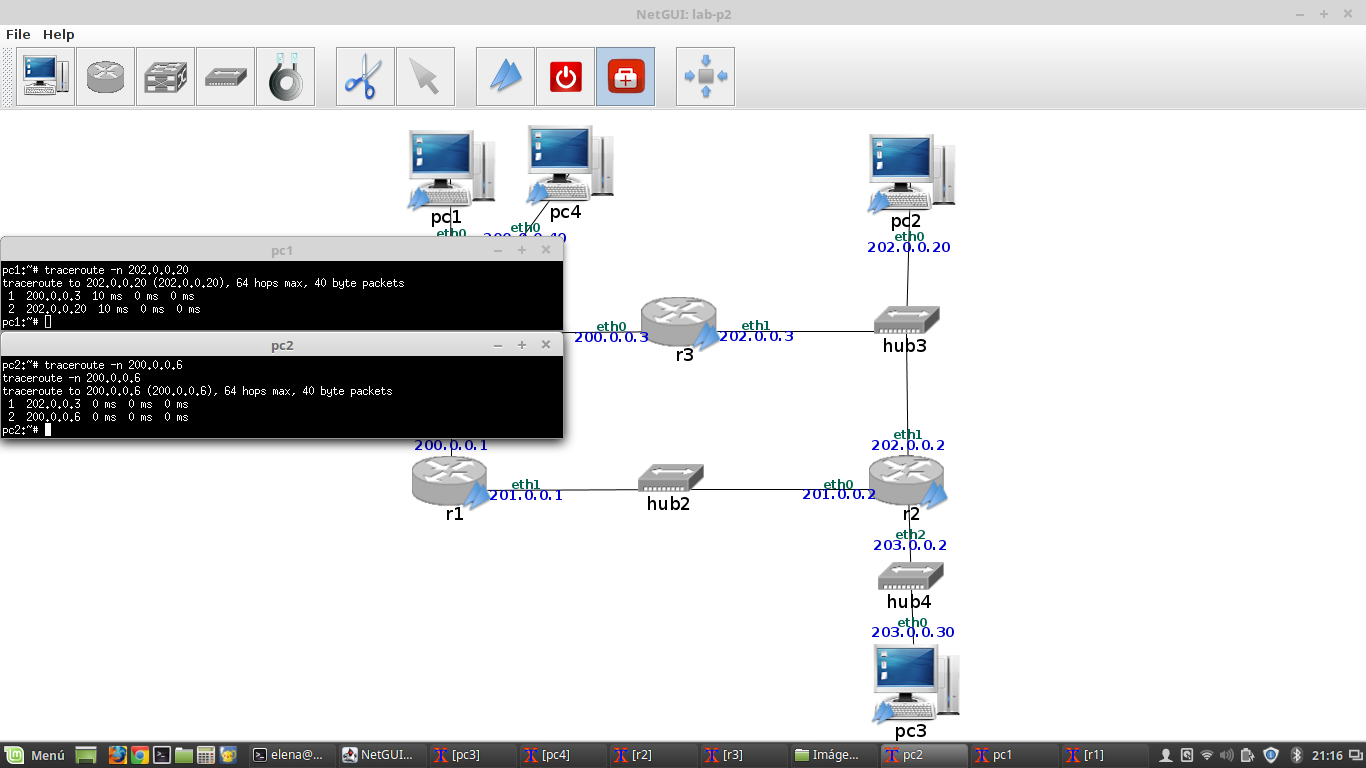
**en pc1 y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar pc3. Esta entrada debería indicar que el siguiente salto es r1. Después, deberás ejecutar route en r1 y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar pc3. Esta entrada debería indicar que el siguiente salto es r2. A continuación en r2 deberás ejecutar route y observar qué entrada de la tabla de encaminamiento se utiliza cuando se desea alcanzar pc3. Esta entrada debería indicar que r2 no necesita ningún router adicional para alcanzar pc3.**

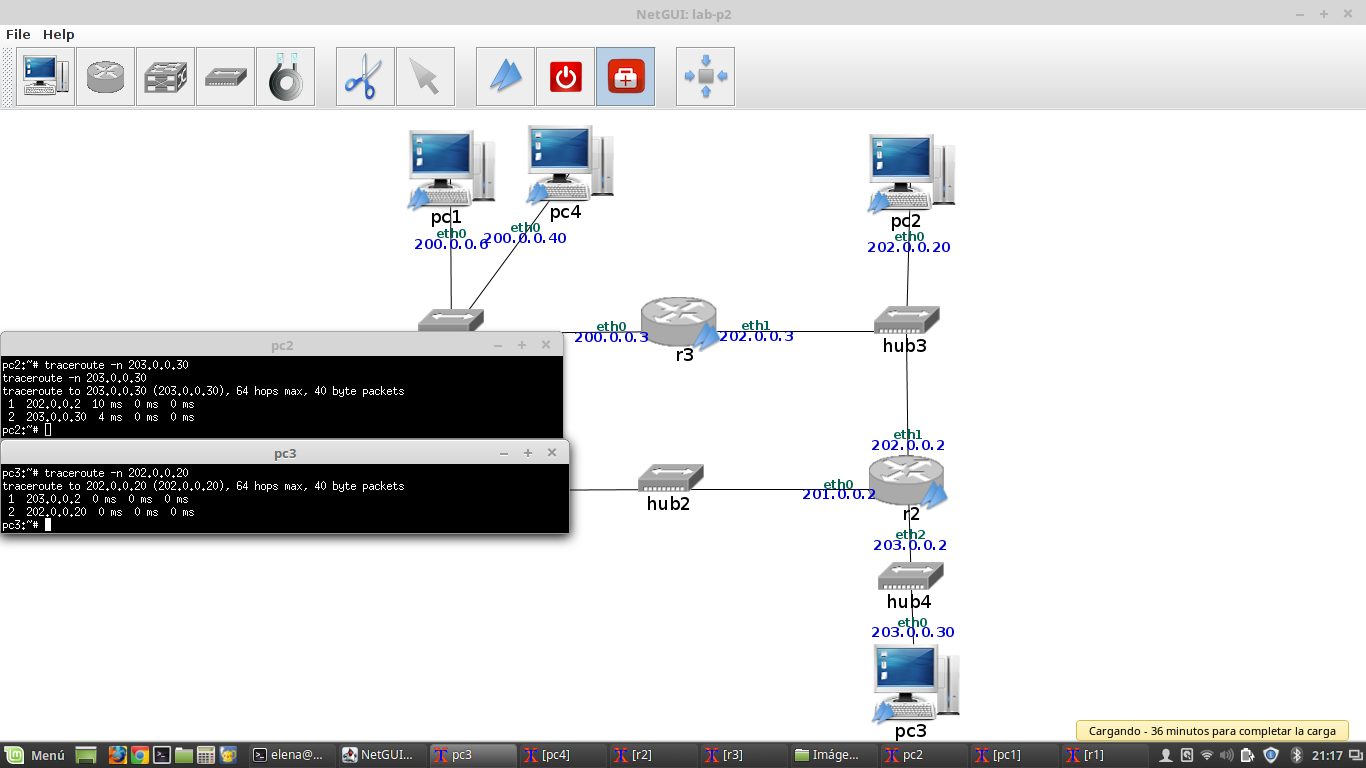


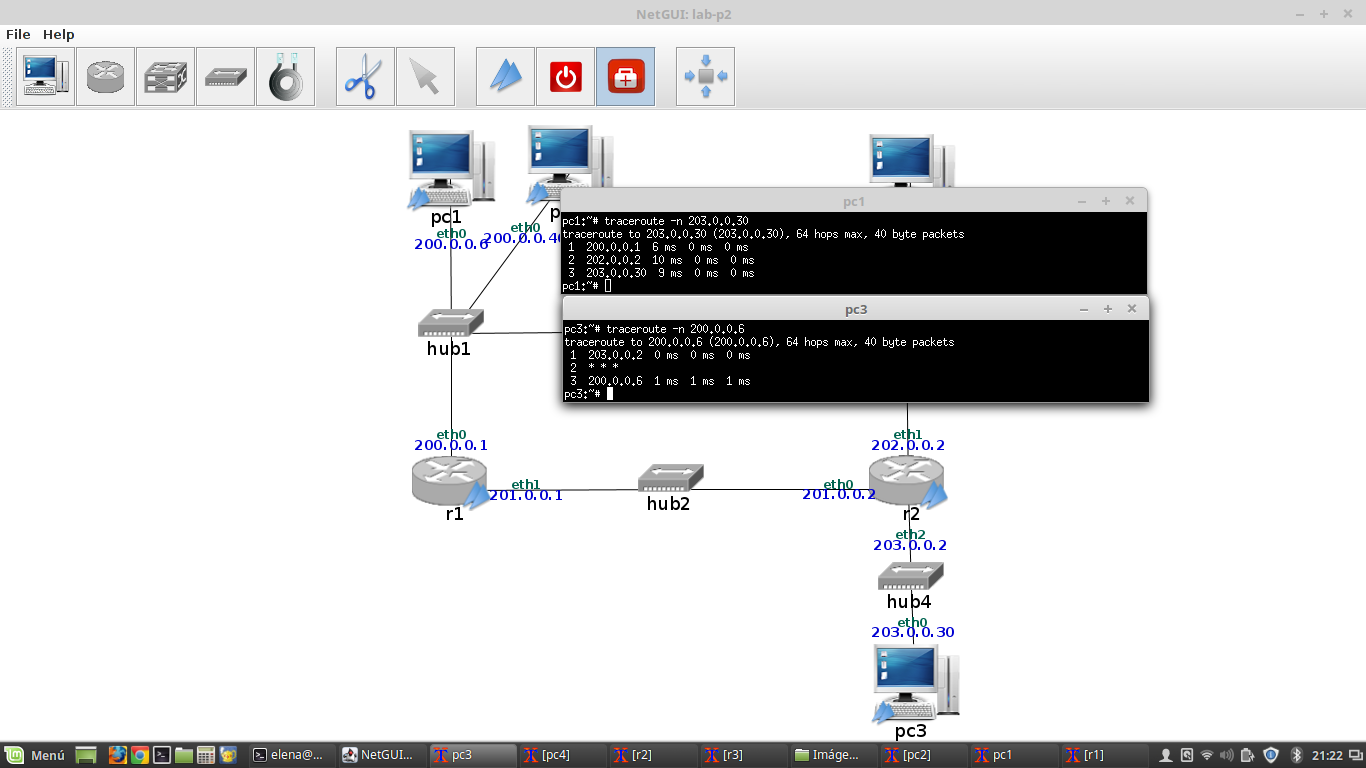




1. **Ejecuta en pc1 un traceroute hacia pc2 y en pc2 uno hacia pc1 para comprobar que las rutas son las especificadas.**

****

1. **Ejecuta en pc2 un traceroute hacia pc3 y en pc3 uno hacia pc2 para comprobar que las rutas son las especificadas.**
2. **Ejecuta en pc1 un traceroute hacia pc3 y en pc3 uno hacia pc1 para comprobar que las rutas son las especificadas. En este último traceroute observarás que aparecen unos \*. ¿A qué crees que se debe? En la Práctica 3 se estudiarán más en detalle este tipo de casos.**

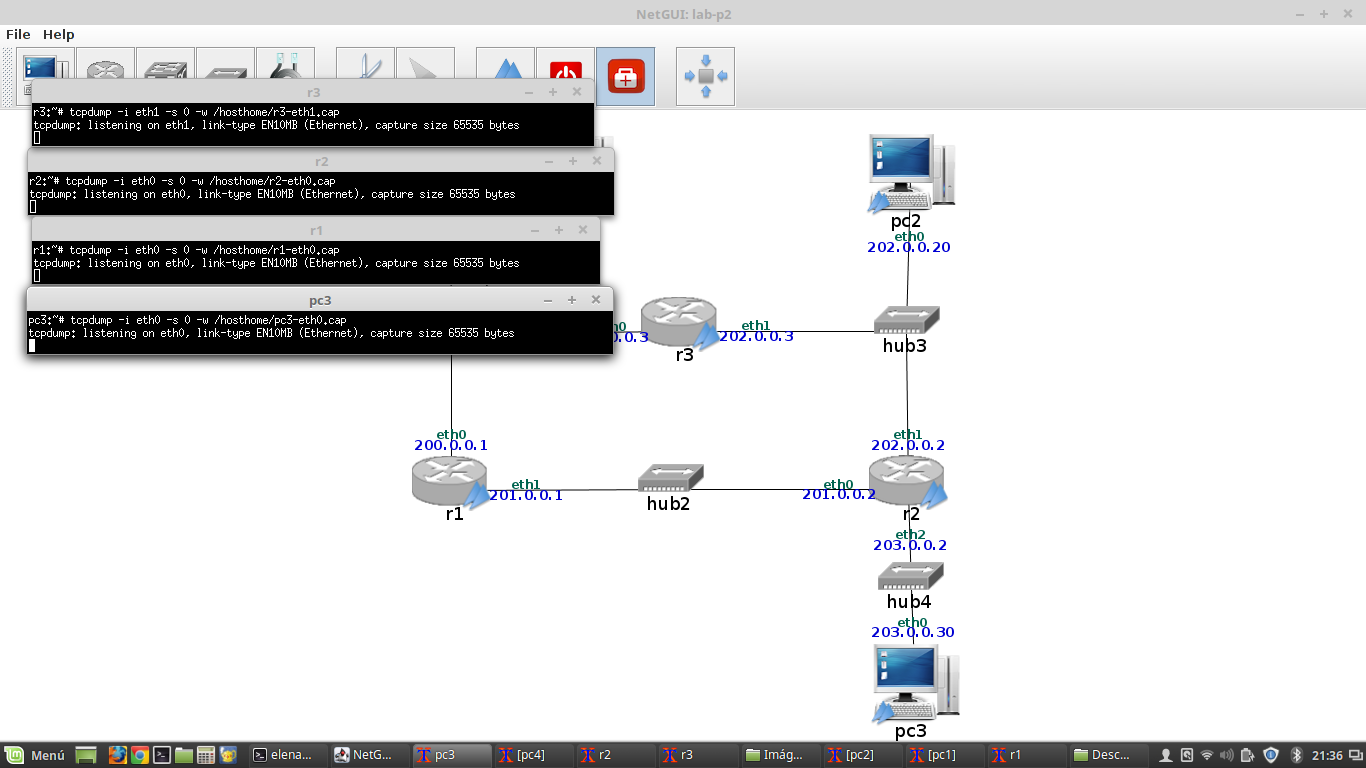
****

Los \*\*\* significan que no llega nada, porque no esta bien la tabla de encaminamiento.

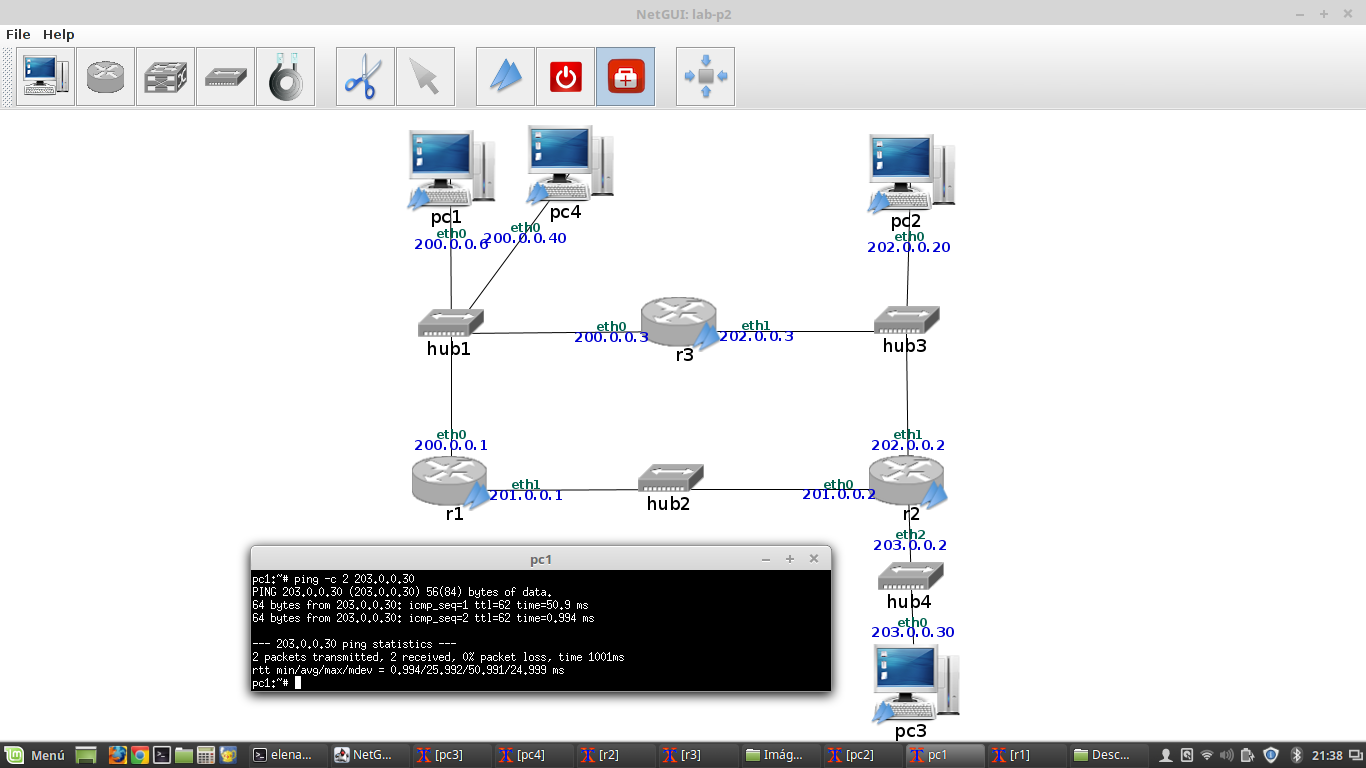
1. **Capturas de tráfico**

**Antes de comenzar a realizar los siguientes ejercicios asegúrate de que las rutas entre las máquinas son las especificadas en el apartado anterior.**

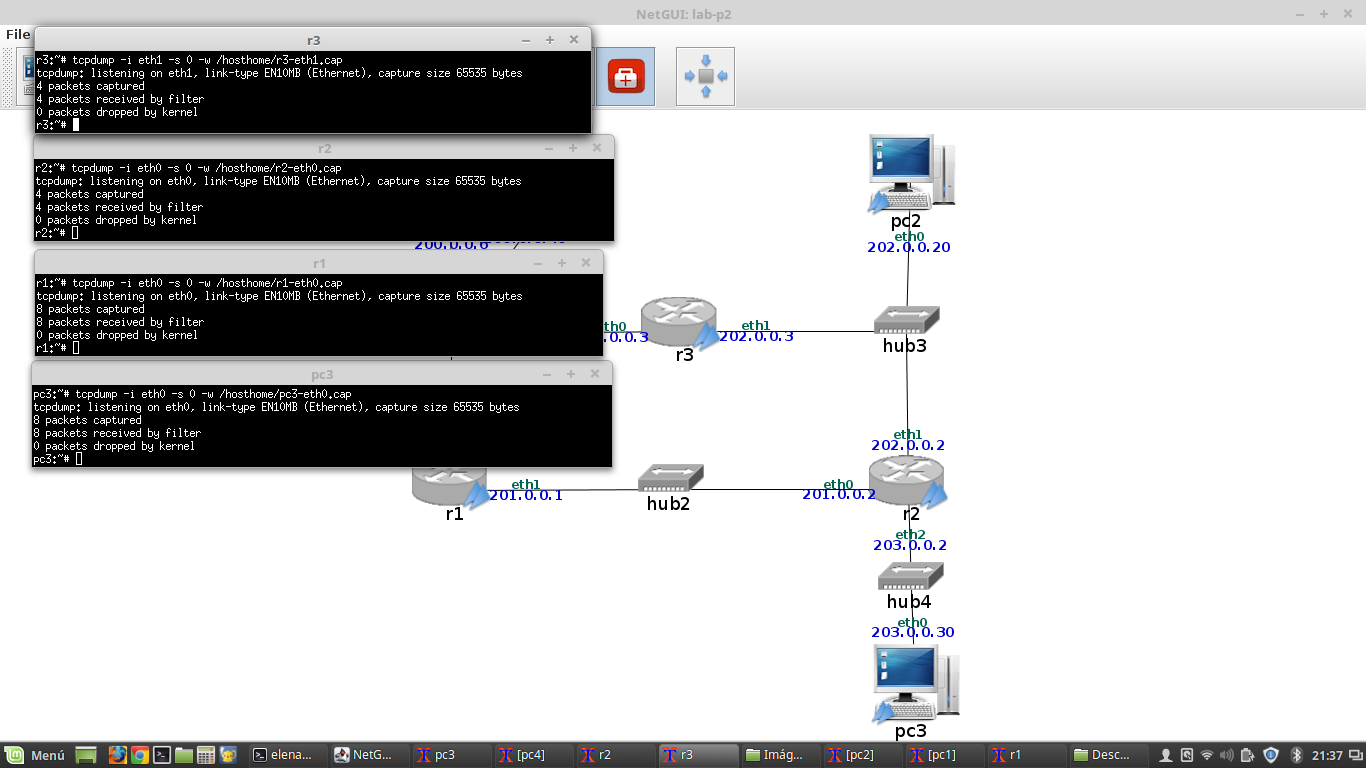
1. **Lanza tcpdump, almacenando los paquetes capturados en ficheros diferentes, capturando tráfico en las si-guientes interfaces: r1(eth0), r2(eth0), en r3(eth1) y pc3(eth0).**



1. **Ejecuta en pc1 un ping a pc3 que envíe sólo 2 paquetes (ping -c 2 <máquinaDestino>).**



1. **Interrumpe las 4 capturas (Ctrl+C).**

****

1. **En un terminal de la máquina real lanza la aplicación wireshark 4 veces, una con cada fichero, para poder ver simultáneamente las distintas capturas. Observa en las capturas cómo los datagramas IP que se envían y reciben con la orden ping contienen un mensaje de ICMP. Comprueba en estos datagramas:**

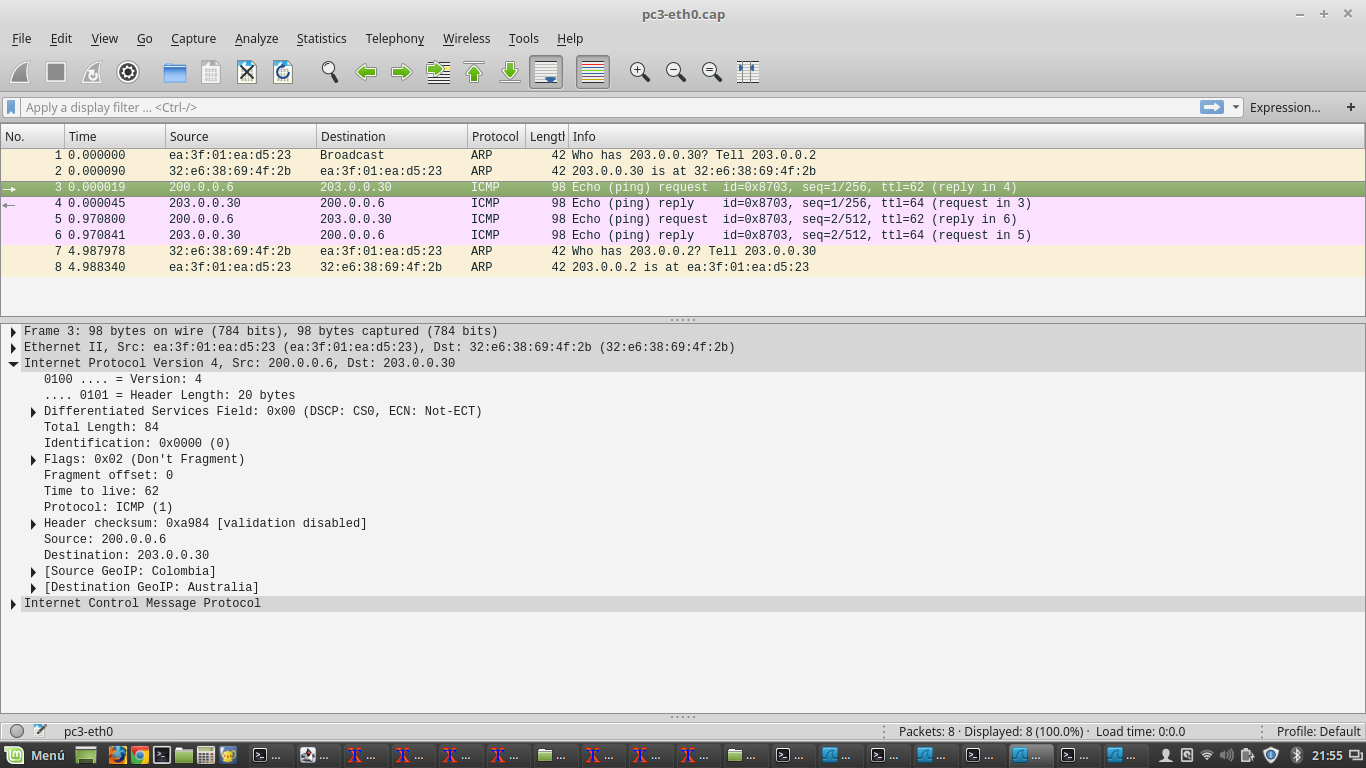
**Dirección IP origen**

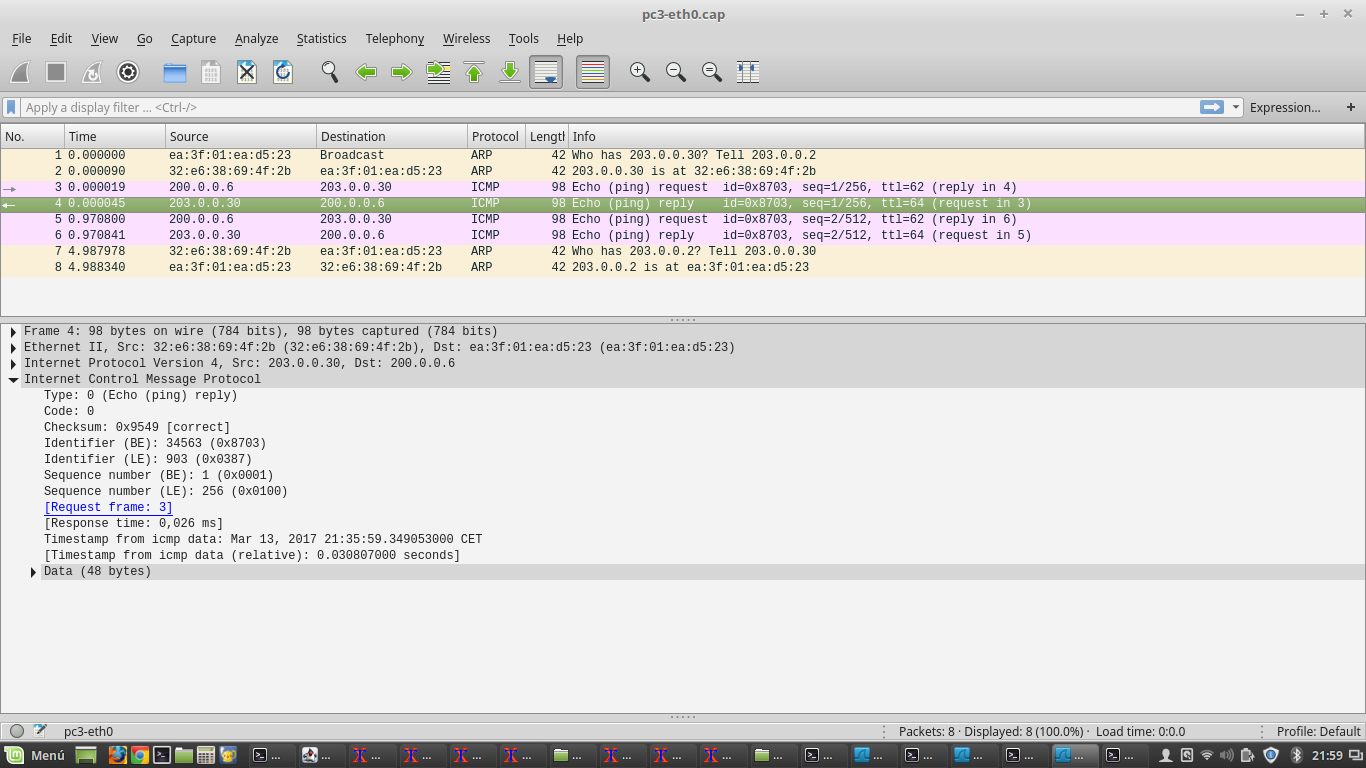
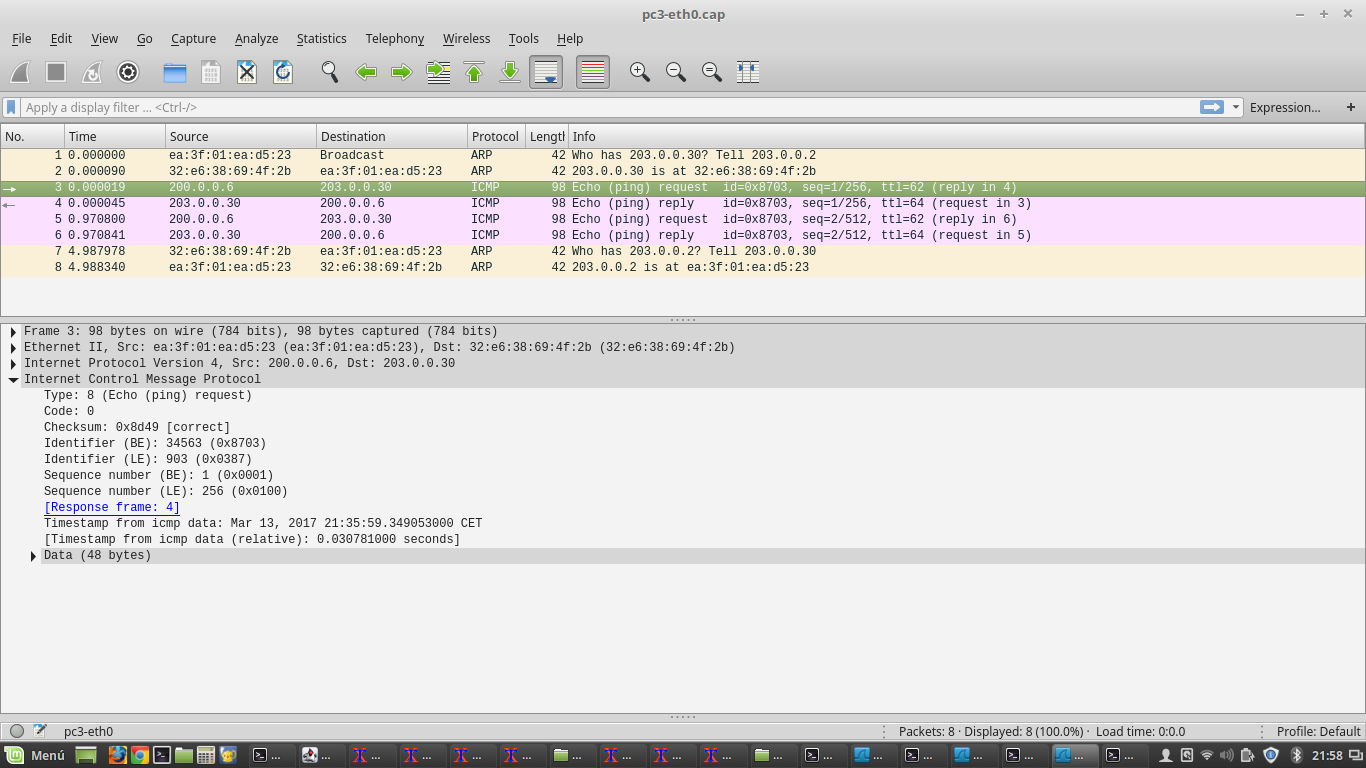
**Dirección IP destino**

**TTL en la cabecera IP**

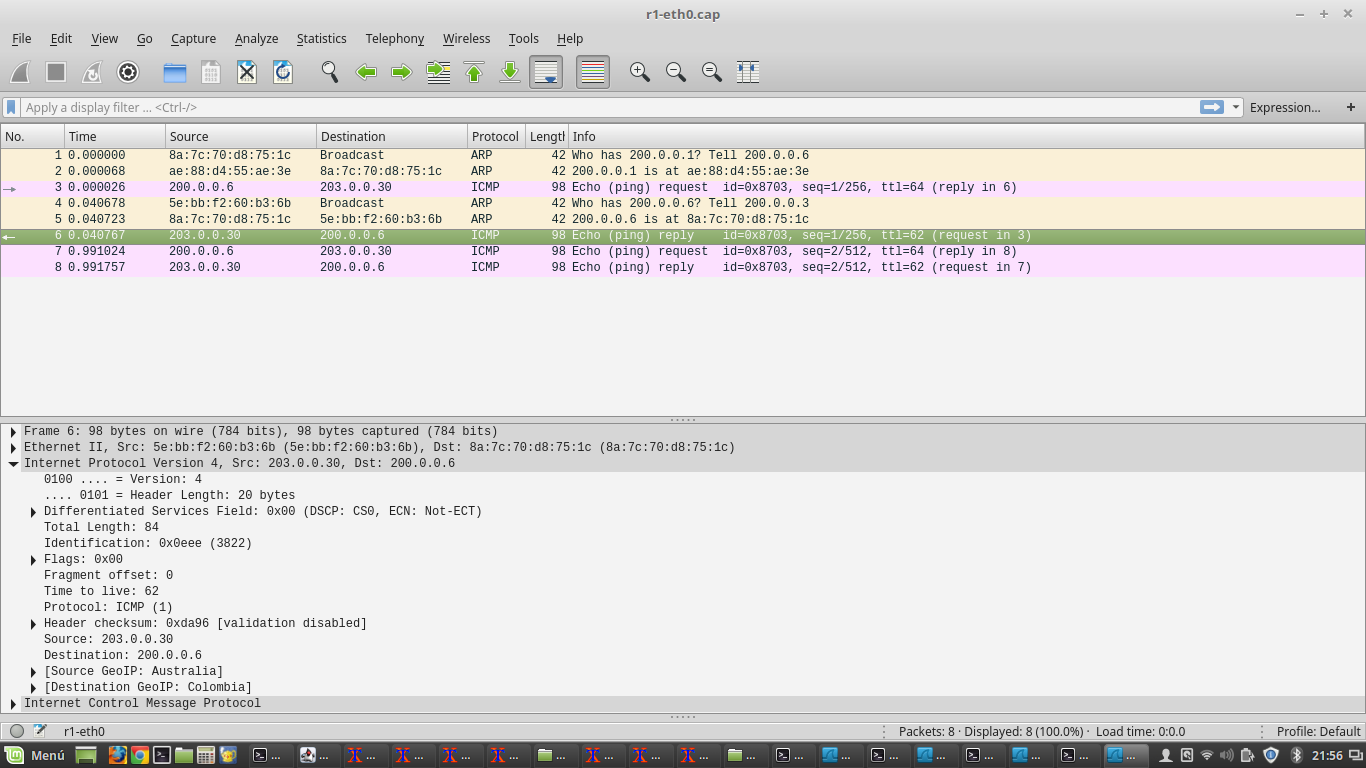
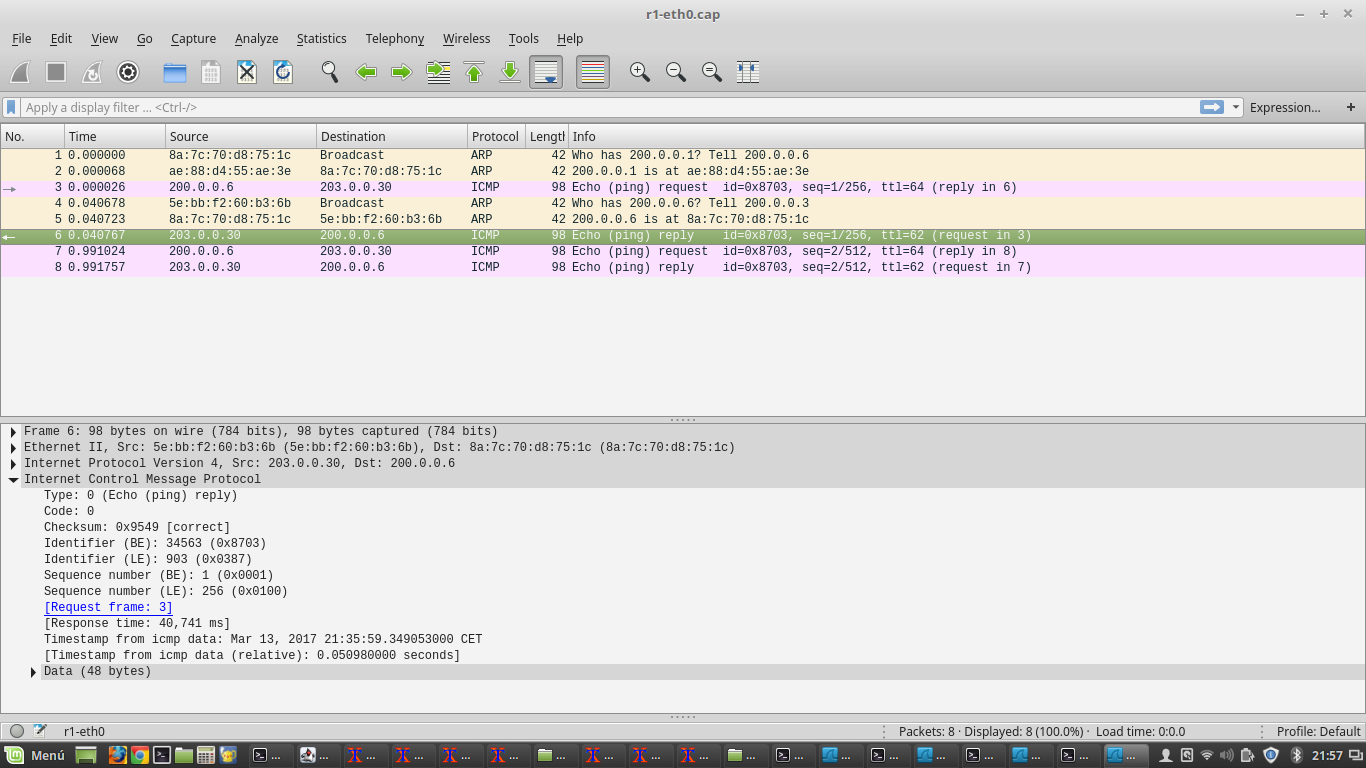
**Tipo de Protocolo en la cabecera IP**

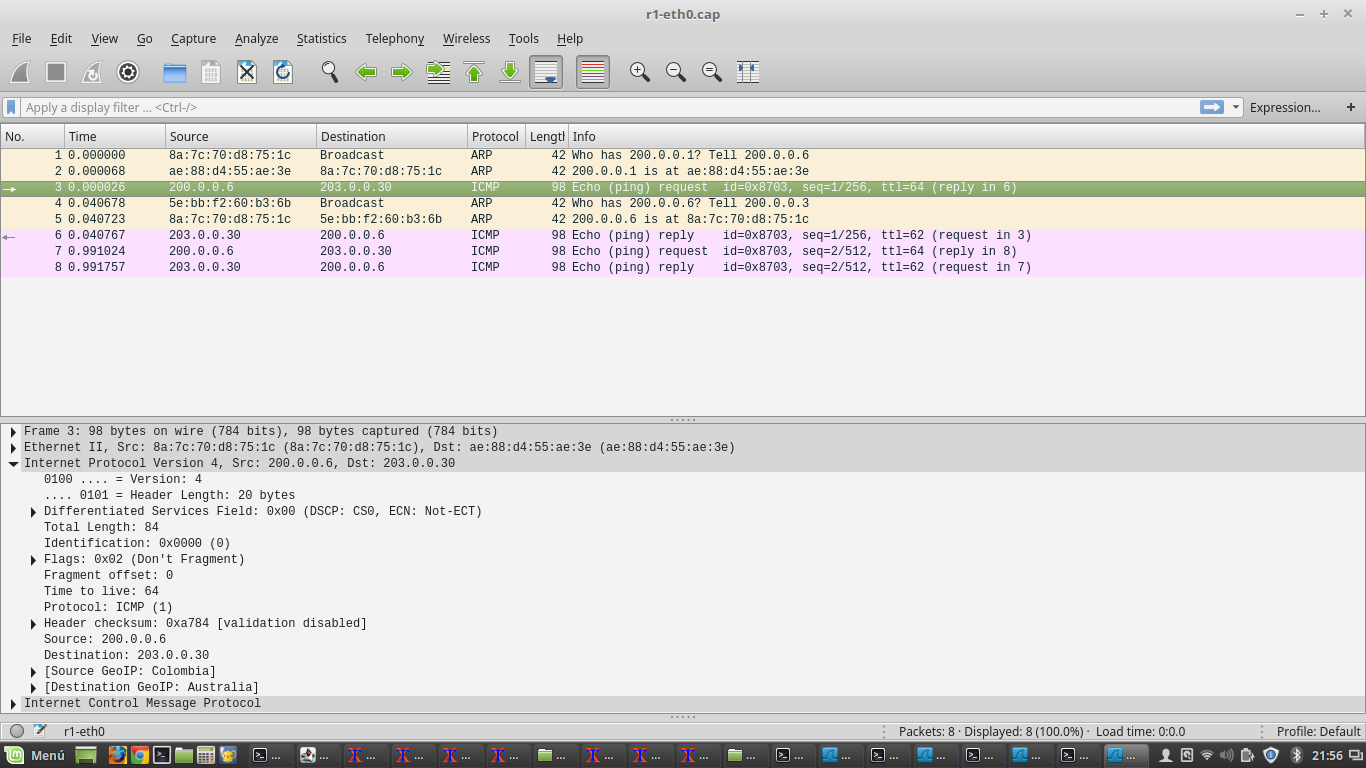
**Tipo y Código en la cabecera ICMP.**

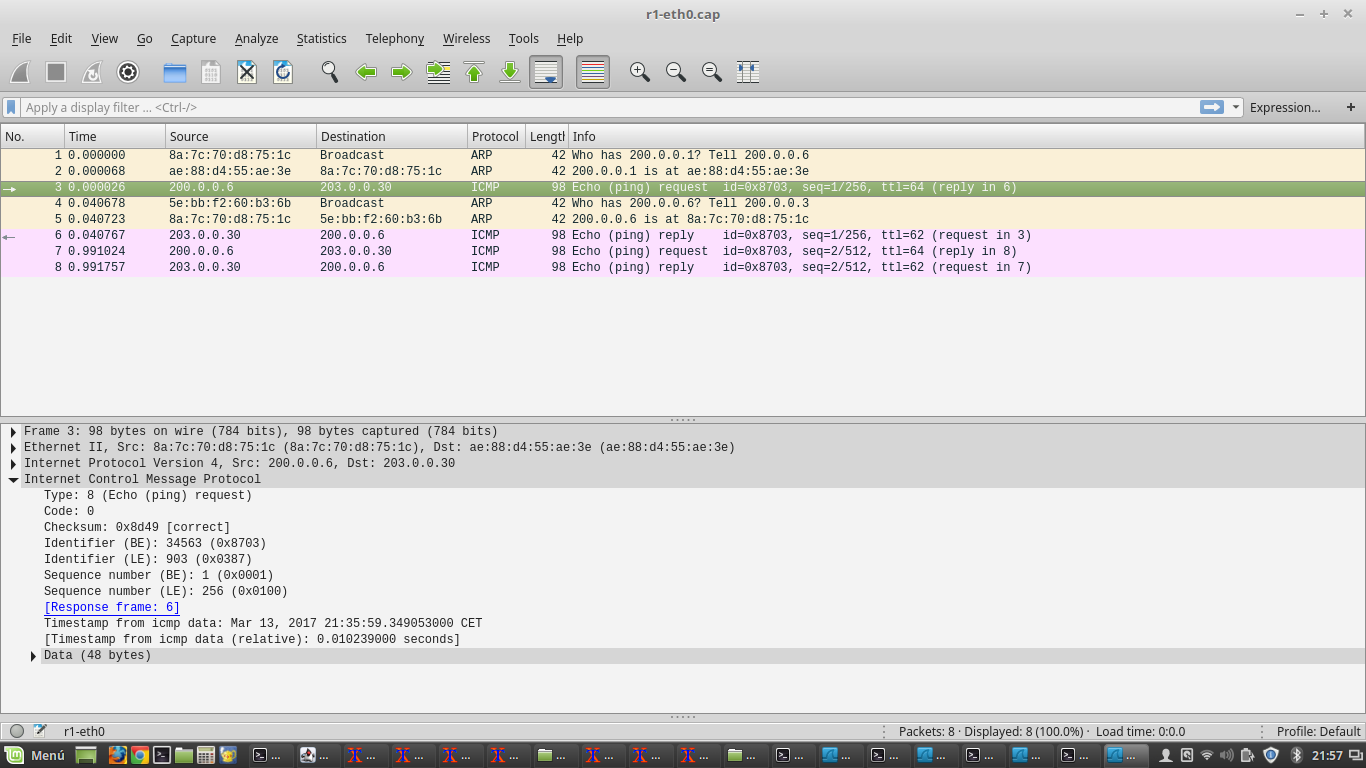
**PC3**

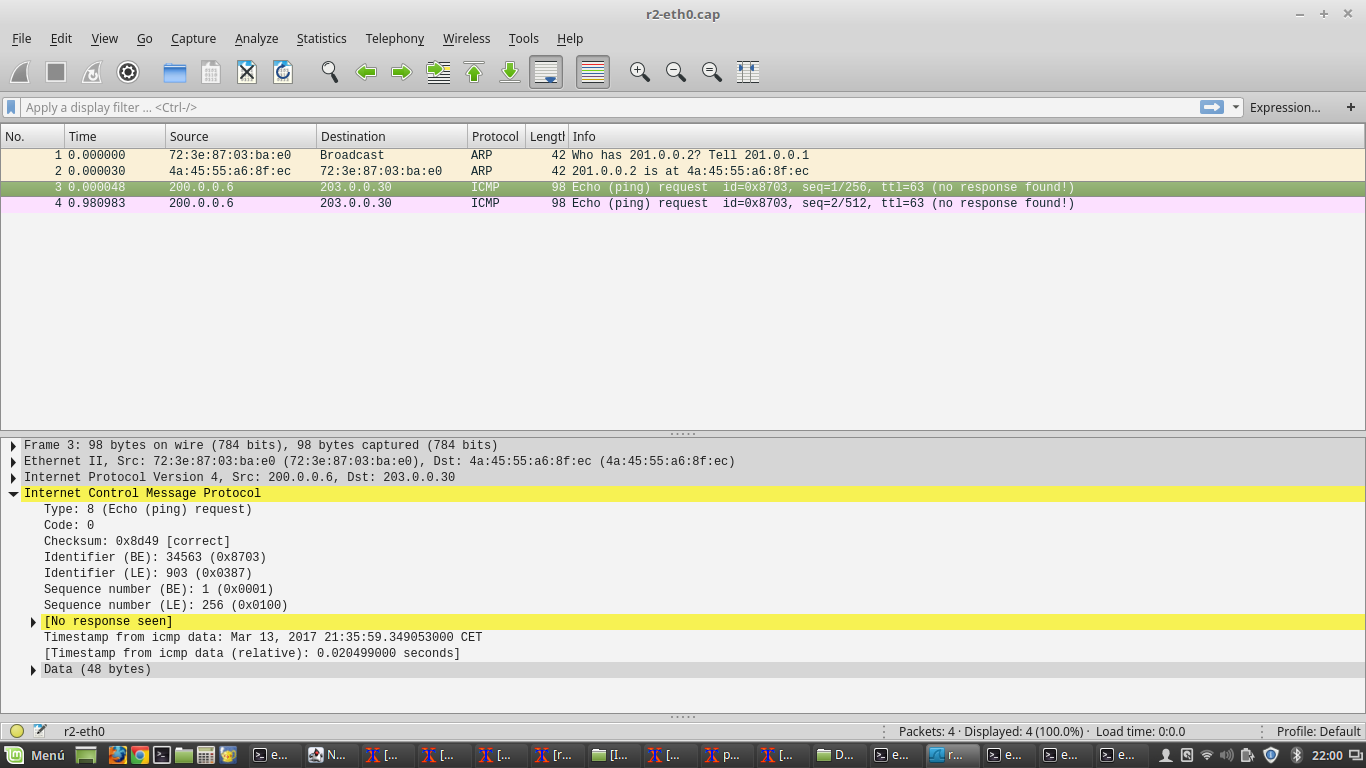
****

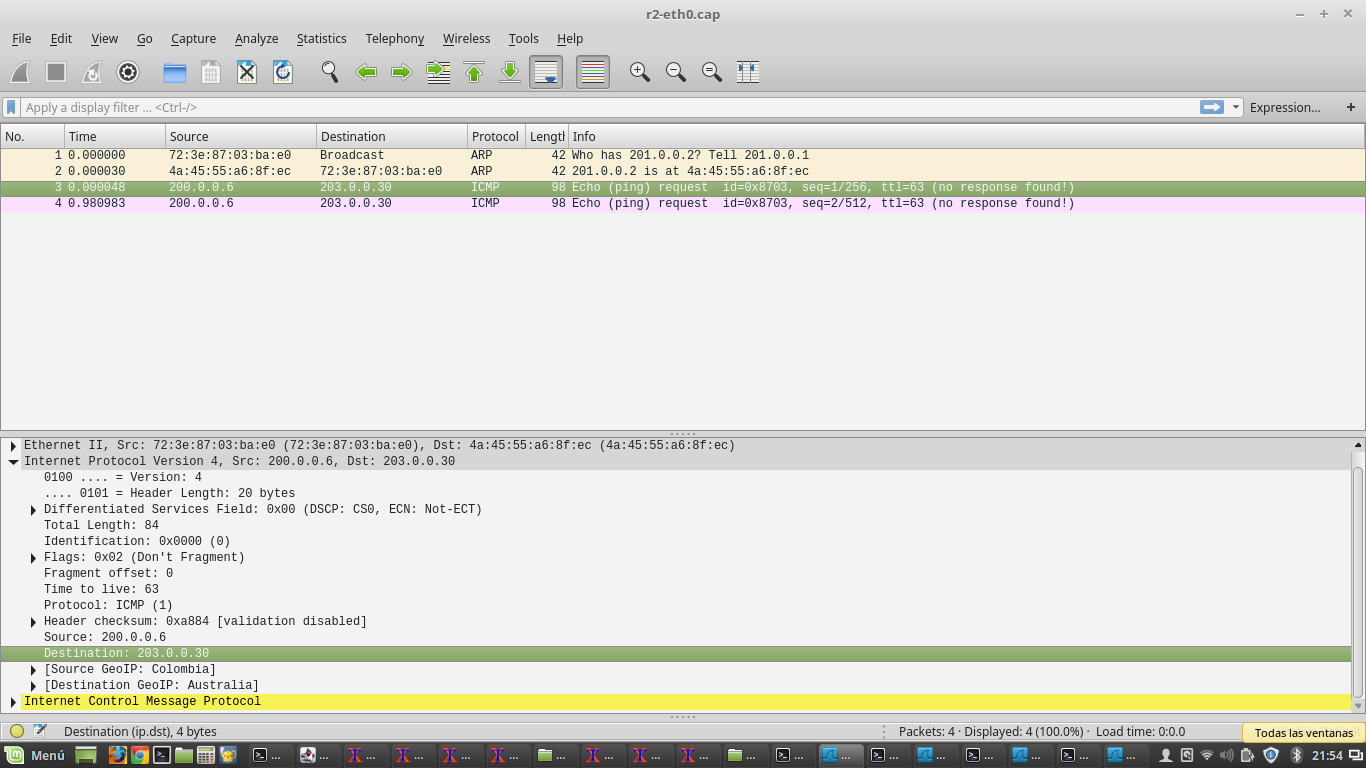
**R1**

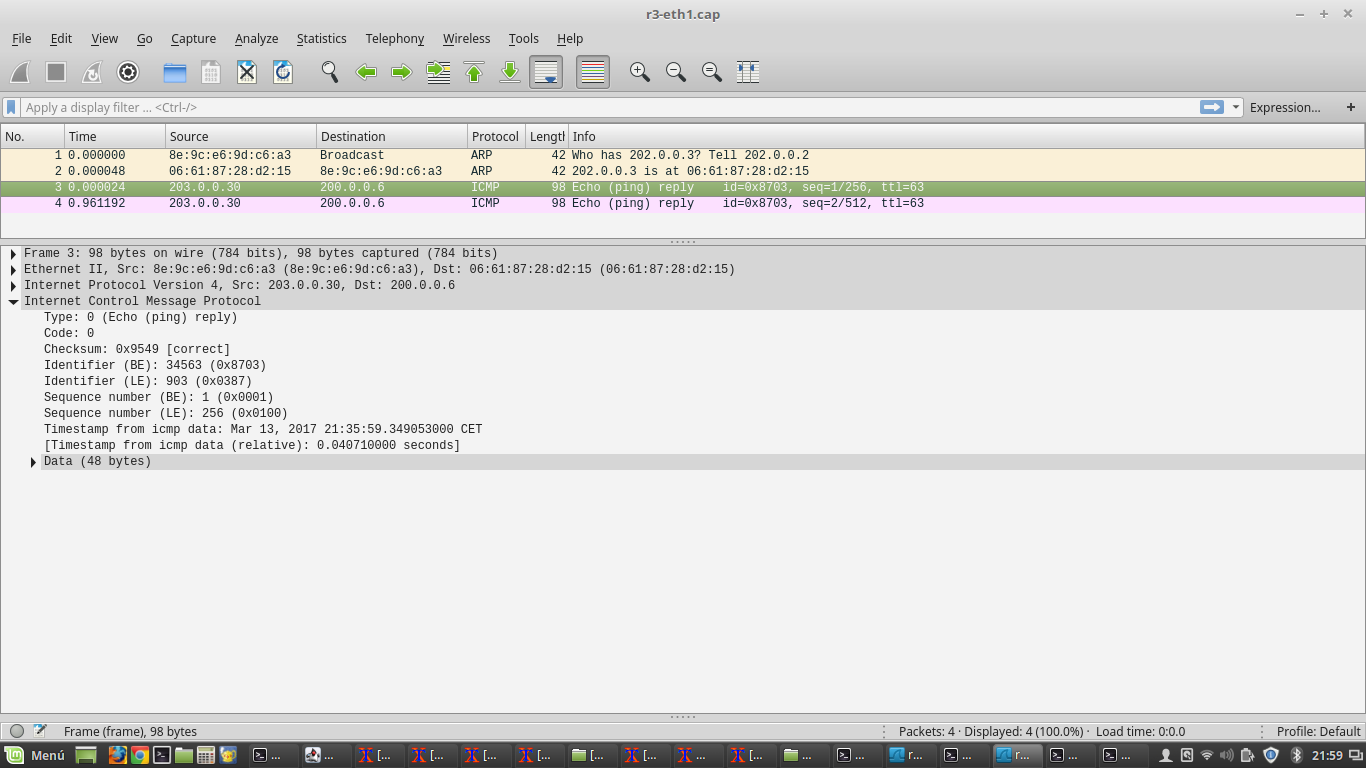
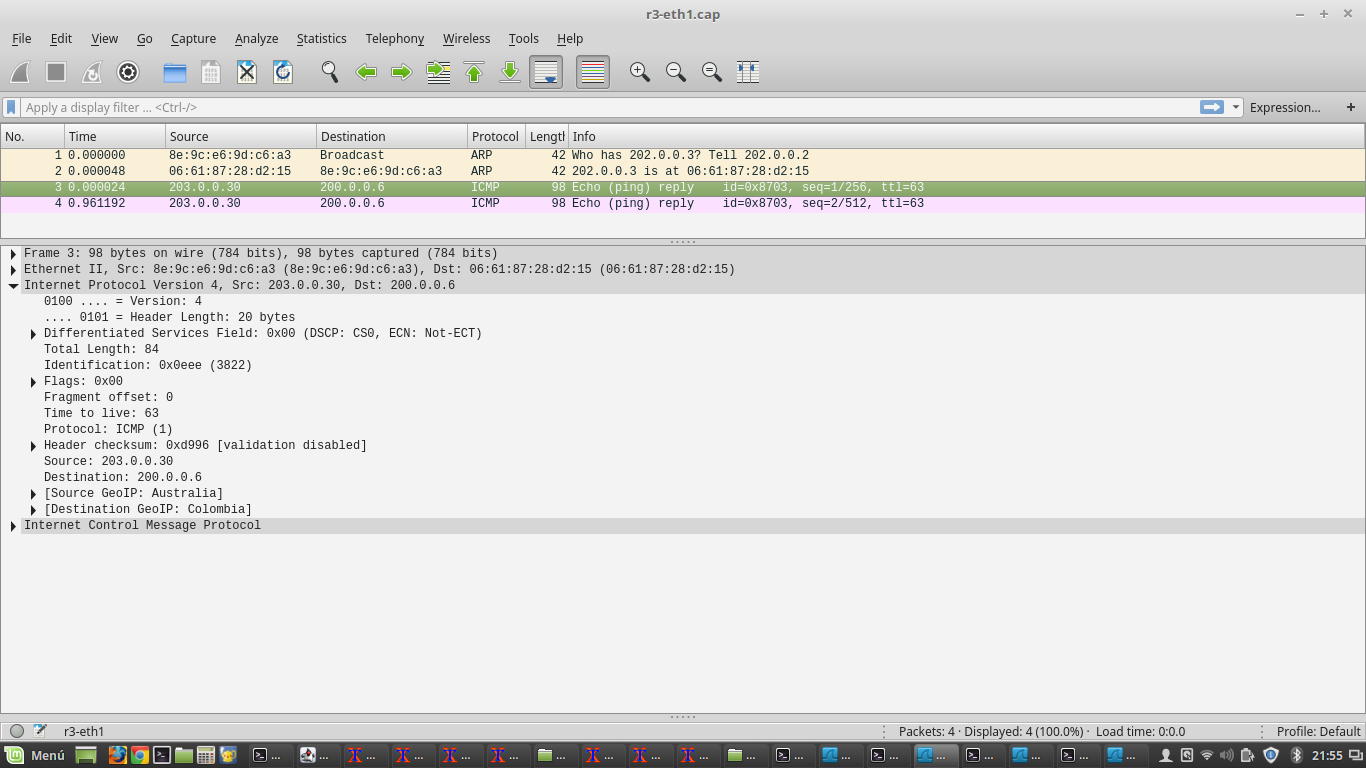
****

****

**R2**

****

**R3**

****

**5. Consultando las capturas, responde a las siguientes cuestiones:**

**a) ¿En qué se distinguen los mensajes “de ida” del ping de los mensajes “de vuelta”?**

En el TTL

**b) ¿En qué capturas se pueden ver los mensajes “de ida” del ping? ¿Y los mensajes de vuelta? ¿Por qué?**

Los mensajes de ida se pueden ver en el r1 en el r2 y en el pc3.

Los mensajes de vuelta se pueden ver en el

**c) Comprueba los valores del campo TTL de la cabecera IP de todos los datagramas de todas las capturas y explica dichos valores.**

En pc3

El reply de datagrama tiene un TTL 62

La request del datagrama tiene un TTL 64

En r3

La reply tiene un TTL 63

En r2

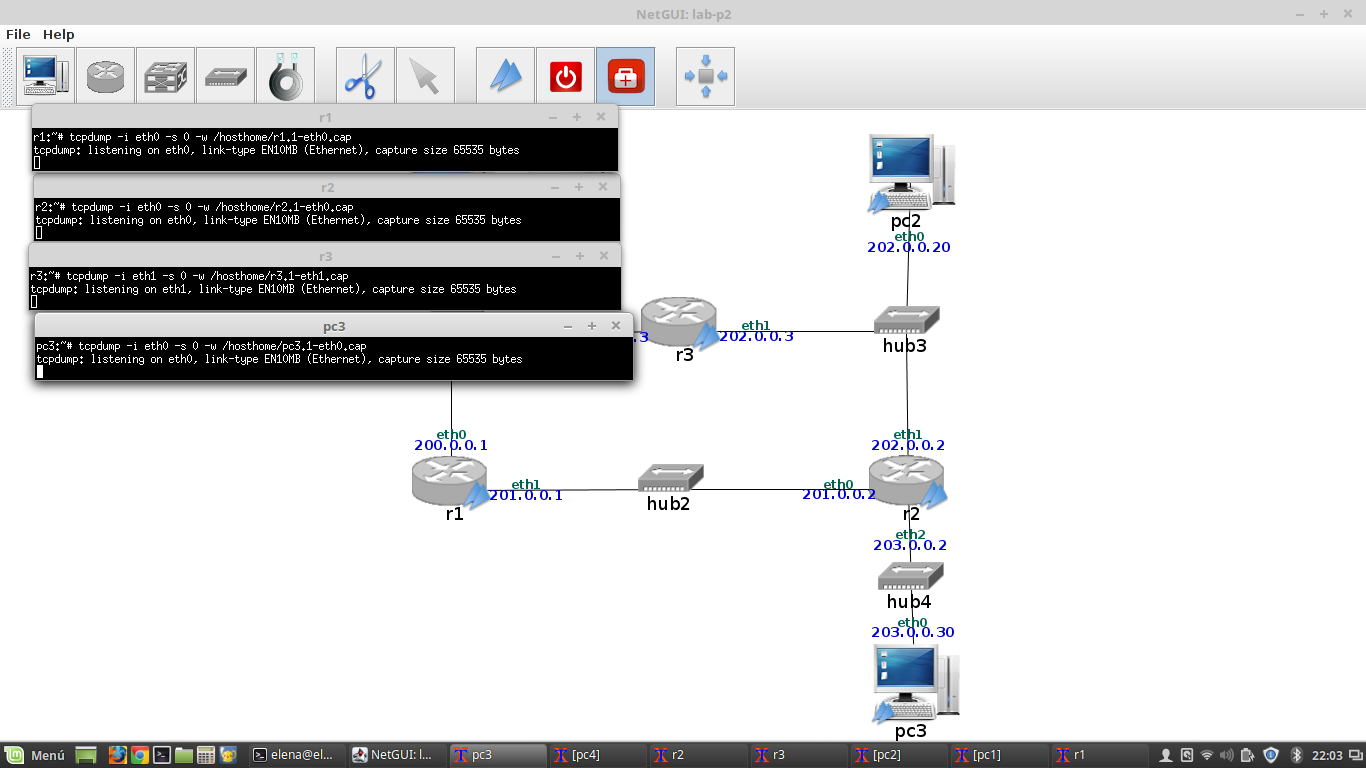
El request tiene un TTL 63

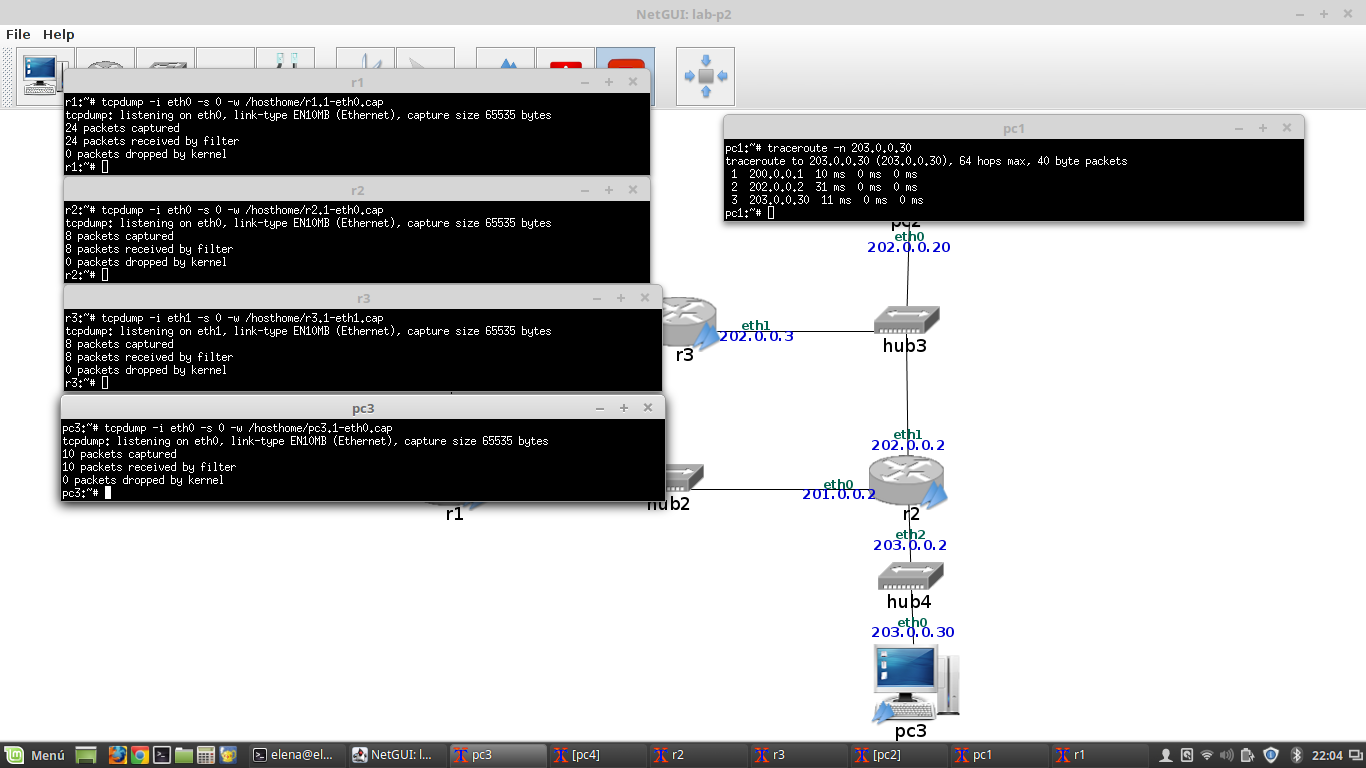
En r1

El reply de datagrama tiene un TTL 62

La request del datagrama tiene un TTL 64

1. **Arranca de nuevo tcpdump en las mismas máquinas e interfaces que lo has hecho anteriormente pero guardando las capturas en otros ficheros diferentes: en r1(eth0), en r2(eth0), en r3(eth1) y en pc3(eth0).**

****

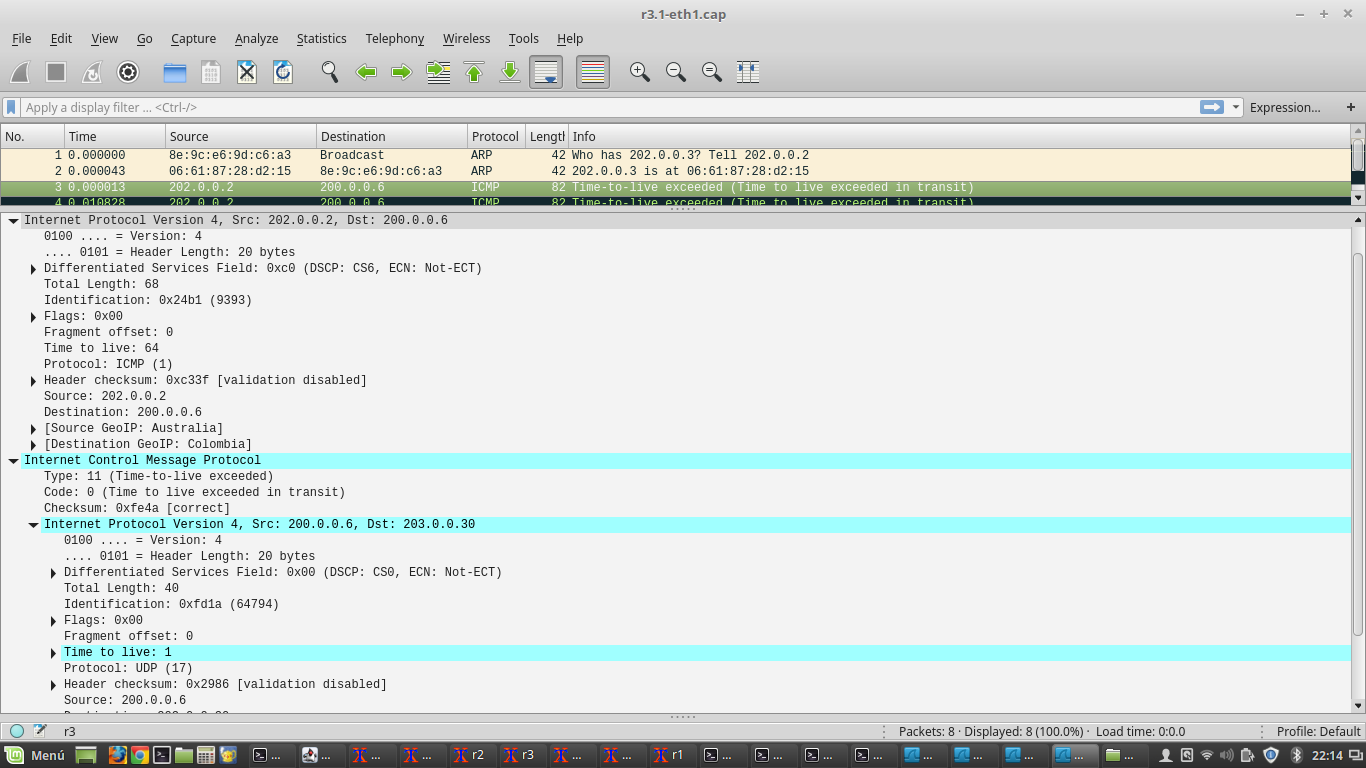
1. **Ejecuta en pc1 la orden traceroute a pc3.**
2. **Cuando la orden anterior haya terminado, interrumpe las capturas (Ctrl+C).**
3. **A la vista del resultado que se ha obtenido en pc1: ¿qué saltos intermedios ha atravesado un paquete para llegar de pc1 a pc3?**

Ha pasado por r1, r2 y pc3.

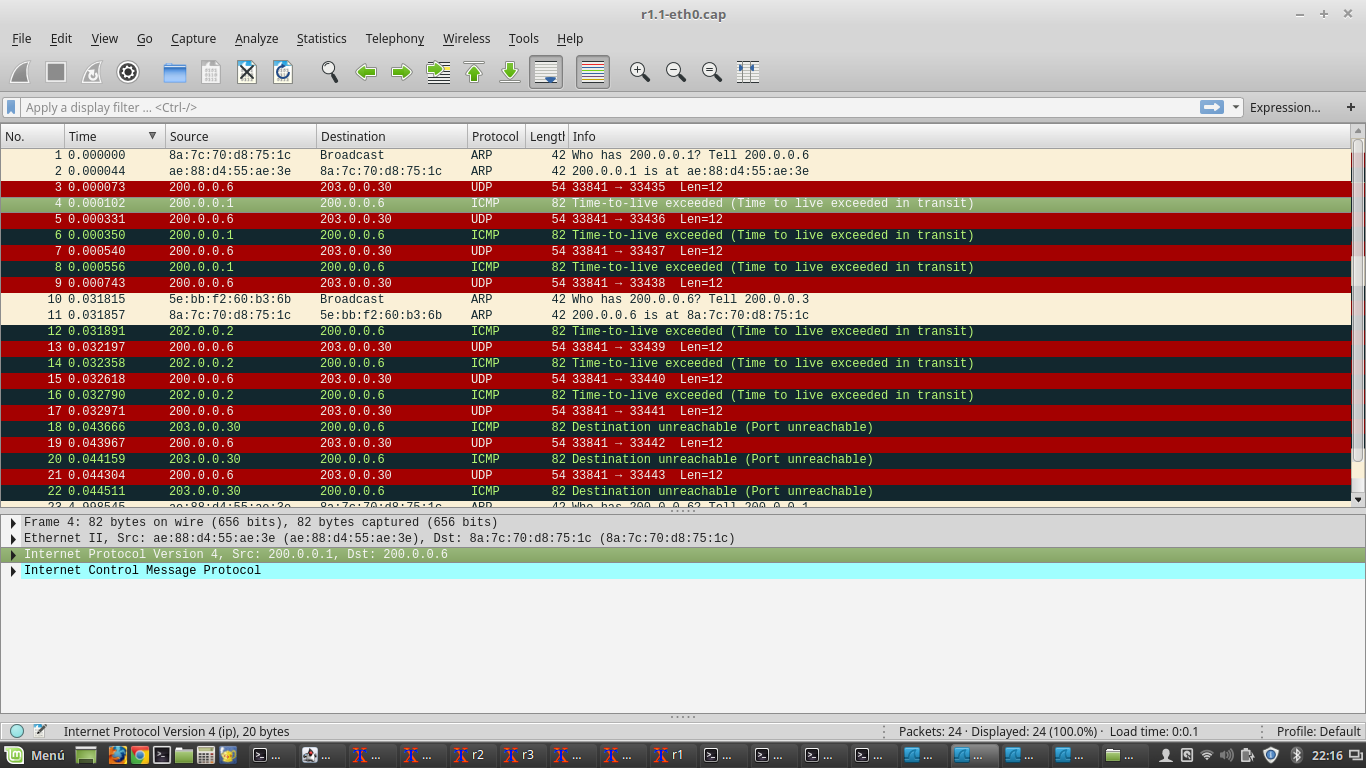
1. **Abre con wireshark los ficheros de captura que has obtenido. Identifica en los ficheros de capturas los siguientes paquetes:**

**Los 3 mensajes enviados por pc1 con TTL=1**

Son los mensajes 3, 5 y 7



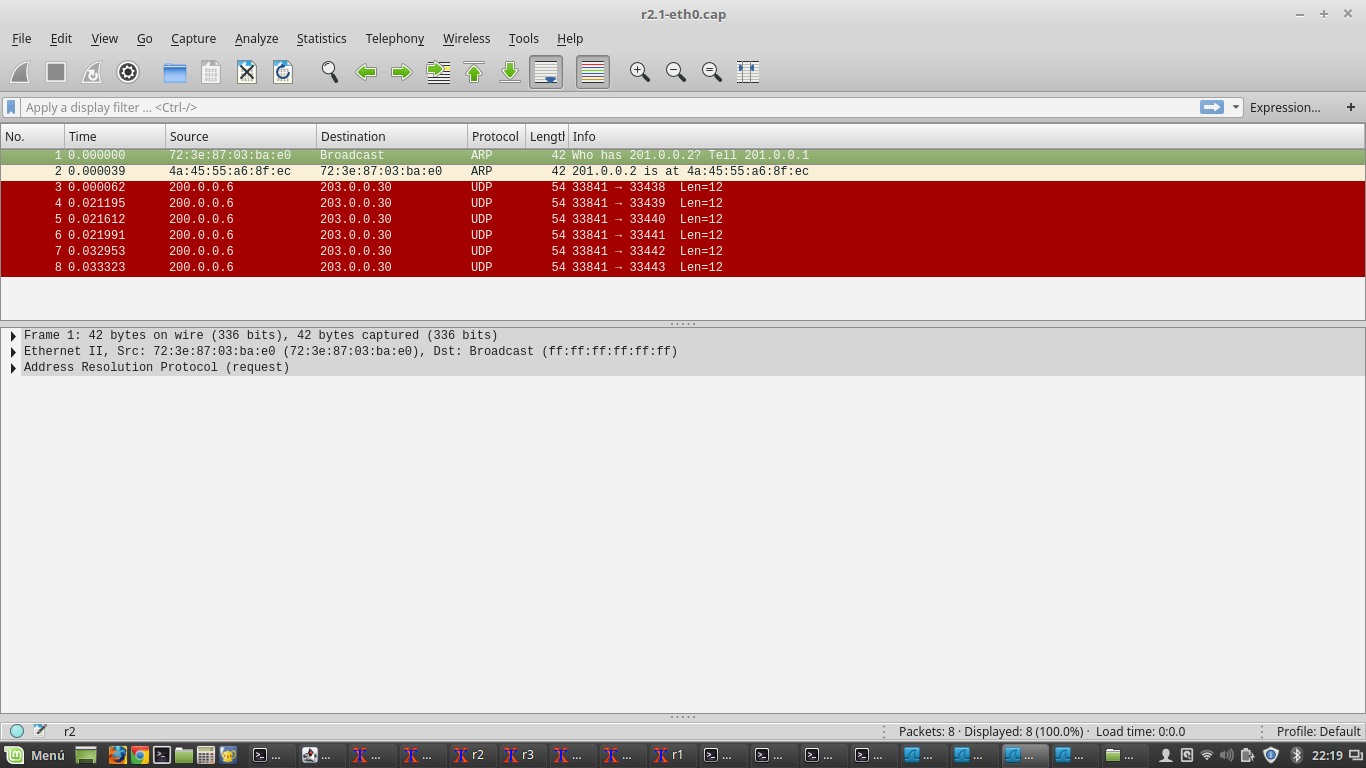
**Los 3 ICMP de TTL excedido enviados por r1**

****

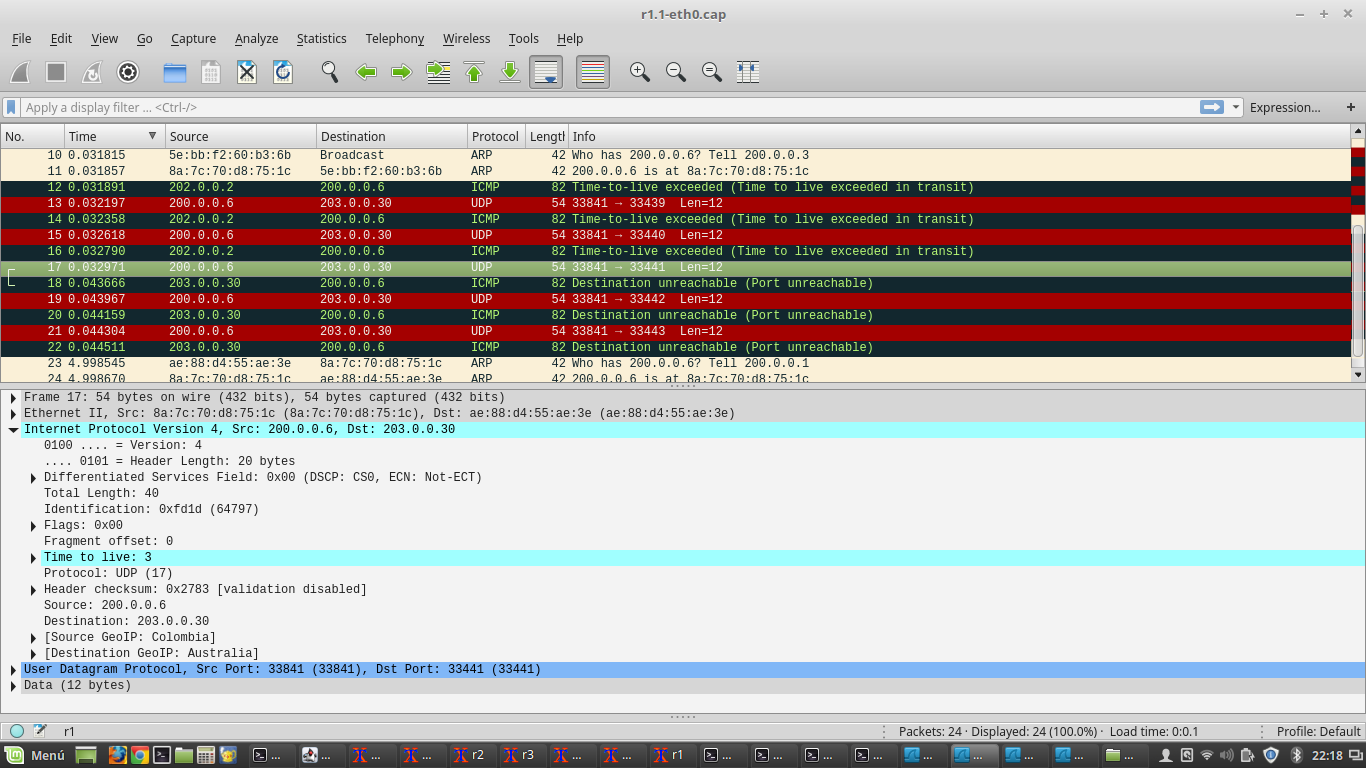
**Los 3 mensajes enviados por pc1 con TTL=2**

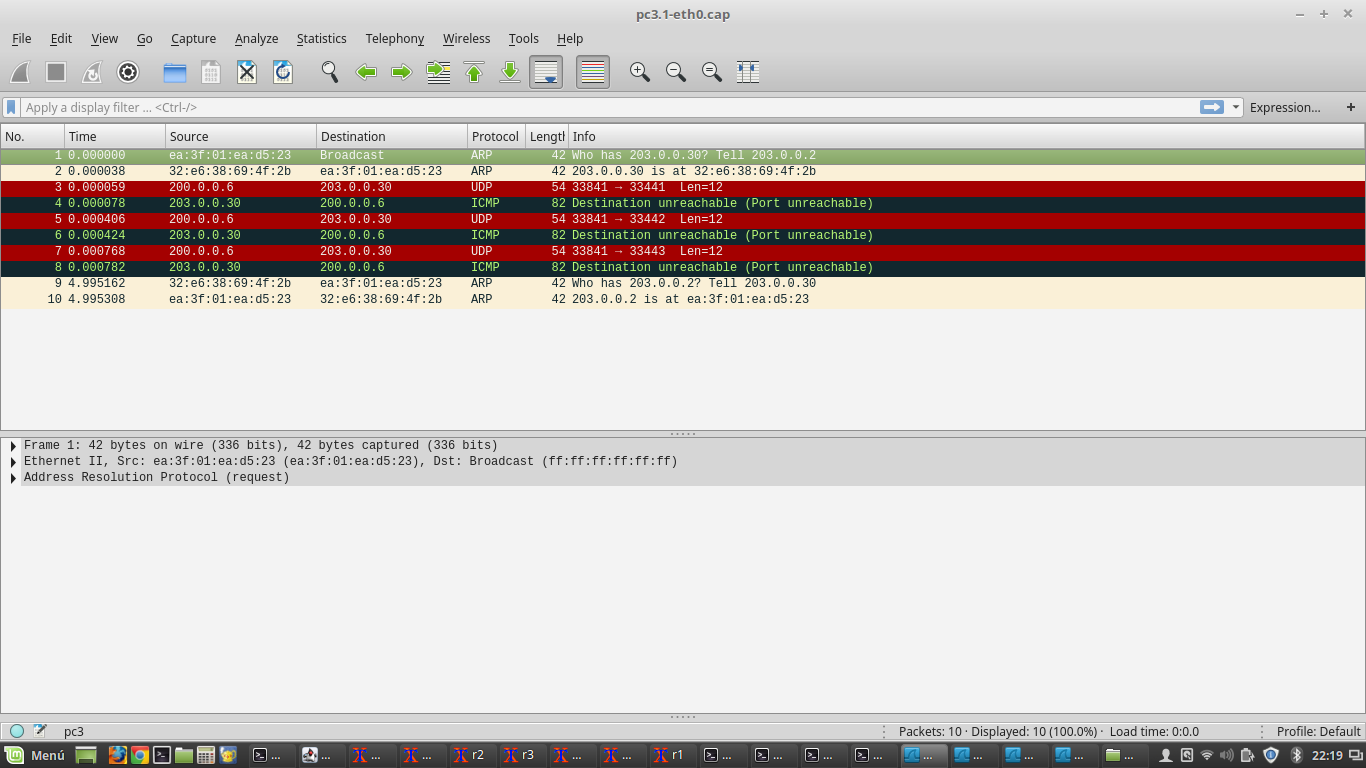
****

**Los 3 ICMP de TTL excedido enviados por r2**

****

**Los 3 mensajes enviados por pc1 con TTL=3**

****

**Los 3 ICMP de puerto inalcanzable enviados por pc3**

**11. Consultando las capturas, responde a las siguientes cuestiones:**

**a) ¿Por qué ruta van viajando los mensajes enviados por pc1 con TTL creciente?**

**b) ¿Por qué ruta viajan los ICMP enviados por r1? ¿Qué dirección IP usa r1 como IP de origen el enviar esos ICMP?**

200.0.0.6 a 203.0.0.30

202.0.0.2 a 203.0.0.30

De r1 a pc3 direccion pc1<r1<pc3

**c) ¿Por qué ruta viajan los ICMP enviados por r2? ¿Qué dirección IP usa r2 como IP de origen el enviar esos ICMP?**

**d ) ¿Por qué ruta viajan los ICMP enviados por pc3?**