PL4 (GP8): soluciones a la práctica de laboratorio de ARP

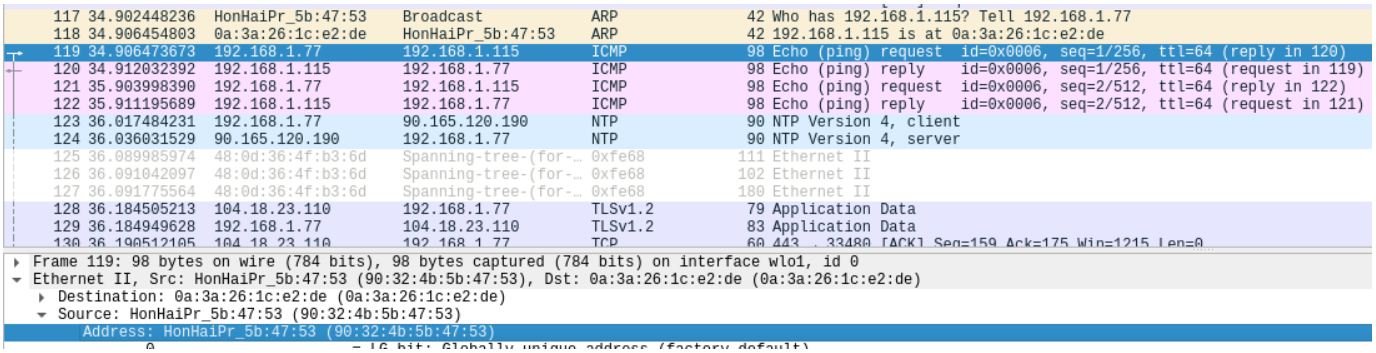
Nombres:Raúl López Llana **Puesto:** **Grupo:Tarde**

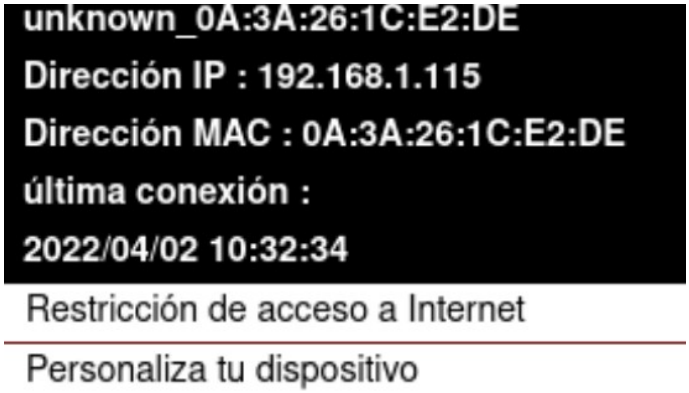
1.- Observe uno de los mensajes ICMP echo request del ping en b) ¿Cuál es la dirección Ethernet de su máquina? ¿Cuál es la dirección destino, coincide con la dirección Ethernet del mismo (pida que lo consulte con ifconfig)? ¿Qué valor tiene el campo “Tipo de trama” y qué indica?

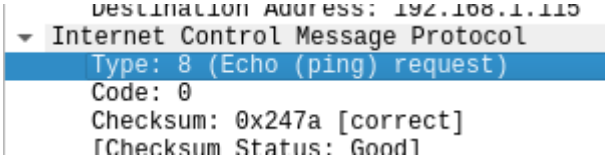
La dirección mac desde la que envío el icmp echo request es “90:32:4b:5b:47:53” como se puede ver en la primera imagen.

La mac destino se encuentra justo en la línea de arriba a la mia, “0a:3a:26:1c:e2:de”. Coinciden tanto la mac como la ip destino, para ello me he asegurado entrando en la configuración del router y he vistos los dispositivos conectados. Otra forma seria mirarlo en el propio dispositivo y también coincide.

El tipo de la trama ICMP es 8 y con un code = 0, esto significa “Echo (ping) request”.



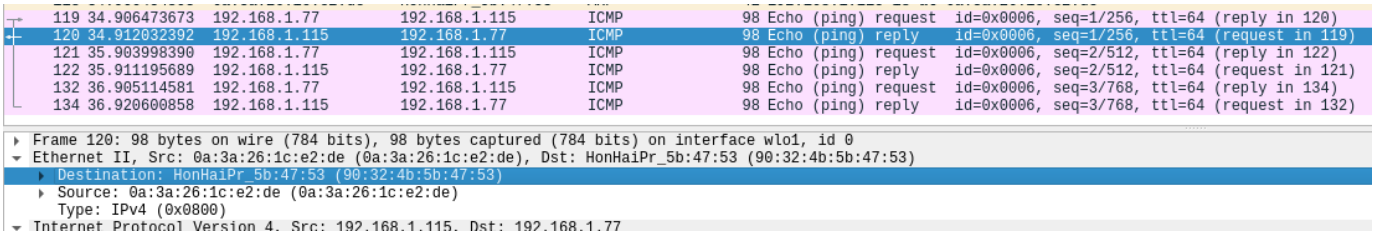


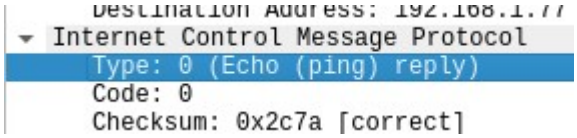


2.- Seleccione ahora uno de los mensajes ICMP echo reply del ping en b) ¿Cuáles son las direcciones Ethernet origen y destino y a quién corresponden? ¿Qué valor tiene el campo “Tipo de trama” y qué indica?

El mensaje ICMP echo reply nos aporta como información que la dirección de origen es “0a:3a:26:1c:e2:de” y la de destino es la “90:32:4b:5b:47:53”. Esto se puede confirmar con la imagen que encontramos abajo.

El campo de tipo de trama contiene 0 y el code también es 0. Esto nos indica que estamos ante un “Echo (ping) reply”.



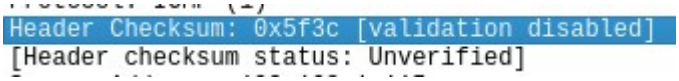


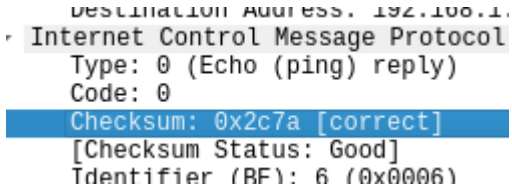
3.- Respecto al último mensaje, ¿qué valor tiene el campo “CRC” de la trama Ethernet? ¿dónde se encuentra ubicado?

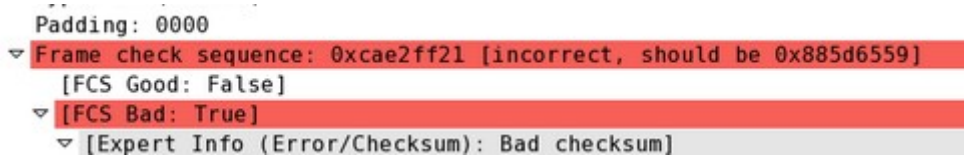
En mi caso, la validación en la cabecera la tengo des habilitada como se observa en la imagen.

En cuanto al contenido, si que realizar el checksum y es correcto.

Tras estar buscando un poco de información, en caso de que el checksum sea incorrecto se nos mostraría como en la tercera imagen.







4.- Observe ahora uno de los mensajes ICMP echo request de cada ping realizado en c) a diferentes destinos ¿Cuál es la dirección Ethernet origen? ¿Cuál es la dirección Ethernet destino, coincide con la dirección Ethernet de los servidores www.google.es o www.yahoo.es? Dibuje un pequeño esquema con las direcciones IP y Ethernet que entran en juego para explicar lo que sucede.

La dirección de origen es " 192.68.1.77" con mac "90:32:4b:5b:47:53" y la destino "142.250.185.3" con mac "48:8d:36:4f:b3:6b0".

Tras buscar información, podemos llegar a ver y afirmar que es la dirección de un servidor de google.

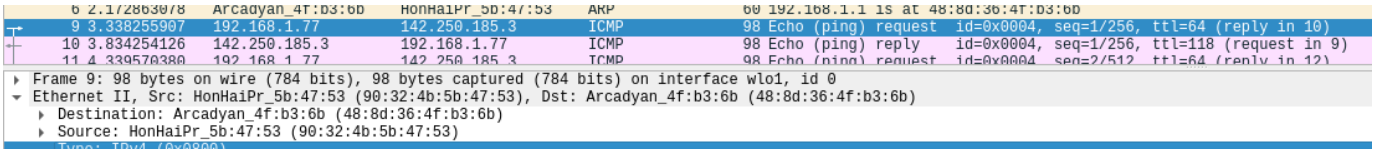
Realizo un traceroute como se observa en la tercera imagen. Lo primero que hace es una ARP para conocer la dirección de nuestro router.

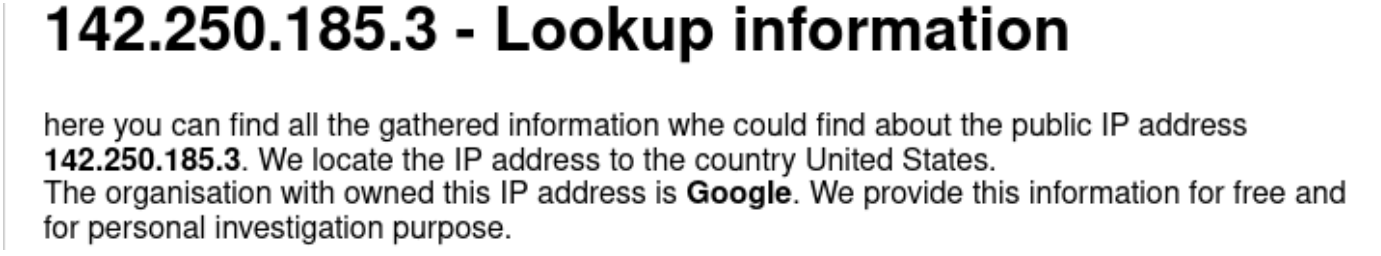
Una vez conocida la mac de nuestro router, empezamos a enviar paquetes de 3 con TTL desde 1 y vamos incrementándolo por cada paso de un nodo. Estos nos irán devolviendo por donde van pasando nuestros paquetes y así podremos saber el camino que han seguido.

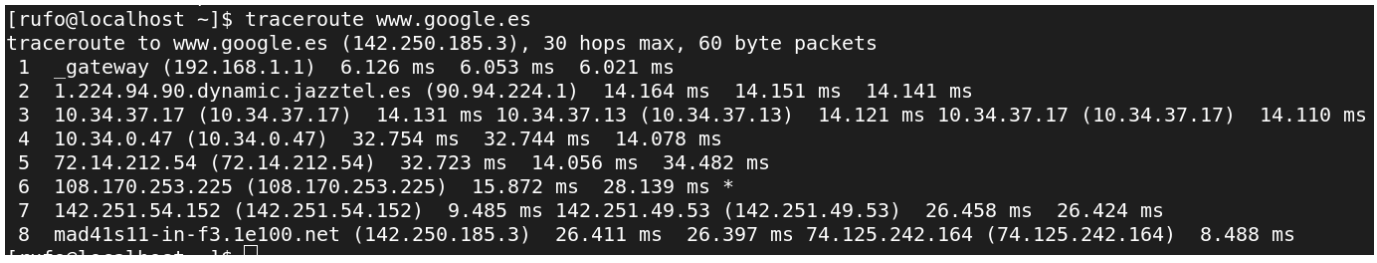
Nosotros enviamos paquetes UDP y como no llegan al destino a causa de su TTL tan bajo, recibiremos paquetes ICMP indicando que el TTL ha expirado.

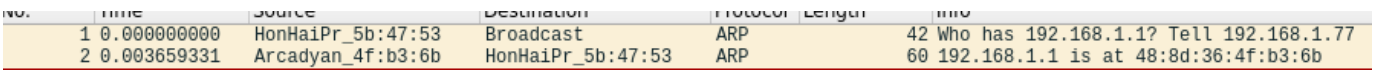
Para que quede más clara la explicación, inserto un dibujo que describe muy bien como van pasando los paquetes por cada router y estos nos van contestando. Esta imagen está sacada de "https://www.hackingarticles.in/working-of-traceroute-using-wireshark/".

Durante el camino del traceroute puedo ir viendo las direcciones IP de por donde pasa pero las direcciones mac no.

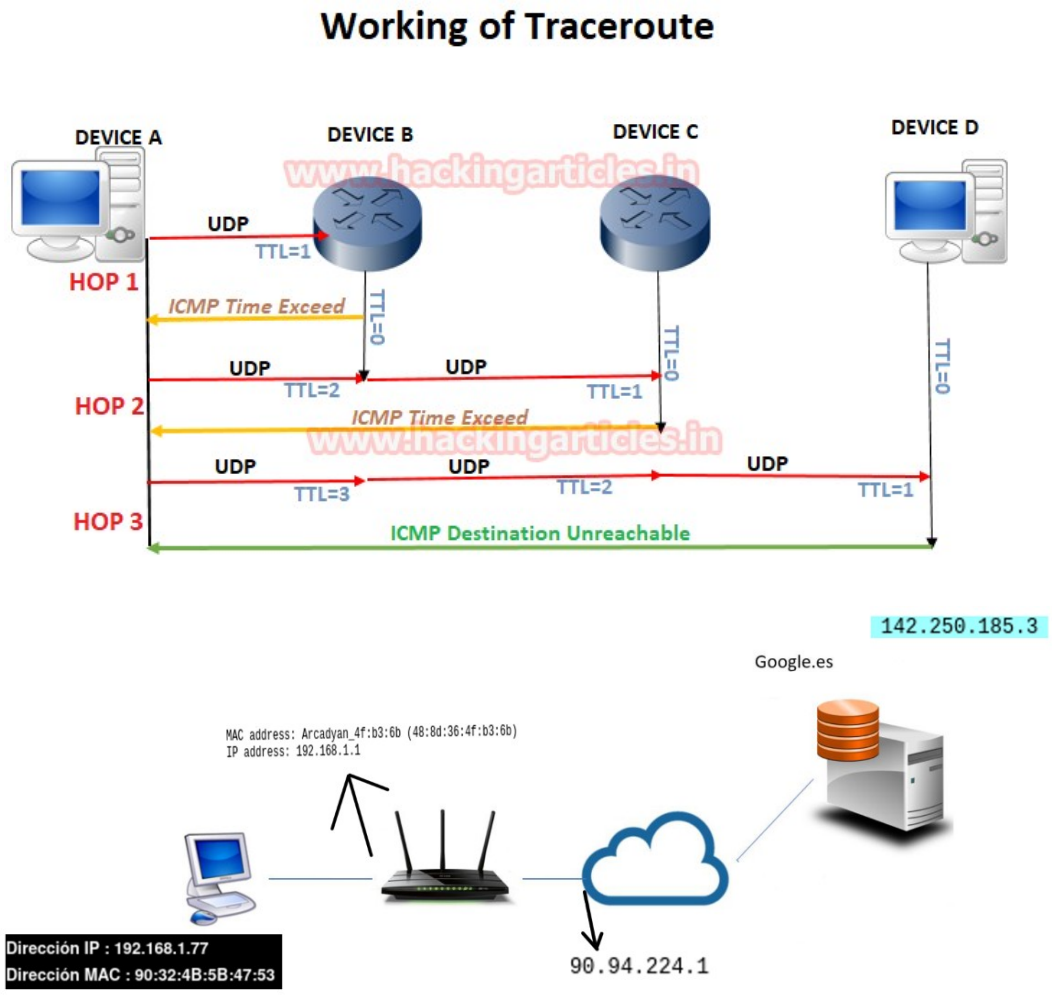








3 0.003662994	192.168.1.77	142.250.185.3	UDP	74 37162 → 33434 Len=32
4 0.003665935	192.168.1.77	142.250.185.3	UDP	74 44303 → 33435 Len=32
5 0.003666689	192.168.1.77	142.250.185.3	UDP	74 49285 → 33436 Len=32
6 0.003667303	192.168.1.77	142.250.185.3	UDP	74 33476 → 33437 Len=32
7 0.003667993	192.168.1.77	142.250.185.3	UDP	74 58493 → 33438 Len=32
8 0.003668600	192.168.1.77	142.250.185.3	UDP	74 42991 → 33439 Len=32
9 0.003669234	192.168.1.77	142.250.185.3	UDP	74 52652 → 33440 Len=32
10 0.003669839	192.168.1.77	142.250.185.3	UDP	74 56206 → 33441 Len=32
11 0.003670528	192.168.1.77	142.250.185.3	UDP	74 60062 → 33442 Len=32
12 0.003671145	192.168.1.77	142.250.185.3	UDP	74 44700 → 33443 Len=32
13 0.003671806	192.168.1.77	142.250.185.3	UDP	74 47253 → 33444 Len=32
14 0.003672475	192.168.1.77	142.250.185.3	UDP	74 37174 → 33445 Len=32
15 0.003673087	192.168.1.77	142.250.185.3	UDP	74 34490 → 33446 Len=32
16 0.003673697	192.168.1.77	142.250.185.3	UDP	74 56460 → 33447 Len=32
17 0.003674299	192.168.1.77	142.250.185.3	UDP	74 34352 → 33448 Len=32
18 0.003674944	192.168.1.77	142.250.185.3	UDP	74 42103 → 33449 Len=32
19 0.006103966	192.168.1.1	192.168.1.77	ICMP	102 Time-to-live exceeded
20 0.006104033	192.168.1.1	192.168.1.77	ICMP	102 Time-to-live exceeded
21 0.006104065	192.168.1.1	192.168.1.77	ICMP	102 Time-to-live exceeded
22 0.006579089	192.168.1.77	142.250.185.3	UDP	74 56912 → 33450 Len=32
23 0.006595255	192.168.1.77	142.250.185.3	UDP	74 47646 → 33451 Len=32
24 0.006628260	192.168.1.77	142.250.185.3	UDP	74 53965 → 33452 Len=32



5.- ¿Qué significado tiene cada columna de las que se muestran al ejecutar la orden “arp -a”?

Con el comando arp -a muestra todos los host´s que están almacenados en ese momento en cache.

El resultado esta compuesto por la direccion IP del dispositivo (no es la nuestra), su dirección mac y la interfaz por la que se puede llegar a el.

Las columnas pueden varias según el entorno en el que ejecutemos el comando. En la segunda imagen se observa la ejecución del mismo comando pero desde un sistema windows y observamos que este muestra si es de tipo estático o dinámico. En otros sistemas llega incluso a mostrar la hora en la que se ha creado esa entrada.

```
? (192.168.1.115) at 0a:3a:26:1c:e2:de [ether] on wlo1
_gateway (192.168.1.1) at 48:8d:36:4f:b3:6b [ether] on wlo1
```

```
C:\>arp -a

Interfaz: 172.20.1.68 --- 0x2
  Dirección de Internet          Dirección física      Tipo
  172.20.1.69           14-da-e9-a[redacted]     dinámico
  172.20.1.70           14-da-e9-a[redacted]     dinámico
  172.20.1.72           14-da-e9-a[redacted]     dinámico
```

6.- Si tras el borrado consultamos de nuevo la tabla caché de ARP, ¿qué información se muestra? Como curiosidad espere 1 o 2 minutos sin interactuar con su PC y vuelva a consultar por tercera vez dicha tabla, ¿observa algún cambio? ¿qué está sucediendo?

Tras borrar la caché, el resultado obtenido es ninguno ya que no le ha dado tiempo a realizar un ARP.

Tras esperar unos minutos obsevamos que ha creado una entrada y es la que nos conectaria con el router, esto se debe a que aunque nosotros no estemos haciendo nada, por detras puede haber un proceso que haya realizado una consulta o petición a fuera de nuestro ordenador y para llevarla a cabo, es necesario realizar un ARP

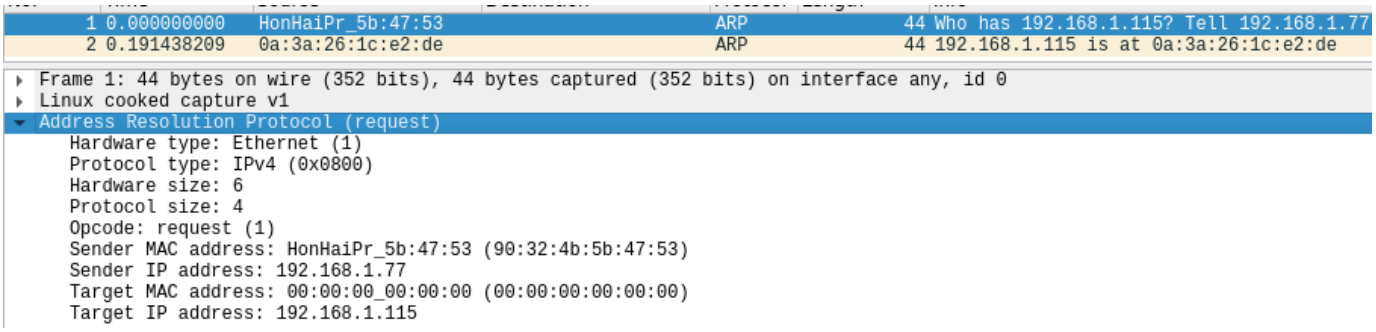
```
[rufo@localhost ~]$ sudo ip -s -s neigh flush all
Nothing to flush.
[rufo@localhost ~]$ sudo ip -s -s neigh flush all
192.168.1.1 dev wlo1 lladdr 48:8d:36:4f:b3:6b ref 1 used 3/3/3 probes 4 REACHABLE

*** Round 1, deleting 1 entries ***
*** Flush is complete after 1 round ***
[rufo@localhost ~]$ arp -a
[rufo@localhost ~]$
```

```
[rufo@localhost ~]$ arp -a
_gateway (192.168.1.1) at 48:8d:36:4f:b3:6b [ether] on wlo1
```

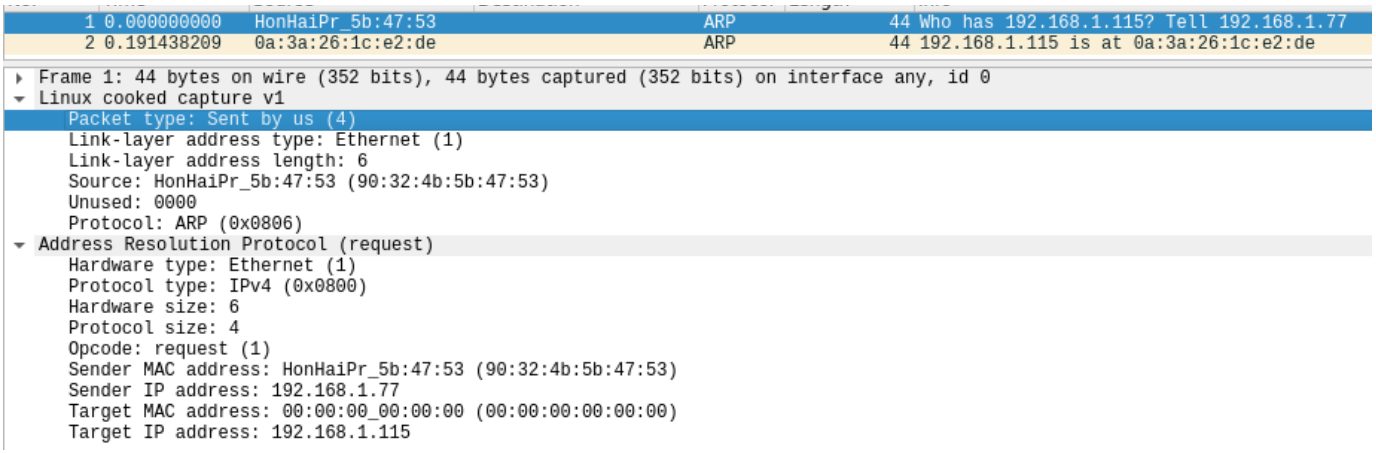
7.- ¿Qué valores hexadecimales contienen las direcciones Ethernet origen y destino en la petición ARP (ARP Request)?

Observamos que la dirección de origen es “192.168.1.77” y la destino es “192.168.1.77”.



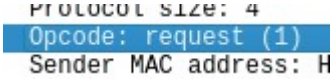
8.- ¿Qué valor tiene el campo “Tipo de trama”? y ¿qué indica?

Asumiendo que “Tipo de trama” hace referencia a “Packet type”, observamos que tiene como valor 4 que significa que el paquete ha sido enviado por nosotros.



9.- ¿Qué valor tiene el campo “opcode” del mensaje ARP? ¿qué significa?

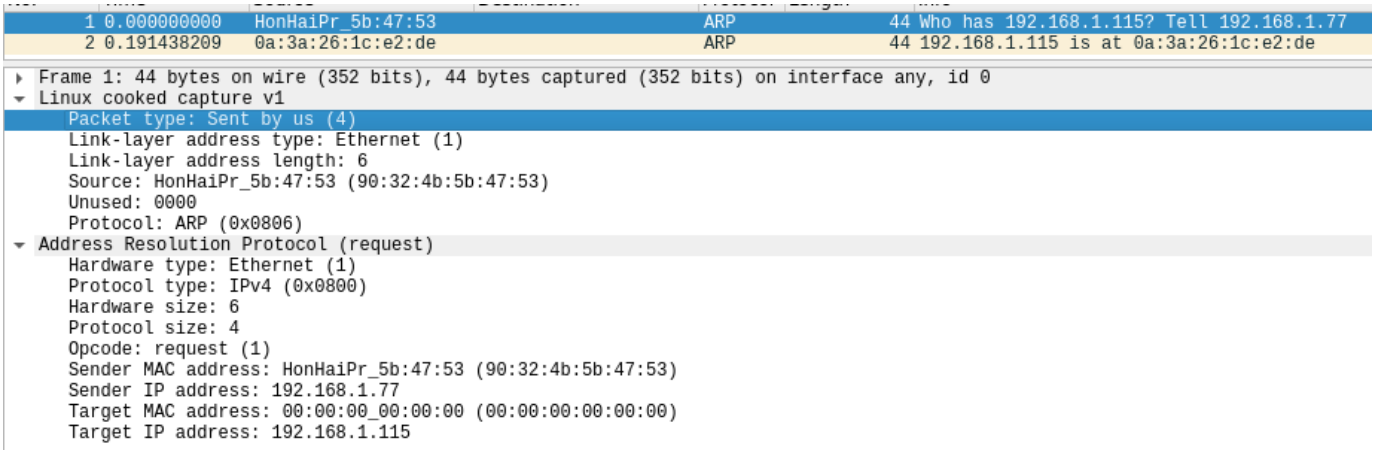
EL CAMPO OPCODE INDICA EL TIPO DE PAQUETE ARP, SOLO EXISTEN 2 VALORES (1 Ó 2) Y ESTE CONTIENE EL VALOR 1 QUE INDICE ARP REQUEST.



10.- ¿Contiene el mensaje ARP la dirección IP de la máquina que envía la petición? ¿dónde aparece la petición en sí, cómo la podemos identificar?

Si, el mensaje ARP contiene nuestra dirección ya que al llegar al destino, este debe saber a donde tiene que responder.

Podemos identificar viendo el primer paquete ARP que es capaz de capturar Wireshark que es el que enviamos nosotros y si bajamos hasta “sender IP” o “sender MAC”, estos campos contendrán tanto la ip como la dirección MAC de nuestro dispositivo.

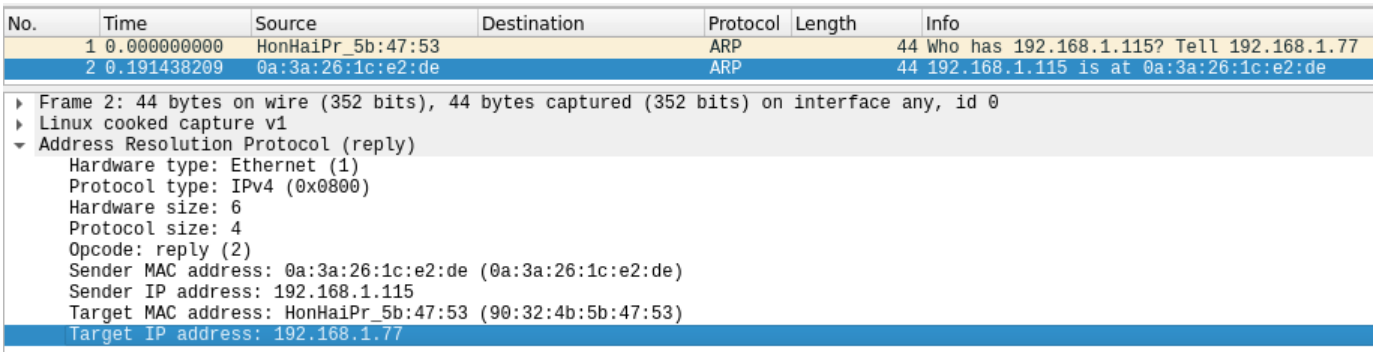


11.- ¿Cuáles son las direcciones Ethernet origen y destino de esta nueva trama? ¿a quién pertenecen? ¿qué diferencias hay entre la petición y la respuesta ARP?

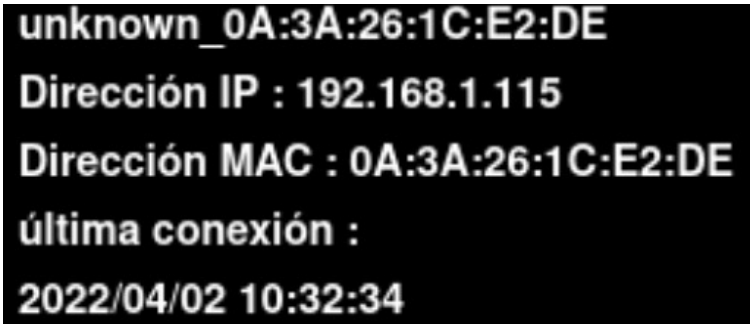
La dirección de origen del paquete ARP Reply es “0a:3a:26:1c:e2:de” y la de destino es “0a:3a:26:1c:e2:de”.

La dirección de origen pertenece al dispositivo contra el que hemos hecho el ping y la de destino es nuestra propia máquina.

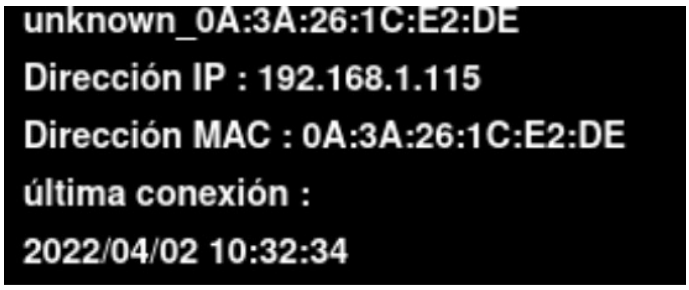
La diferencia entre una y otra es que se intercambia la Mac de origen por la de destino y viceversa. Y cambia el “Packet type” que al enviarlo es 4 “Sent by us” y a la vuelta es 0 “Unicast to us”.



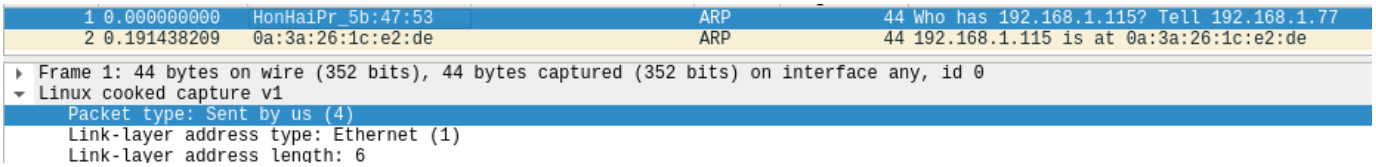
El móvil



El ordenador



Request

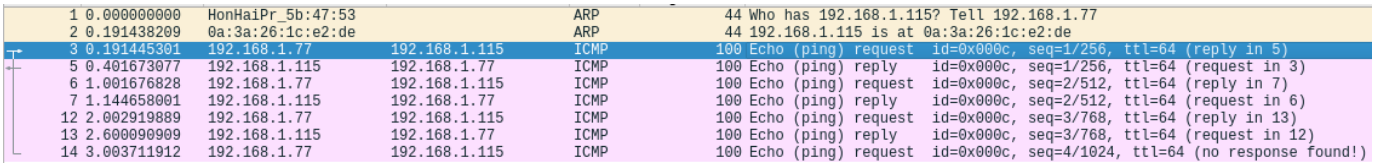


Reply

12.- ¿Explique el proceso ARP tras el primer ping?, ¿qué sucede cuando ejecuta el segundo ping?

Tras el primer ping, el ordenador tiene almacenado en caché el resultado del ARP por lo que no le hace falta volver a enviar una consulta para saber la MAC del destinatario.

Hará uso de esta entrada y continuará con el ping



13.- ¿Cree que es posible diferenciar cuándo se ha emitido un ARP y cuándo no, en el terminal, viendo los resultados (tiempos) que muestra la orden ping ejecutada? Razone la respuesta

Dependiendo de lo lejano que se encuentre el dispositivo al que queremos realizar el ping.

Si ha de pasar por muchos intermediarios podremos llegar a ver una demora superior a la media en el primer paquete enviado. Pero si por el contrario el dispositivo se encuentra muy cerca (1 o 2 saltos), el tiempo en realizar ARP será tan pequeño que será difícil observar desde consola esto.

14.- Finalmente, busque en la captura otras peticiones ARP (ARP Request) no emitidos por su máquina, ¿qué significa esto? ¿Por qué sin embargo no se ve ninguna respuesta (ARP Reply) aparte de la que se generó con el comando ping?

En mi caso no he encontrado un paquete como el se está pidiendo pero podría llegarse a encontrar cuando alguno de los hosts que se encuentran en mi misma red estuviesen intentando hacer un ARP para encontrar a otro equipo.

No veríamos ningún ARP Reply ya que no están atentando contra nuestro equipo, sino con otro mediante un unicast.

OPCIONAL

Op 1.- ¿Qué ocurre? ¿Es capaz ARP de resolver este problema de forma automática?, ¿hasta cuándo se tendrá esta situación?

Observamos que se ha creado una nueva entrada con los datos que hemos introducido.

No es capaz de resolver este problema ya que para la máquina no existe ningún problema. Al intentar hacer un ping contra el dispositivo, seremos incapaces de llegar a el pero esto no se cambiará hasta que pase el tiempo que dura cada entrada en la tabla de ARP.

```
[rufo@localhost ~]$ arp -a
_gateway (192.168.1.1) at 48:8d:36:4f:b3:6b [ether] on wlo1
[rufo@localhost ~]$ sudo arp -s 192.168.1.115 01:00:5f:ab:cc:de
[sudo] password for rufo:
[rufo@localhost ~]$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.115            ether   01:00:5f:ab:cc:de   CM                    wlo1
192.168.1.1              ether   48:8d:36:4f:b3:6b   C                     wlo1
[rufo@localhost ~]$
```

Op 2.- ¿Cuánto tiempo dura una entrada en la caché? (/proc/sys/net/ipv4/Leigh/eth0/gc_stale_time).

El tiempo que dura una nueva entrada en caché es de 60 segundos en mi ordenador, esto puede variar segun el dispositivo o lo que nosotros queramos configurar.

```
[rufo@localhost ~]$ cat /proc/sys/net/ipv4/neigh/wlo1/gc_stale_time
60
[rufo@localhost ~]$
```