Universidad Rey Juan Carlos

E.T.S. Ingeniería de Telecomunicación

Fundamentos de redes de ordenadores

Práctica 3

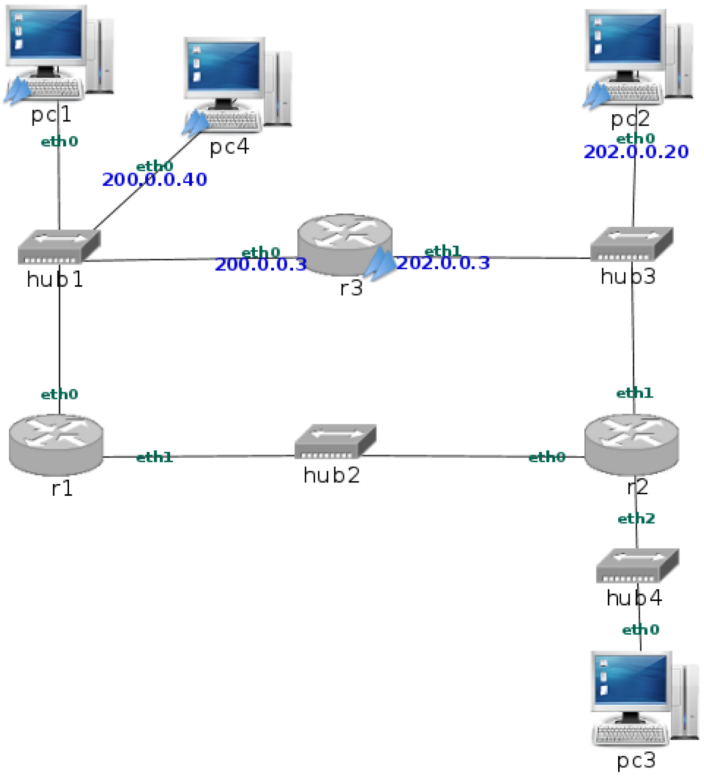
Autor:
Javier Izquierdo Hernández

November 1, 2022

Contenidos

1 Configuración de tablas de encaminamiento con route

Este escenario aplica 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.



Teniendo en cuenta que sólo están arrancadas pc1, pc2, pc3 y pc4, responde a las siguientes cuestiones:

1. Escribe en pc1 la orden ping 127.0.0.1 . ¿Por qué se obtiene respuesta pese a no tener configurada pc1 una dirección IP? Utilizando route comprueba el

contenido actual de la tabla de encaminamiento (routing) de pc1.

Porque esa dirección IP es la correspondiente a la dirección de loopback. La tabla de encaminamiento está vacía.

```
pc1:~# ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.049 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.107 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.083 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.066 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.049/0.076/0.107/0.022 ms
pc1:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
pc1:~#
```

2. Modifica el fichero /etc/network/interfaces de pc1 para que tenga una direccion IP acorde a la de la subred a la que esta conectado. (Nota: Deberas consultar previamente la mascara de la subred que tienen las otras maquinas conectadas a la misma subred que pc1). Reinicia la red en pc1 para que se aplique la configuracion que has escrito en el fichero /etc/network/interfaces.

```
pc1:~# nano /etc/network/interfaces
pc1:~# /etc/init.d/networking restart
Reconfiguring network interfaces...done.
pc1:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
200.57.0.0      *               255.255.255.0   U     0      0        0 eth0
pc1:~#
```

   La IP será 200.57.0.10, ya que la máscara es 255.255.255.0

3. Comprueba con route el contenido actual de su table de encaminamiento. Veras como, tras asignar la direccion IP a su interfaz de red, se ha anadido automaticamente una entrada en la tabla. Con esta tabla actual pc1, ¿a que otras direcciones IP crees que pc1 podra enviar datagramas IP?

   Podrá enviar datagramas IP a 200.57.0.40 pc4.

4. Dado que el resto de las maquinas encendidas tienen ya configurada una direccion IP, podras suponer facilmente cual es el contenido de su tabla de encaminamiento. Mira la tabla de encaminamiento de pc2 y pc4. ¿A que otras direcciones IP crees que esas maquinas podran enviar datagramas IP?

   Pc2 solo podrá enviar datagramas a sí mismo o a r2 y r3. Pc4 podrá enviar datagramas a pc1 o a r1 y r3.

5. Intenta deducir cual crees que sera la tabla de encaminamiento de r3,dado que tiene dos interfaces con IP asignada. Compruebalo consultando su tabla.

Con esta tabla de encaminamiento, ¿crees que r3 puede enviar datagramas IP a pc1 y pc4? ¿Y a pc2?

La tabla de encaminamiento de r3 será la de las 2 interfaces Ip con gateway de 0.0.0.0.

R3 podrá enviar datagramas a pc1 y a pc4 porque están conectadas a la interfaz Ip a la que esta conectada r3.

R3 tambíen podrá enviar un datagrama a pc2 porque tienen una conexión directa.

6. Haz ping desde pc1 a pc4 y haz ping desde pc1 a la direccion 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? ¿Que entradas de las tablas de encaminamiento se consultan en cada caso?

   Los dos ping funcionan, y las entradas que se consultan son las correspondientes a 200.57.0.0 con máscara de 255.255.255.0.

7. Haz un ping de pc1 a pc2 y haz un ping de pc1 a la direccion r3(eth1). ¿Funcionan estos ping? ¿Por que?

   No funcionan, porque la tabla de encaminamiento de pc1 no tiene esa direcciones Ip

8. Añade una ruta con el comando route en pc1 para que los datagramas IP que no sean para su propia subred los envie a traves del router r3.

```
pc1:~# route add -net 202.57.0.0 netmask 255.255.255.0 gw 200.57.0.3
pc1:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
200.57.0.0      *               255.255.255.0   U     0      0        0 eth0
202.57.0.0      200.57.0.3      255.255.255.0   UG    0      0        0 eth0
pc1:~#
```

9. Haz ahora ping desde pc1 a r3(eth1). ¿Funciona este ping? ¿Que entradas de las tablas de encaminamiento se consultan?

   Si funciona, se consulta la última entrada de la tabla de encaminamiento.

10. Haz un ping de pc1 a pc2. ¿Por que crees que no funciona este ping?

    Porque pc2 no tiene configurada en la tabla de encaminamiento la subred de pc1, por lo que no puede enviar el mensaje de vuelta.

11. Añade las rutas necesarias utilizando el comado route para que funcione un ping de pc1 a pc2 y un ping de pc4 a pc2. Ten en cuenta que podras utilizar, rutas de maquina, rutas de subred o ruta por defecto.

12. ¿Crees que con la configuracion que has realizado funcionara un ping de pc2 pc1 a y un ping pc2 a pc4? Compruebalo.

    Si funciona.

13. Antes de continuar espera unos 10 minutos despues de haber ejecutado el ultimo ping del apartado anterior. Consulta el estado de las caches de ARP en los pcs y en el router hasta que esten vacias.
    Arranca en pc4 un tcpdump para capturar trafico en su interfaz eth0, guardando la captura en el fichero p3-a-01.cap.
    Ejecuta en pc1 un ping a pc4 que envie solo 1 paquete **(ping -c 1 <maquinaDestino>)**.
    Interrumpe la captura en pc4 **(Ctrl+C)**.
    Comprueba el estado de las caches de ARP en pc1, pc4, pc2 y r3 y explica su contenido.

    Las caches de ARP en pc1 contiene la dirección IP y Ethernet de pc4, y en pc4 al contrario. En pc2 y en r3 las caches de ARP se encuentran vacías.

14. Analiza la captura con wireshark. Observa los siguientes campos en los mensajes:

    - Mensaje de solicitud de ARP que envia pc1 a pc4.
      - Direccion Ethernet destino: ff:ff:ff:ff:ff:ff
      - Direccion Ethernet origen: ce:42:01:bb:1b:2c
      - Tipo en la cabecera Ethernet: ARP
      - Contenido del mensaje de solicitud de ARP: localiza el campo que contiene la direccion IP de la maquina sobre la que se esta preguntando su direccion Ethernet.
        Target IP address: 200.57.0.40
    - Mensaje de respuesta de ARP que envia pc4 a pc1.
      - Dirección Ethernet destino: ce:42:01:bb:1b:2c
      - Dirección Ethernet origen: 42:d6:24:8c:dc:02
      - Tipo en la cabecera Ethernet: ARP
      - Contenido del mensaje de respuesta de ARP: localiza el campo que contiene la dirección Ethernet solicitada.
        Sender Ethernet address: 42:d6:24:8c:dc:02
    - Datagrama IP que envia pc1 a pc4.
      - Dirección Ethernet destino: 42:d6:24:8c:dc:02
      - Dirección Ethernet origen: ce:42:01:bb:1b:2c

  - Tipo en la cabecera Ethernet: IPv4
  - Dirección IP origen: 200.57.0.10
  - Dirección IP destino: 200.57.0.40
  - Campo TTL: 64
- Datagrama IP que envia pc4 a pc1.
  - Dirección Ethernet destino: ce:42:01:bb:1b:2c
  - Dirección Ethernet origen: 42:d6:24:8c:dc:02
  - Tipo en la cabecera Ethernet: IPv4
  - Dirección IP origen: 200.57.0.40
  - Dirección IP destino: 200.57.0.10
  - Campo TTL: 64

NOTA: Si tu captura ha durado mas de 5 segundos, podras ver que, 5 segundos despues de la solictud de ARP de pc1 preguntando por pc4, pc4 hace una solicitud de ARP preguntando por pc1, pero esta solicitud de ARP no tiene direccion de destino broadcast, sino la direccion Ethernet de pc1. Esto demuestra que pc4 ya tenia en su cache de ARP la direccion Ethernet de pc1 (la aprendio de la solicitud recibida de pc1), y este ARP es simplemente de confirmacion. No todas las implementaciones de TCP/IP realizan esta confirmacion, y en esta asignatura nunca le prestaremos atencion ni preguntaremos sobre ella.

15. Espera a que la cache de ARP de pc1 este vacia. Ahora vamos a analizar el trafico desde pc1 a pc2. ¿Cuantas capturas de trafico crees que son necesarias para ver todos los paquetes que se generan en el escenario cuando se comunican pc1 y pc2?

    Serán necesarias 2 capturas.
    Arranca un tcpdump en r3(eth0) guardando la captura en el fichero p3-a-02.cap.
    Arranca otro tcpdump en pc2 guardando la captura en el fichero p3-a-03.cap.
    Ejecuta en pc1 un ping a pc2 que envie solo 1 paquete **(ping -c 1 <maquinaDestino>)**.
    Interrumpe las capturas **(Ctrl+C)**.
    Comprueba el estado de las caches de ARP en pc1, pc2, pc4 y r3. Explica su contenido.

    Pc1 y Pc2 tiene la dirección de r3, r3 tiene la dirección de ambos, y pc4 está vacia.

16. Analiza las capturas realizadas con wireshark. Observa en los mensajes los mismo campos que analizaste el apartado anterior. Presta especial atencion a

los datagramas IP. Identifica los mensajes en las dos capturas que contienen el mismo datagrama IP. ¿Que direcciones Ethernet tiene la trama que contiene esos datagramas en cada captura? ¿Que valor tiene el campo TTL de la cabecera IP en cada uno?

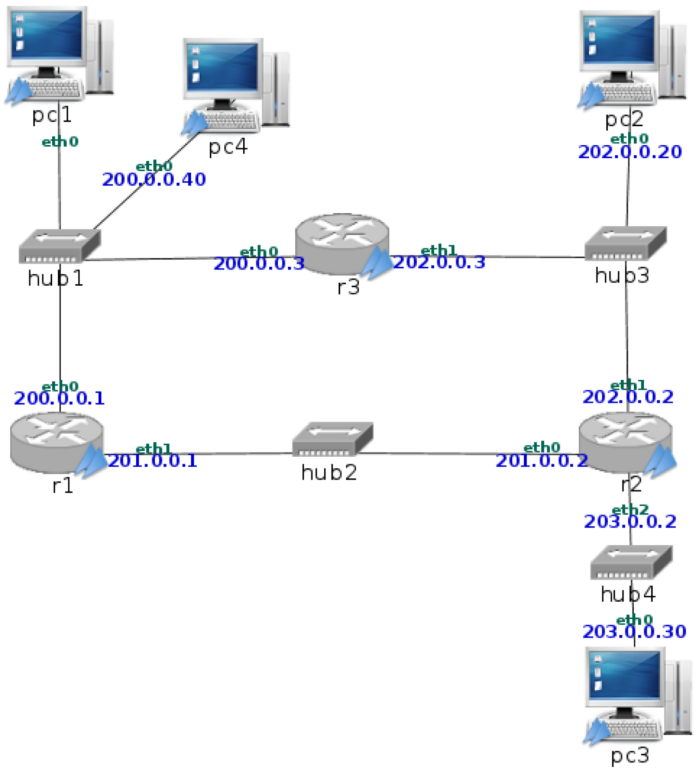
En la primera captura el primer datagrama Ip tiene la dirección Ethernet de pc1 y la eth0 de r3, y en la segunda captura las direcciones Ip son las de pc2 y la de eth1 de r3.

En el segundo datagrama las direcciones de el primer datagrama están invertidas.

En cuanto al ttl del primer mensaje: en la primera captura es 64 y en la segunda 63; sin embargo para el segundo datagrama es justo al revés, ya que es la respuesta.

2 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. Ten en cuenta que en pc1 ya tendrás configurada una dirección IP, mantén esta configuración.



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

En la figura se observan 4 subredes: 200.0.0.0, 201.0.0.0, 202.0.0.0 y 203.0.0.0 ; todas con la máscara 255.255.255.0

2. Reinicia las máquinas pc1, pc2 y pc4.
   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 hacia las subredes a las que están directamente conectados. Por tanto sólo podrán enviar paquetes a sus máquinas vecinas.

3. Añade rutas en las máquinas adecuadas modificando su fichero /etc/network/interfaces de forma que funcionen las siguientes rutas:

```
################################################################################
# /etc/network/interfaces -- configuration file for ifup(8), ifdown(8)

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 200.57.0.10
        netmask 255.255.255.0
        up route add -host 202.57.0.20 gw 200.57.0.3
```

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

   - pc1 a r3 a pc2
   - pc2 a r3 a pc1

   NOTA: Puedes emplear rutas de máquina, rutas de red o rutas por defecto.

   Ejecuta en pc1 la orden ping -c 3 <dirIPpc2 >para comprobar si hay conectividad entre las máquinas. Para verficar 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.

   De forma análoga deberás consultar las tablas de encaminamiento en el sentido pc2 a r3 a pc1.

```
pc1:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
202.57.0.20     200.57.0.3      255.255.255.255 UGH   0      0        0 eth0
200.57.0.0      *               255.255.255.0   U     0      0        0 eth0
pc1:~# arp -a
? (200.57.0.3) at 8E:DB:98:64:0F:6F [ether] on eth0
pc1:~#
```

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

- pc2 a r2 a pc3
- pc3 a r2 a 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 a r2 a pc2.

```
pc2:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
203.57.0.30     202.57.0.2      255.255.255.255 UGH   0      0        0 eth0
200.57.0.10     202.57.0.3      255.255.255.255 UGH   0      0        0 eth0
202.57.0.0      *               255.255.255.0   U     0      0        0 eth0
pc2:~# arp -a
? (202.57.0.2) at 8E:50:D1:16:16:CF [ether] on eth0
pc2:~#
```

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

- pc1 a r1 a pc3
- pc3 a r2 a 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.

De forma análoga deberás consultar las tablas de encaminamiento en el sentido pc3 a r2 a r3 a pc1

```
pc1:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
202.57.0.20     200.57.0.3      255.255.255.255 UGH   0      0        0 eth0
203.57.0.30     200.57.0.1      255.255.255.255 UGH   0      0        0 eth0
200.57.0.0      *               255.255.255.0   U     0      0        0 eth0
pc1:~# arp -a
? (200.57.0.3) at 8E:DB:98:64:0F:6F [ether] on eth0
? (200.57.0.1) at 8A:F4:F5:92:09:AC [ether] on eth0
pc1:~#
```

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

```
pc1:~# traceroute -n 202.57.0.20
traceroute to 202.57.0.20 (202.57.0.20), 64 hops max, 40 byte packets
 1  200.57.0.3  11 ms  0 ms  0 ms
 2  202.57.0.20  8 ms  1 ms  1 ms
pc1:~#
```

```
pc2:~# traceroute -n 200.57.0.10
traceroute to 200.57.0.10 (200.57.0.10), 64 hops max, 40 byte packets
 1  202.57.0.3  0 ms  0 ms  0 ms
 2  200.57.0.10  1 ms  1 ms  0 ms
pc2:~#
```

5. Ejecuta en pc2 un traceroute hacia pc3 y en pc3 uno hacia pc2 para comprobar que las rutas son las especificadas.

```
pc2:~# traceroute -n 203.57.0.30
traceroute to 203.57.0.30 (203.57.0.30), 64 hops max, 40 byte packets
 1  202.57.0.2  11 ms  0 ms  0 ms
 2  203.57.0.30  1 ms  0 ms  1 ms
pc2:~#
```

```
pc3:~# traceroute -n 202.57.0.20
traceroute to 202.57.0.20 (202.57.0.20), 64 hops max, 40 byte packets
 1  203.57.0.2  0 ms  0 ms  0 ms
 2  202.57.0.20  1 ms  1 ms  1 ms
pc3:~#
```

6. 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 *, en el final del tema 4 de teoría veremos a qué se deben. En la siguiente práctica se estudiarán más en detalle estas situaciones.

```
pc1:~# traceroute -n 203.57.0.30
traceroute to 203.57.0.30 (203.57.0.30), 64 hops max, 40 byte packets
 1  200.57.0.1  10 ms  0 ms  0 ms
 2  202.57.0.2  1 ms  1 ms  0 ms
 3  203.57.0.30  1 ms  1 ms  1 ms
pc1:~#
```

```
pc3:~# traceroute -n 200.57.0.10
traceroute to 200.57.0.10 (200.57.0.10), 64 hops max, 40 byte packets
 1  203.57.0.2  0 ms  0 ms  0 ms
 2  * * *
 3  200.57.0.10  1 ms  1 ms  1 ms
pc3:~#
```

7. Antes de continuar asegúrate de que las rutas entre las máquinas son las especificadas en el apartado anterior.

   Lanza con tcpdump capturas en las siguientes máquinas, guardando los ficheros con el nombre que se indica:

   - captura en r1(eth0) con nombre de fichero p3-b-01.cap
   - captura en r2(eth0) con nombre de fichero p3-b-02.cap
   - captura en r3(eth1) con nombre de fichero p3-b-03.cap
   - captura en pc3(eth0) con nombre de fichero p3-b-04.cap

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

   Interrumpe las 4 capturas (Ctrl+C).

   Analiza con wireshark las 4 capturas. Observa en ellas cómo los datagramas IP que se envían y reciben con la orden ping contienen un mensaje de ICMP. Comprueba en estos datagramas:

   Captura en r1

Source IP	Destination IP	TTL	Protocolo en IP	Tipo ICMP	Código ICMP
200.57.0.10	203.57.0.30	64	ICMP	8	0
203.57.0.30	200.57.0.10	62	ICMP	0	0
200.57.0.10	203.57.0.30	64	ICMP	8	0
203.57.0.30	200.57.0.10	62	ICMP	0	0

   Captura en r2

Source IP	Destination IP	TTL	Protocolo en IP	Tipo ICMP	Código ICMP
200.57.0.10	203.57.0.30	63	ICMP	8	0
200.57.0.10	203.57.0.30	63	ICMP	8	0

   Captura en r3

Source IP	Destination IP	TTL	Protocolo en IP	Tipo ICMP	Código ICMP
203.57.0.30	200.57.0.10	63	ICMP	0	0
203.57.0.30	200.57.0.10	63	ICMP	0	0

   Captura en pc3

Source IP	Destination IP	TTL	Protocolo en IP	Tipo ICMP	Código ICMP
200.57.0.10	203.57.0.30	62	ICMP	8	0
203.57.0.30	200.57.0.10	64	ICMP	0	0
200.57.0.10	203.57.0.30	62	ICMP	8	0
203.57.0.30	200.57.0.10	64	ICMP	0	0

Consultando las capturas, responde a las siguientes cuestiones:

a ¿En qué se distinguen los mensajes "de ida" del ping de los mensajes "de vuelta"?

Se distinguen en el campo type de ICMP, si vale 8 es un mensaje de "ida" y si vale 0 es una respueta.

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 r1, r2 y pc3, ya que es la ruta de "ida" configurada.

Los mensajes de vuelta se pueden ver en r3 y pc3, ya que es la rura configurada de "vuelta". También se pueden ver en r1, ya que para que el datagrama sea enviado desde r3 a pc1 debe de pasar por un hub, lo que hace que el mensaje llegue.

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

Cuando el valor es 64, es el mensaje sin haber pasado por ninguna otra máquina.

Si el valor es 63, el mensaje ha sido reenviado por un router

Y finalmente si el valor es 62, en este caso ya habrá de llegar al destino.

8. Arranca de nuevo tcpdump en las mismas máquinas e interfaces que lo has hecho anteriormente pero guardando las capturas en otros ficheros diferentes:

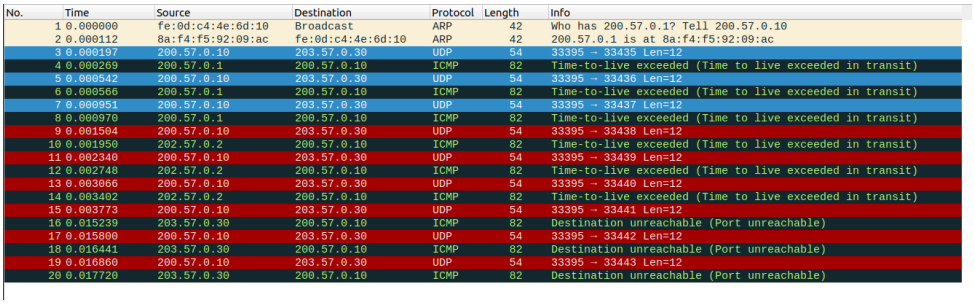
- captura en r1(eth0) con nombre de fichero p3-b-05.cap
- captura en r2(eth0) con nombre de fichero p3-b-06.cap
- captura en r3(eth1) con nombre de fichero p3-b-07.cap
- captura en pc3(eth0) con nombre de fichero p3-b-08.cap

Ejecuta en pc1 la orden traceroute a pc3.
Cuando la orden anterior haya terminado completament, interrumpe las capturas (Ctrl+C). A la vista del resultado que se muesta en pc1: ¿por qué router intermedios ha pasado un paquete para llegar de pc1 a pc3?

Habrá pasado por r1 y por r2.

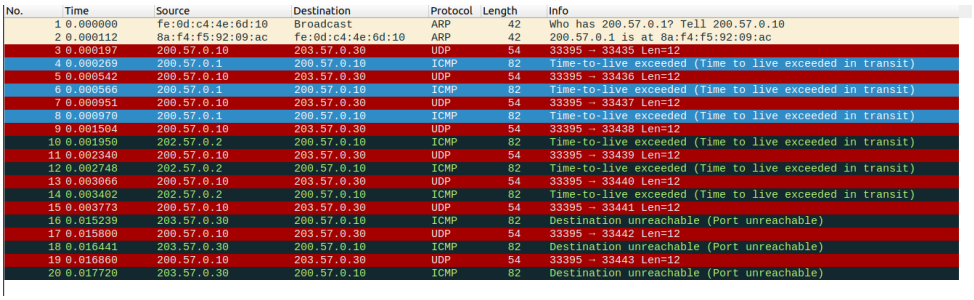
9. Abre con wireshark los ficheros de captura que has obtenido. Identifica en los ficheros de capturas los siguientes paquetes:

   - Los 3 mensajes enviados por pc1 con TTL=1



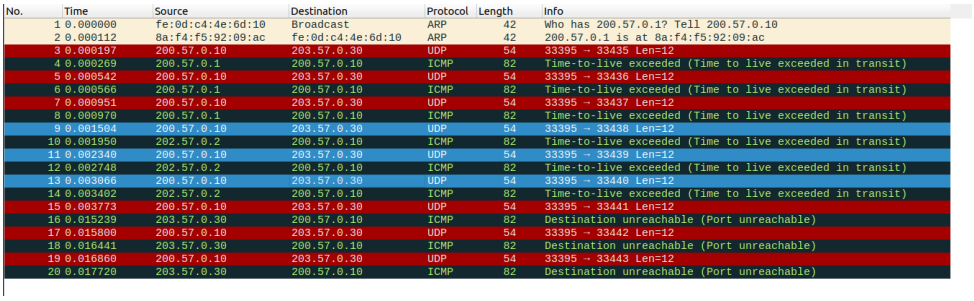
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe:0d:c4:4e:6d:10	Broadcast	ARP	42	Who has 200.57.0.1? Tell 200.57.0.10
2	0.000112	8a:f4:f5:92:09:ac	fe:0d:c4:4e:6d:10	ARP	42	200.57.0.1 is at 8a:f4:f5:92:09:ac
3	0.000197	200.57.0.10	203.57.0.30	UDP	54	33395 → 33435 Len=12
4	0.000269	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
5	0.000542	200.57.0.10	203.57.0.30	UDP	54	33395 → 33436 Len=12
6	0.000566	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
7	0.000951	200.57.0.10	203.57.0.30	UDP	54	33395 → 33437 Len=12
8	0.000970	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
9	0.001504	200.57.0.10	203.57.0.30	UDP	54	33395 → 33438 Len=12
10	0.001950	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
11	0.002340	200.57.0.10	203.57.0.30	UDP	54	33395 → 33439 Len=12
12	0.002748	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
13	0.003066	200.57.0.10	203.57.0.30	UDP	54	33395 → 33440 Len=12
14	0.003402	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
15	0.003773	200.57.0.10	203.57.0.30	UDP	54	33395 → 33441 Len=12
16	0.015239	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)
17	0.015800	200.57.0.10	203.57.0.30	UDP	54	33395 → 33442 Len=12
18	0.016441	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)
19	0.016860	200.57.0.10	203.57.0.30	UDP	54	33395 → 33443 Len=12
20	0.017720	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)

   - Los 3 ICMP de TTL excedido enviados por r1



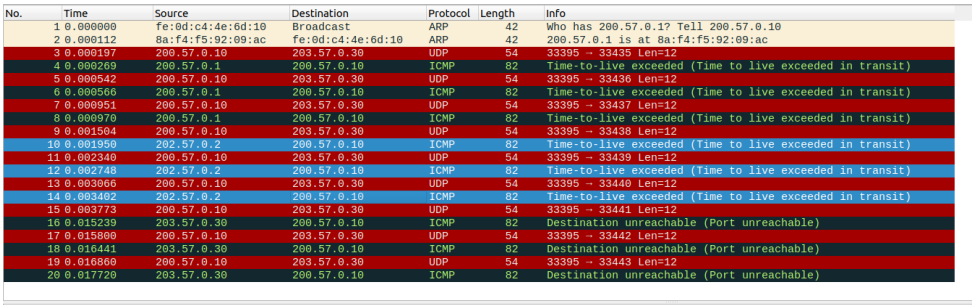
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe:0d:c4:4e:6d:10	Broadcast	ARP	42	Who has 200.57.0.1? Tell 200.57.0.10
2	0.000112	8a:f4:f5:92:09:ac	fe:0d:c4:4e:6d:10	ARP	42	200.57.0.1 is at 8a:f4:f5:92:09:ac
3	0.000197	200.57.0.10	203.57.0.30	UDP	54	33395 → 33435 Len=12
4	0.000269	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
5	0.000542	200.57.0.10	203.57.0.30	UDP	54	33395 → 33436 Len=12
6	0.000566	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
7	0.000951	200.57.0.10	203.57.0.30	UDP	54	33395 → 33437 Len=12
8	0.000970	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
9	0.001504	200.57.0.10	203.57.0.30	UDP	54	33395 → 33438 Len=12
10	0.001950	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
11	0.002340	200.57.0.10	203.57.0.30	UDP	54	33395 → 33439 Len=12
12	0.002748	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
13	0.003066	200.57.0.10	203.57.0.30	UDP	54	33395 → 33440 Len=12
14	0.003402	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
15	0.003773	200.57.0.10	203.57.0.30	UDP	54	33395 → 33441 Len=12
16	0.015239	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)
17	0.015800	200.57.0.10	203.57.0.30	UDP	54	33395 → 33442 Len=12
18	0.016441	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)
19	0.016860	200.57.0.10	203.57.0.30	UDP	54	33395 → 33443 Len=12
20	0.017720	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)

   - Los 3 mensajes enviados por pc1 con TTL=2



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe:0d:c4:4e:6d:10	Broadcast	ARP	42	Who has 200.57.0.1? Tell 200.57.0.10
2	0.000112	8a:f4:f5:92:09:ac	fe:0d:c4:4e:6d:10	ARP	42	200.57.0.1 is at 8a:f4:f5:92:09:ac
3	0.000197	200.57.0.10	203.57.0.30	UDP	54	33395 → 33435 Len=12
4	0.000269	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
5	0.000542	200.57.0.10	203.57.0.30	UDP	54	33395 → 33436 Len=12
6	0.000566	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
7	0.000951	200.57.0.10	203.57.0.30	UDP	54	33395 → 33437 Len=12
8	0.000970	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
9	0.001504	200.57.0.10	203.57.0.30	UDP	54	33395 → 33438 Len=12
10	0.001950	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
11	0.002340	200.57.0.10	203.57.0.30	UDP	54	33395 → 33439 Len=12
12	0.002748	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
13	0.003066	200.57.0.10	203.57.0.30	UDP	54	33395 → 33440 Len=12
14	0.003402	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
15	0.003773	200.57.0.10	203.57.0.30	UDP	54	33395 → 33441 Len=12
16	0.015239	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)
17	0.015800	200.57.0.10	203.57.0.30	UDP	54	33395 → 33442 Len=12
18	0.016441	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)
19	0.016860	200.57.0.10	203.57.0.30	UDP	54	33395 → 33443 Len=12
20	0.017720	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)

   - Los 3 ICMP de TTL excedido enviados por r2



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe:0d:c4:4e:6d:10	Broadcast	ARP	42	Who has 200.57.0.1? Tell 200.57.0.10
2	0.000112	8a:f4:f5:92:09:ac	fe:0d:c4:4e:6d:10	ARP	42	200.57.0.1 is at 8a:f4:f5:92:09:ac
3	0.000197	200.57.0.10	203.57.0.30	UDP	54	33395 → 33435 Len=12
4	0.000269	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
5	0.000542	200.57.0.10	203.57.0.30	UDP	54	33395 → 33436 Len=12
6	0.000566	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
7	0.000951	200.57.0.10	203.57.0.30	UDP	54	33395 → 33437 Len=12
8	0.000970	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
9	0.001504	200.57.0.10	203.57.0.30	UDP	54	33395 → 33438 Len=12
10	0.001950	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
11	0.002340	200.57.0.10	203.57.0.30	UDP	54	33395 → 33439 Len=12
12	0.002748	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
13	0.003066	200.57.0.10	203.57.0.30	UDP	54	33395 → 33440 Len=12
14	0.003402	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
15	0.003773	200.57.0.10	203.57.0.30	UDP	54	33395 → 33441 Len=12
16	0.015239	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)
17	0.015800	200.57.0.10	203.57.0.30	UDP	54	33395 → 33442 Len=12
18	0.016441	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)
19	0.016860	200.57.0.10	203.57.0.30	UDP	54	33395 → 33443 Len=12
20	0.017720	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)

   - Los 3 mensajes enviados por pc1 con TTL=3

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe:0d:c4:4e:6d:10	Broadcast	ARP	42	Who has 200.57.0.1? Tell 200.57.0.10
2	0.000112	8a:f4:f5:92:09:ac	fe:0d:c4:4e:6d:10	ARP	42	200.57.0.1 is at 8a:f4:f5:92:09:ac
3	0.000197	200.57.0.10	203.57.0.30	UDP	54	33395 → 33435 Len=12
4	0.000269	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
5	0.000542	200.57.0.10	203.57.0.30	UDP	54	33395 → 33436 Len=12
6	0.000566	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
7	0.000951	200.57.0.10	203.57.0.30	UDP	54	33395 → 33437 Len=12
8	0.000970	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
9	0.001504	200.57.0.10	203.57.0.30	UDP	54	33395 → 33438 Len=12
10	0.001950	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
11	0.002340	200.57.0.10	203.57.0.30	UDP	54	33395 → 33439 Len=12
12	0.002748	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
13	0.003066	200.57.0.10	203.57.0.30	UDP	54	33395 → 33440 Len=12
14	0.003402	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
15	0.003773	200.57.0.10	203.57.0.30	UDP	54	33395 → 33441 Len=12
16	0.015239	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)
17	0.015800	200.57.0.10	203.57.0.30	UDP	54	33395 → 33442 Len=12
18	0.016441	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)
19	0.016860	200.57.0.10	203.57.0.30	UDP	54	33395 → 33443 Len=12
20	0.017720	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)

- Los 3 ICMP de puerto inalcanzable enviados por pc3

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe:0d:c4:4e:6d:10	Broadcast	ARP	42	Who has 200.57.0.1? Tell 200.57.0.10
2	0.000112	8a:f4:f5:92:09:ac	fe:0d:c4:4e:6d:10	ARP	42	200.57.0.1 is at 8a:f4:f5:92:09:ac
3	0.000197	200.57.0.10	203.57.0.30	UDP	54	33395 → 33435 Len=12
4	0.000269	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
5	0.000542	200.57.0.10	203.57.0.30	UDP	54	33395 → 33436 Len=12
6	0.000566	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
7	0.000951	200.57.0.10	203.57.0.30	UDP	54	33395 → 33437 Len=12
8	0.000970	200.57.0.1	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
9	0.001504	200.57.0.10	203.57.0.30	UDP	54	33395 → 33438 Len=12
10	0.001950	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
11	0.002340	200.57.0.10	203.57.0.30	UDP	54	33395 → 33439 Len=12
12	0.002748	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
13	0.003066	200.57.0.10	203.57.0.30	UDP	54	33395 → 33440 Len=12
14	0.003402	202.57.0.2	200.57.0.10	ICMP	82	Time-to-live exceeded (Time to live exceeded in transit)
15	0.003773	200.57.0.10	203.57.0.30	UDP	54	33395 → 33441 Len=12
16	0.015239	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)
17	0.015800	200.57.0.10	203.57.0.30	UDP	54	33395 → 33442 Len=12
18	0.016441	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)
19	0.016860	200.57.0.10	203.57.0.30	UDP	54	33395 → 33443 Len=12
20	0.017720	203.57.0.30	200.57.0.10	ICMP	82	Destination unreachable (Port unreachable)

10. Consultando las capturas, responde a las siguientes cuestiones:

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

    Van viajando hacia r1, desde r1 a r2, y de r2 a pc3

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

    Viajan desde r1 a pc1 usando la dirección IP de r1 eth0 como origen, 200.57.0.1

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

    Viajan desde r2 a r3, y de r3 a pc1 usando como IP origen 202.57.0.2

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

    Viajan desde pc3 a r2, de r2 a r3, y desde r3 a pc1.