

Universidad Nacional Autónoma de Nicaragua
UNAN - León
Facultad de Ciencias y Tecnologías



Practica 1

Componente:

o **Redes de Computadoras**

Integrante:

➤ **Bismarck Antonio Berrios Lopez**

1. Análisis de ficheros de captura de tráfico

1. Selecciona el primer paquete que aparece en la captura, pulsando sobre la primera línea del Panel 1 (lista de paquetes). Éste quedará marcado en un color diferente:

1	0.000000	13.0.0.13	21.0.0.21	TCP	74	54689 → 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM=1 TSval=94568 TSecr=0 WS=2
2	0.004014	21.0.0.21	13.0.0.13	TCP	74	80 → 54689 [SYN, ACK] Seq=9 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=94568 TSecr=35696 WS=2
3	0.004322	13.0.0.13	21.0.0.21	TCP	66	54689 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=35696 TSecr=94568
4	0.005756	13.0.0.13	21.0.0.21	TCP	92	54689 → 80 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=26 TSval=35696 TSecr=94888 [TCP segment of a reassembled PDU]
5	0.006086	21.0.0.21	13.0.0.13	TCP	66	80 → 54689 [ACK] Seq=1 Ack=27 Win=5792 Len=0 TSval=95458 TSecr=35696
6	15.845293	13.0.0.13	21.0.0.21	TCP	78	54689 → 80 [PSH, ACK] Seq=27 Ack=1 Win=5840 Len=12 TSval=37284 TSecr=95458 [TCP segment of a reassembled PDU]
7	15.845595	21.0.0.21	13.0.0.13	TCP	66	80 → 54689 [ACK] Seq=1 Ack=39 Win=5792 Len=0 TSval=96152 TSecr=37284
8	17.189318	13.0.0.13	21.0.0.21	HTTP	68	GET /index.html HTTP/1.1
9	17.189493	21.0.0.21	13.0.0.13	TCP	66	80 → 54689 [ACK] Seq=1 Ack=41 Win=5792 Len=0 TSval=96287 TSecr=37419
10	17.190414	21.0.0.21	13.0.0.13	HTTP	418	HTTP/1.1 200 OK (text/html)
11	17.190928	13.0.0.13	21.0.0.21	TCP	66	54689 → 80 [ACK] Seq=41 Ack=353 Win=6912 Len=0 TSval=37419 TSecr=96287
12	20.704320	13.0.0.13	21.0.0.21	TCP	91	54689 → 80 [PSH, ACK] Seq=41 Ack=353 Win=6912 Len=25 TSval=38670 TSecr=96287 [TCP segment of a reassembled PDU]
13	29.736216	21.0.0.21	13.0.0.13	TCP	66	80 → 54689 [ACK] Seq=353 Ack=66 Win=5792 Len=0 TSval=97542 TSecr=38670
14	35.058536	13.0.0.13	21.0.0.21	TCP	78	54689 → 80 [PSH, ACK] Seq=66 Ack=353 Win=6912 Len=12 TSval=39206 TSecr=97542 [TCP segment of a reassembled PDU]
15	35.058856	21.0.0.21	13.0.0.13	TCP	66	80 → 54689 [ACK] Seq=353 Ack=78 Win=5792 Len=0 TSval=98074 TSecr=39206
16	36.113382	13.0.0.13	21.0.0.21	HTTP	68	GET /foto1.jpg HTTP/1.1
17	36.113418	21.0.0.21	13.0.0.13	TCP	66	80 → 54689 [ACK] Seq=353 Ack=88 Win=5792 Len=0 TSval=98180 TSecr=39314

2. En el Panel 1 (lista de paquetes), Con el primer paquete seleccionado, observa en el Panel 2 de wireshark los detalles de los protocolos para ese paquete. Indica qué protocolos se usan en ese primer paquete y a qué nivel de la arquitectura TCP/IP corresponden dichos protocolos.

```
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f), Dst: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)
Internet Protocol Version 4, Src: 13.0.0.13, Dst: 21.0.0.21
Transmission Control Protocol, Src Port: 54689, Dst Port: 80, Seq: 0, Len: 0
```

1. Protocolo Ethernet => Nivel de Enlace
2. Protocolo IP => Nivel de Red
3. Protocolo TCP => Nivel de Transporte

3. Teniendo seleccionado el primer paquete de la captura, en la primera pestaña (Frame) del Panel 2 se muestra información estadística relativa a la captura de ese paquete. Es la única pestaña que no tiene información de ningún protocolo contenido en el paquete, y en general no necesitaremos consultar dicha pestaña.

4. El resto de pestañas del Panel 2 contiene las cabeceras de los protocolos reconocidos en el paquete, empezando por Ethernet y siguiendo con los protocolos de niveles superiores.

5. Teniendo seleccionado el primer paquete de la captura, despliega la pestaña que se corresponde con el protocolo Ethernet. Indica qué campos observas en la cabecera de Ethernet, comprueba que la longitud de estos campos se corresponde con lo que hemos visto en la parte de teoría. Apunta los valores de estos campos.

```
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f), Dst: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)
  Destination: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)
    Address: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)
      ... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
      ... ..0 .... = IG bit: Individual address (unicast)
  Source: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f)
    Address: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f)
      ... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
      ... ..0 .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 13.0.0.13, Dst: 21.0.0.21
Transmission Control Protocol, Src Port: 54689, Dst Port: 80, Seq: 0, Len: 0
```

1. Mac Destino => 6 bytes
2. Mac Origen => 6 bytes
3. Tipo => 2 bytes

Todos ellos tienen la longitud que se esperaría según la teoría.

6. Pulsa sobre el campo Type de la cabecera Ethernet y observa cómo en la zona del Panel 3 que muestra el contenido del paquete en hexadecimal, se colorea dicho valor. Observa que wireshark interpreta el valor de Type 0x0800 como el código asociado al protocolo IP. ¿Qué significa que el valor del campo Type se corresponda con el código asociado al protocolo IP?

```

▶ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▼ Ethernet II, Src: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f), Dst: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)
  ▼ Destination: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)
    Address: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)
    ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f)
    Address: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f)
    ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 13.0.0.13, Dst: 21.0.0.21
▶ Transmission Control Protocol, Src Port: 54689, Dst Port: 80, Seq: 0, Len: 0

```


0000	7e 24 6e dd 8f 0e a2 ea 21 a9 90 5f 08 00 45 10	~\$n.... !...E
0010	00 3c b9 62 40 00 3f 06 60 28 0d 00 00 0d 15 00	< b? ? '(.....
0020	00 15 d5 a1 00 50 a6 f2 32 12 00 00 00 00 a0 02P 2.....
0030	16 d0 d4 ad 00 00 02 04 05 b4 04 02 08 0a 00 00
0040	8b 70 00 00 00 00 01 03 03 01	.p.....

7. Observa que en las capturas no aparecen los bytes ni el preámbulo, ni el comienzo de trama . El hardware de la tarjeta Ethernet elimina estos campos, pues no forman parte propiamente de la trama Etherente. Observa que tampoco aparece el CRC: el hardware de la tarjeta Ethernet comprueba que es correcto y lo elimina también de la trama. Si no fuera correcto descartaría la trama y no aparecería en la captura.

8. Selecciona el segundo paquete y observa en el Panel 2 de wireshark los detalles de los protocolos para ese paquete. Indica qué protocolos se usan en ese segundo paquete y a qué nivel de la arquitectura TCP/IP corresponden dichos protocolos.

```

▶ Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▶ Ethernet II, Src: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e), Dst: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f)
▶ Internet Protocol Version 4, Src: 21.0.0.21, Dst: 13.0.0.13
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 54689, Seq: 0, Ack: 1, Len: 0

```

1. Protocolo Ethernet => Nivel de Enlace
2. Protocolo IP => Nivel de Red
3. Protocolo TCP => Nivel de Transporte

9. Con el segundo paquete seleccionado, despliega la pestaña que se corresponde con el protocolo Ethernet. Indica qué campos observas en la cabecera de Ethernet. A la vista de los valores de estos campos indica si crees que este segundo paquete lo envía la misma máquina que envía el primer paquete.

```

▶ Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▼ Ethernet II, Src: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e), Dst: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f)
  Destination: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f)
    Address: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f)
      ... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
      ... ..0. .... = IG bit: Individual address (unicast)
  Source: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)
    Address: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e)
      ... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
      ... ..0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 21.0.0.21, Dst: 13.0.0.13
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 54689, Seq: 0, Ack: 1, Len: 0

```

1. Mac Destino
2. Mac Origen
3. Tipo

No creo que lo envíe la misma máquina que envío el primer paquete.

10. Fíjate en la longitud del primer paquete que aparece en su columna Length del Panel 1. Dicha longitud hace referencia a la longitud de toda la trama Ethernet sin el CRC. Para calcular la longitud de toda la trama Ethernet habría que sumar a la columna Length de una trama los 4 bytes del CRC que no aparecen en la trama capturada. ¿Crees que la primera trama lleva bits de relleno en Ethernet?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	13.0.0.13	21.0.0.21	TCP	74	54689 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=35696 TSecr=0 WS=2
2	0.004014	21.0.0.21	13.0.0.13	TCP	74	80 → 54689 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=94568 TSecr=35696 WS=2
3	0.004322	13.0.0.13	21.0.0.21	TCP	66	54689 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=35696 TSecr=94568
4	8.895756	13.0.0.13	21.0.0.21	TCP	92	54689 → 80 [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=26 TSval=36589 TSecr=94888 [TCP segment of a reassembled PDU]

Length = 74 + 4 bytes CRC = 78 bytes totales | No lleva bits de relleno en Ethernet.

11. Si la columna Length de la trama tuviera un valor igual a 60 bytes (longitud total de la trama igual a 64 bytes: 60 más 4 bytes del CRC) ¿podrías decir si dicha trama tiene o no relleno?

No podría.

12. Observa el paquete número 18. Indica qué protocolos se usan en ese paquete y a qué nivel de la arquitectura TCP/IP corresponden dichos protocolos.

```

▶ Frame 18: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
▶ Ethernet II, Src: 7e:24:6e:dd:8f:0e (7e:24:6e:dd:8f:0e), Dst: a2:ea:21:a9:90:5f (a2:ea:21:a9:90:5f)
▶ Internet Protocol Version 4, Src: 21.0.0.21, Dst: 13.0.0.13
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 54689, Seq: 353, Ack: 80, Len: 1448

```

1. Protocolo Ethernet => Nivel de Enlace
2. Protocolo IP => Nivel de Red
3. Protocolo TCP => Nivel de Transporte

13. Observa el campo longitud de la trama Ethernet asociada al paquete número 18. Si la máquina que está enviando esa información hubiese tenido más datos para enviar dentro de la trama 18, explica si hubiera podido incluirlos también en el campo de datos de dicha trama.

No.	Time	Source	Destination	Protocol	Length	Info
16	36.113382	13.0.0.13	21.0.0.21	HTTP	68	GET /foto1.jpg HTTP/1.1
17	36.114318	21.0.0.21	13.0.0.13	TCP	66	80 → 54689 [ACK] Seq=353 Ack=80 Win=5792 Len=0 TSval=98180 TSecr=39311
18	36.127774	21.0.0.21	13.0.0.13	TCP	1514	80 → 54689 [ACK] Seq=353 Ack=80 Win=5792 Len=1448 TSval=98180 TSecr=39311 [TCP segment of a reassembled PDU]
19	36.127782	21.0.0.21	13.0.0.13	TCP	1514	80 → 54689 [ACK] Seq=1801 Ack=80 Win=5792 Len=1448 TSval=98180 TSecr=39311 [TCP segment of a reassembled PDU]
20	36.128423	13.0.0.13	21.0.0.21	TCP	66	54689 → 80 [ACK] Seq=80 Ack=1801 Win=9808 Len=0 TSval=39312 TSecr=98180

Length = 1514 bytes + 4 bytes CRC = 1518 bytes Length Total de la trama. | No sería posible debido a que el tamaño máximo de la trama en Ethernet II es de 1518 bytes y la trama 18 llega a él.

Cierra el fichero de captura cap1.cap y abre el fichero de captura cap2.cap con wireshark y responde a las siguientes preguntas:

1. Teniendo seleccionado el primer paquete de la captura, despliega la pestaña que se corresponde con el protocolo Ethernet. Indica qué campos observas en Ethernet. Apunta los valores de estos campos.

```
▶ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on 0
▼ Ethernet II, Src: Cisco251_af:f4:54 (00:07:0d:af:f4:54), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
    .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
    .... ..1. .... = IG bit: Group address (multicast/broadcast)
  ▼ Source: Cisco251_af:f4:54 (00:07:0d:af:f4:54)
    Address: Cisco251_af:f4:54 (00:07:0d:af:f4:54)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  Padding: 0601040000000000201000302000005010301
▶ Address Resolution Protocol (request)
```

1. Destino = ff: ff: ff: ff: ff: ff
2. Origen = 00:07:0d:af:f4:54
3. Tipo = ARP (0x0806)
4. Padding = 0601040000000000201000302000005010301

2. Fíjate en el campo Type. El valor es diferente al que viste en el fichero de captura anterior. ¿A qué protocolo se refiere este valor?

Al protocolo ARP

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

Que se envió la trama a la dirección destino de broadcast.

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco251_af:f4:54	Broadcast	ARP	60	Who has 24.166.173.159? Tell 24.166.172.1
2	0.098594	Cisco251_af:f4:54	Broadcast	ARP	60	Who has 24.166.172.141? Tell 24.166.172.1
3	0.110617	Cisco251_af:f4:54	Broadcast	ARP	60	Who has 24.166.173.161? Tell 24.166.172.1

Length = 60 bytes + 4 bytes CRC = 64 bytes Longitud total de la Trama.

5. En este caso, el paquete es un mensaje del protocolo ARP que va encapsulado dentro de Ethernet. Todos los mensajes del protocolo ARP tienen la misma longitud, 28 bytes. La cabecera de Ethernet ocupa 14 bytes y el CRC 4 bytes. Por tanto la longitud total de la trama sería 46 bytes y será necesario introducir relleno para alcanzar la longitud de trama mínima en Ethernet (64 bytes). El relleno debería ser 18 bytes.

6. Observa para este paquete el campo Padding. ¿Qué longitud tiene? ¿Qué crees que significa este campo?

```
▶ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▼ Ethernet II, Src: Cisco251_af:f4:54 (00:07:0d:af:f4:54), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
    ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
    ....1. .... = IG bit: Group address (multicast/broadcast)
  ▼ Source: Cisco251_af:f4:54 (00:07:0d:af:f4:54)
    Address: Cisco251_af:f4:54 (00:07:0d:af:f4:54)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  Padding: 0601040000000000201000302000005010301
▶ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff 00 07 0d af f4 54 08 06 00 01  .....T...
0010  08 00 06 04 00 01 00 07 0d af f4 54 18 a6 ac 01  .....T...
0020  00 00 00 00 00 00 18 a6 ad 9f 06 01 04 00 00 00  .....
0030  00 02 01 00 03 02 00 00 05 01 03 01  .....

```

Ethernet Padding (eth.padding), 18 bytes

Tiene 18 bytes de longitud por lo que creo que se refiere a la cantidad de relleno que se agrego para alcanzar la cantidad mínima de bytes del protocolo Ethernet II.

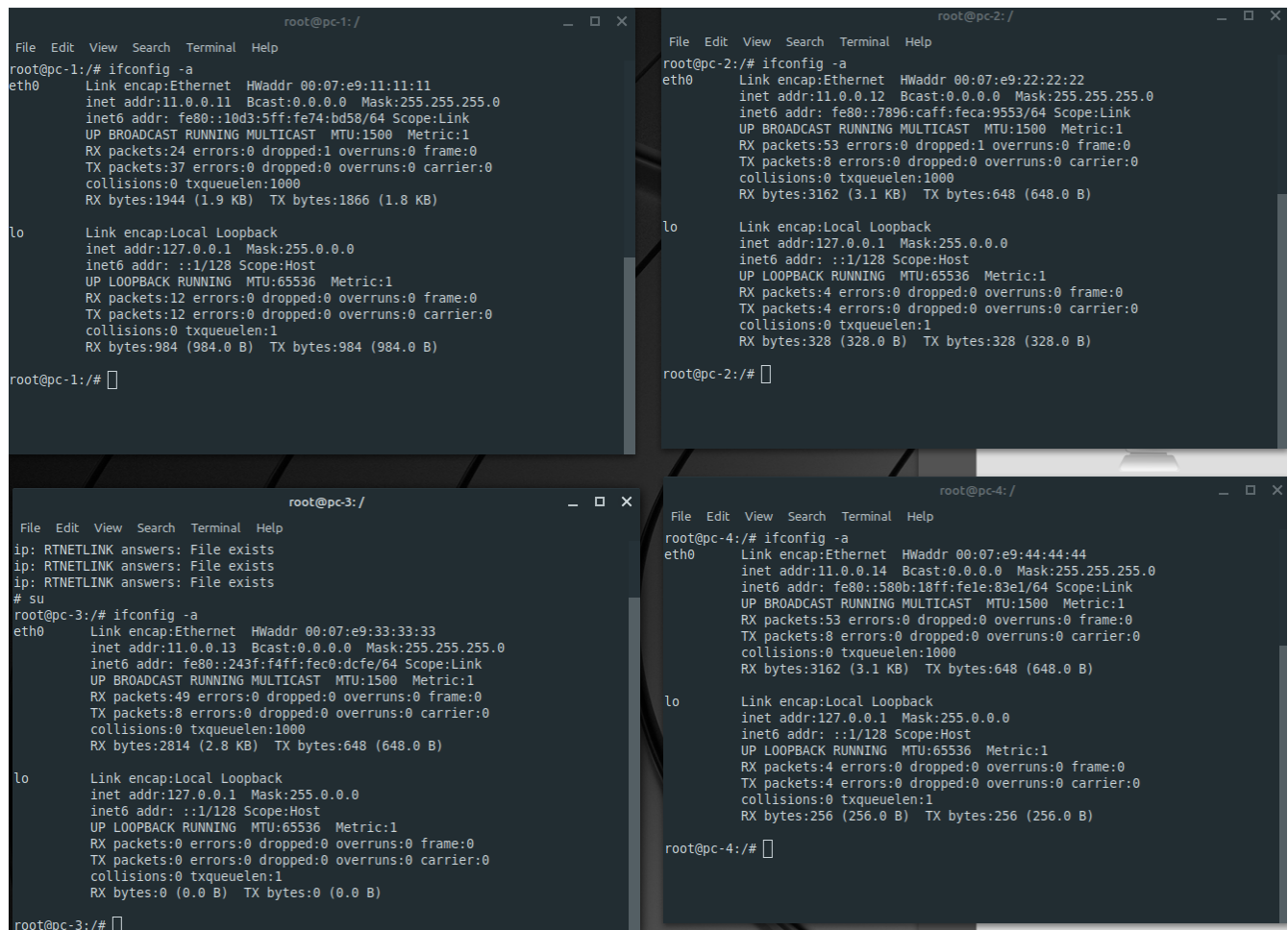
2. Generación de tráfico Ethernet y análisis de la captura de tráfico

Arranca cada uno de los PCs y el router, de uno en uno, esperando que termine de arrancar una máquina para arrancar la siguiente. Observarás que el icono de las máquinas aparece ahora con dos triángulos azules, que indican que las máquinas están ejecutándose. Al arrancar las máquinas se configuran con una dirección de nivel de red, una dirección IP. El protocolo IP será objeto de estudio del tema siguiente.

1. Consulta las direcciones Ethernet que hay configuradas en cada una de las interfaces de las máquinas, para ello ejecuta por ejemplo en pc1:

```
pc1:~# ifconfig eth0
```

Apunta las direcciones Ethernet de cada interfaz y dispositivo.



```
root@pc-1:/# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:07:e9:11:11:11
          inet addr:11.0.0.11  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::10d3:5ff:fe74:bd58/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:24 errors:0 dropped:1 overruns:0 frame:0
          TX packets:37 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1944 (1.9 KB)  TX bytes:1866 (1.8 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:984 (984.0 B)  TX bytes:984 (984.0 B)

root@pc-1:/#

root@pc-2:/# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:07:e9:22:22:22
          inet addr:11.0.0.12  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::7896:caff:feca:9553/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:53 errors:0 dropped:1 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3162 (3.1 KB)  TX bytes:648 (648.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:328 (328.0 B)  TX bytes:328 (328.0 B)

root@pc-2:/#

root@pc-3:/# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:07:e9:33:33:33
          inet addr:11.0.0.13  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::243f:f4ff:fec0:dcfe/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:49 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2814 (2.8 KB)  TX bytes:648 (648.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@pc-3:/#

root@pc-4:/# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:07:e9:44:44:44
          inet addr:11.0.0.14  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::580b:18ff:fe1e:83e1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:53 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3162 (3.1 KB)  TX bytes:648 (648.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:256 (256.0 B)  TX bytes:256 (256.0 B)

root@pc-4:/#
```

2. Inicia una captura de tráfico en pc3. Para ello ejecuta los siguientes comandos. En pc3:

```
pc3:~# tcpdump -i eth0 -s 0 -w /hosthome/pc3.cap
```

Ahora vas a generar tráfico de la siguiente forma: pc1 va a enviar una trama Ethernet a pc2 y pc2 va a responder. Para ello ejecuta en pc1:

```
pc1:~# arping -c 1 00:07:e9:22:22:22
```

Donde:

La dirección Ethernet que estamos utilizando (00:07:e9:22:22:22) es la dirección Ethernet destinataria de las tramas, en este caso la de pc2.

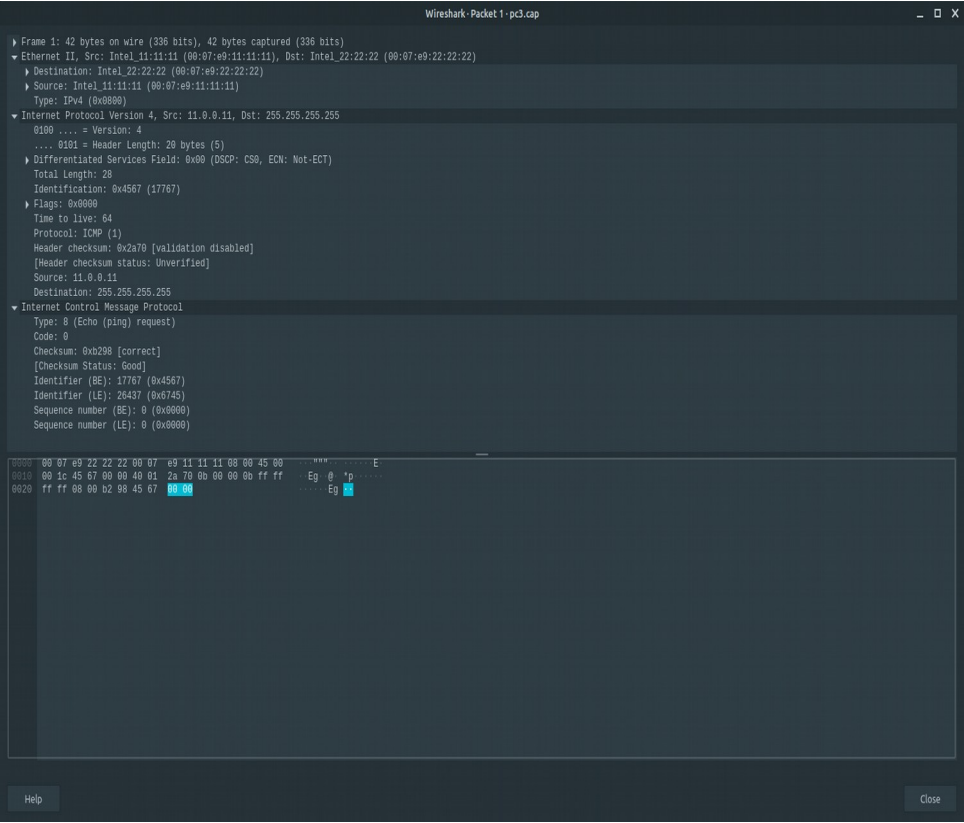
La opción -c 1 hace que arping envíe un único paquete a la máquina pc2 y que ésta le responda.

Interrumpe la captura pulsando Ctrl+C en la ventanas de pc3.

Analiza las tramas Ethernet que aparecen en la captura. Para cada paquete indica:

- (a) Dirección Ethernet origen.
- (b) Dirección Ethernet destino.
- (c) ¿Qué crees que se hubiera capturado en las interfaces de pc1(eth0), pc2(eth0), pc4(eth0) si hubiéramos arrancado también tcpdump en dichas interfaces? ¿Por qué?
- (d) Indica qué máquinas reciben la primera trama capturada y qué máquinas la procesan y se la entregan al protocolo de nivel superior.
- (e) Indica qué máquinas reciben la segunda trama capturada y qué máquinas la procesan y se la entregan al protocolo de nivel superior.
- (f) Si la primera trama llevara como dirección destino ff:ff:ff:ff:ff:ff indica qué máquinas recibirían dicha trama y qué máquinas se la entregarían al protocolo de nivel superior.

Primer Paquete:



(a) 11.0.0.11

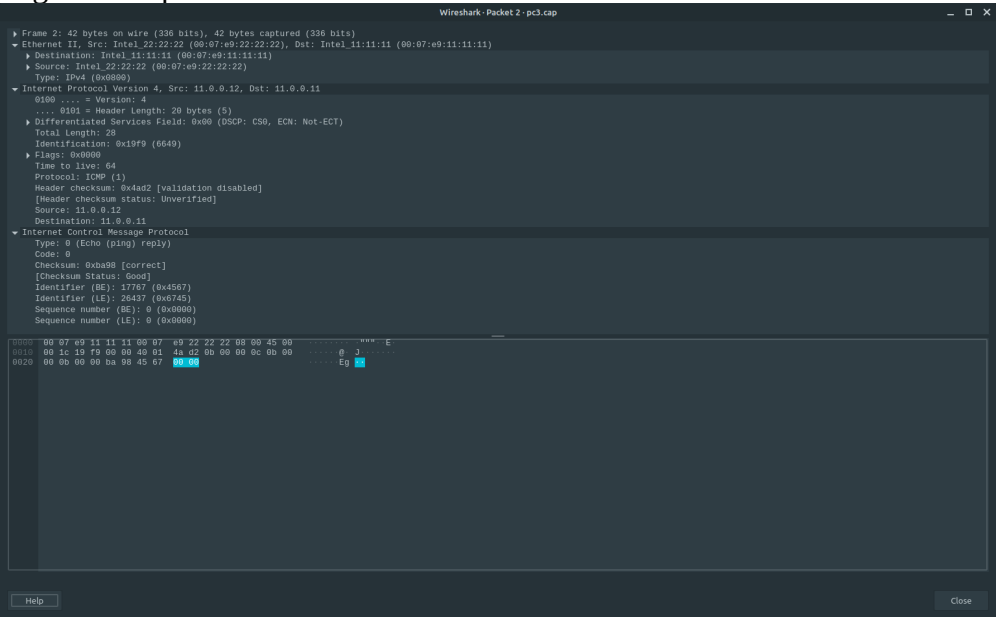
(b) 11.0.0.12

(c) Todas hubieran capturado exactamente lo mismo debido que al estar conectadas a un hub las pc todas reciben los mismos paquetes siempre. Sin importar a donde se dirijan.

(d) todas las maquinas la reciben, pero es procesada solo por pc2.

(f) La recibirían todas las maquinas aunque solo pc2 la entregaría al protocolo de nivel superior.

Segundo Paquete:



(a) 11.0.0.12

(b) 11.0.0.11

(c) Todas hubieran capturado exactamente lo mismo debido que al estar conectadas a un hub las pc todas reciben los mismos paquetes siempre. Sin importar a donde se dirijan.

(e) todas las maquinas la reciben, pero solo es procesada por pc1.

