CAPÍTULO 7
ENLACE: ETHERNET, ARP Y SWITCHING

Matías Robles

Introducción

Para finalizar con el conjunto de actores introducidos en el Capítulo 1 vamos a analizar los dos últimos, Ethernet[SZ14] y ARP[Plu82], correspondientes a la capa de enlace. Esta capa se diferencia del resto de las capas vistas hasta el momento en que puede ir cambiando a medida que un mensaje se mueve entre distintas redes. Por ejemplo, el host origen de un paquete IP podría estar en una red wireless, del tipo IEEE 802.11, que define un formato específico de trama (en inglés frame) en la capa de enlace, pero, si en su camino hacia el host destino debe ser enviado por una red con una tecnología diferente, posiblemente Ethernet, el paquete IP será encapsulado en otro tipo de trama.

En ese camino entre un origen y un destino el direccionamiento lógico, direcciones IP, es común a todas las redes, pero no sucede lo mismo con el direccionamiento físico, que es propio de cada tecnología de interfaz de red (network interface). En el caso de Ethernet, ese direccionamiento físico está representado por direcciones MAC (Medium Access Control, también llamada Media Access Control). Para poder enviar un mensaje son necesarias direcciones de esos dos niveles, pero son dos identificadores totalmente diferentes. Si se necesita enviar un mensaje a un host y se conoce su dirección IP se requiere algún mecanismo que sea capaz de averiguar la dirección MAC asociada a esa dirección IP. Cómo funciona este mecanismo es uno de los temas que se verán en este capítulo.

Antes de introducirnos en esos temas es necesario que se comprendan dos conceptos fundamentales para entender el contenido de este capítulo: dominio de colisión y dominio de broadcast. El primero, define cual es la parte de la red en la que si un nodo transmite tiene posibilidades de colisionar con la trasmisión de otro nodo y, por su parte, el segundo define cual es la parte de una red en la que un mensaje de tipo broadcast viajará sin ser detenido. El alcance de cada uno de esos dominios depende de los dispositivos de red que se utilicen. Los switches dividen los dominios de colisión y los routers hacen lo mismo tanto con los dominios de colisión como con los de broadcast (los hubs no dividen ninguno de los dos dominios). Usando el gráfico en la figura 7.1, que es una parte de la red usada en el desarrollo del libro, podemos ver cuales son cada uno de estos dominios.

La posibilidad de colisión se debe a que Ethernet originalmente se definió como un mecanismo de acceso a un medio de forma compartida, CSMA/CD, donde solo se podía tener una transmisión en

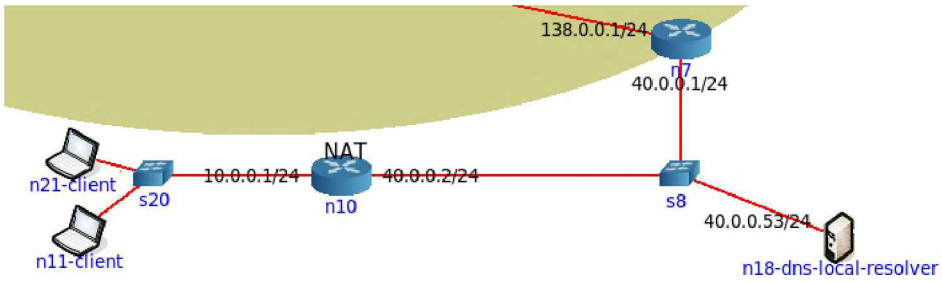

Figura 7.1: Dominios de Colisión y de Broadcast

curso. En la parte de la red donde está el switch *s20* hay 3 dominios de colisión. Cada uno de los nodos están conectados punto a punto a ese switch, inclusive la interfaz del router en esa red, lo que se conoce como micro-segmentación, y cada una de esos conexiones es un dominio de colisión diferente. Por su parte, se tiene un solo dominio de broadcast. Dentro de esa misma red, cualquier mensaje de tipo broadcast llegará a todos los nodos, pero el router no lo reenviará hacia la otra red: el router detiene los mensajes broadcast. Siguiendo con el gráfico en la red donde está el switch *s8* también se tienen 3 dominios de colisión y uno solo de broadcast.

Ethernet

Ethernet es un estándar que define las dos últimas capas del modelo OSI, la capa de enlace y la física, y consta de dos versiones: Ethernet, definida por el consorcio DIX (Digital Equipment Corporation (DEC), Xerox e Intel) y actualmente en la versión 2, Ethernet II, y el estándar IEEE 802.3. Ambas versiones son similares y coexisten en la realidad (si se realiza una captura de tráfico muy probablemente se verá tráfico de ambas versiones). Solo tiene alcance dentro del dominio de broadcast en el cual es generada, lo que significa que una trama, ese es el nombre que recibe una PDU en la capa de enlace aunque también se lo suele llamar marco o directamente en su término nativo frame, no será reenviada por un dispositivo de capa 3. Esto implica que la trama viajará por la propia LAN sin alteraciones ni modificaciones y será recibida y procesada por uno o más equipos según el direccionamiento y los equipos de red involucrados.

Con el fin de comprender el papel que desempeña en todo el proceso que se viene desarrollando a lo largo del libro, es que se comenzará por analizar una trama Ethernet, la cual se puede ver en la figura 7.2

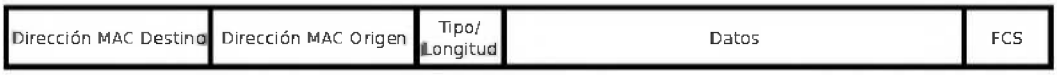

Figura 7.2: Trama Ethernet II/IEEE 802.3

Dirección MAC Destino: 6 bytes. Puede ser de tipo unicast, multicast o broadcast. Indica cual o cuales son los posibles receptores de la trama.

Dirección MAC Origen: 6 bytes. Solo puede ser de tipo unicast e indica cual es el dispositivo que generó la trama. Un dispositivo utilizará su dirección MAC como dirección origen en cualquier trama

que transmita. Si tuviese más de una interfaz de red seleccionará la dirección MAC de la interfaz por donde enviará la trama.

Tipo/Longitud: 2 bytes. Este campo es diferente en Ethernet II y IEEE 802.3. En Ethernet II se usa como Tipo e indica que protocolo de capa superior se está transportando en el campo Datos, en cambio, en IEEE 802.3 se usa como Longitud e indica la cantidad de bytes transportados en el campo Datos. Si el valor del campo es menor o igual a 1500 (decimal) entonces el campo está siendo usado como Tipo y si es mayor o igual a 1536 decimal (0x600 hexadecimal) entonces se lo está usando como Longitud.

Datos: mínimo de 46 bytes, máximo de 1500. Si es menor a 46 bytes se deben agregar bytes de padding hasta llegar a ese tamaño. En Ethernet II, el tamaño mínimo de trama esta garantizado por la capa superior y en IEEE 802.3 el campo Longitud indica la cantidad de datos sin relleno (padding). Por ejemplo, en este campo viajarían los paquetes IP o ARP.

FCS (Frame Check Sequence): 4 bytes. Permite chequear la integridad de la trama. Su valor es calculado usando un CRC, Cyclic Redundancy Check, por el emisor. Si su chequeo falla en el receptor de la trama, éste la descartará sin avisarle al emisor.

Una trama Ethernet, sin modificaciones, tiene un tamaño máximo de 1518 bytes, pero este valor puede sufrir alteraciones. Por ejemplo, si definimos VLANs usando el estándar IEEE 802.1Q se le deben agregar 4 bytes a cada trama para transportar información de la VLAN, lo que lleva el tamaño de la misma a 1522 bytes. Evoluciones del estándar Ethernet permiten sobrepasar este límite dando lugar a lo que se conoce como jumbo-frames, comúnmente puede llevar una carga útil (datos) de hasta 9000 bytes.

En cuanto al direccionamiento en la trama, tanto las direcciones origen como destino son direcciones MAC. Estas son direcciones de 48 bits que se las divide en 2 partes de 24 bits cada una. La primera mitad es conocida como OUI, Organizationally Unique Identifier, sirve para identificar a los distintos fabricante (Cisco, Intel, Broadcom, etc.) y es administrada por la IEEE. La segunda mitad de la dirección es asignada por cada uno de los fabricantes, quienes deben garantizar la unicidad de cada dirección MAC. Cada dispositivo en el mundo que forme parte de una red de tipo Ethernet tiene una dirección MAC diferente. Esta dirección pertenece a la placa de red, no al dispositivo (si se le cambia la placa de red a un dispositivo también se le cambia su dirección MAC).

Ethernet ha estado evolucionando constantemente desde sus inicios en la década del 70, pasando de los 10 Mbits/s iniciales a los 100 Gbit/s en la actualidad. También, ha dejado de ser un medio half-duplex (todos los dispositivos pueden transmitir pero no simultáneamente) para transformarse en un medio completamente full-duplex (todos los dispositivos pueden transmitir simultáneamente), lo que sucede desde la versión de los 10 Gbit/s (IEEE 802.3ae del año 2002). Aunque originalmente no fue la única tecnología disponible para las redes LANs, en sus inicios compitió entre otras con Token Bus (IEEE 802.4) y Token Ring (IEEE 802.5), con el tiempo se convirtió en el estándar de-facto para ese tipo de redes. En los últimos años se puede ver que las redes WI-FI, IEEE 802.11, han gozado de gran

popularidad entre las redes LAN.

Entre las características en las que se ha basado su éxito se puede mencionar su simplicidad. Comparada con el resto de sus competidores, Ethernet es más simple de entender, implementar y configurar. Simplemente, se puede decir que en Ethernet cuando un nodo quiere enviar una trama, lo hace. No tiene que esperar un turno o, como en Token Ring, un token que lo habilite a transmitir. Sin embargo, es preciso indicar que tiene un procesamiento distinto entre las versiones half-duplex y full-duplex.

Al operar en modo half-duplex, cuando un nodo quiere transmitir hace uso del método de acceso CSMA/CD (Carrier Sense Multiple Access/Collision Detection). Sin profundizar en los detalles, antes de transmitir una trama el nodo debe "sensar el medio", es decir, escuchar el medio para determinar si hay otra transmisión en curso. Si la hay, debe esperar hasta que la actual transmisión finalice para luego intentar transmitir. En caso contrario, el nodo envía su trama. Si dos o más dispositivos transmiten simultáneamente las tramas colisionarán y, en consecuencia, se perderán. Obviamente, estas tramas se deben volver a enviar, pero si todos los nodos involucrados en la colisión deciden enviar esas tramas inmediatamente después de la colisión, volverán a colisionar. Para evitar esto, es que cada nodo, de manera totalmente independiente, ejecuta un algoritmo de back-off que indica un tiempo aleatorio que cada nodo deberá esperar antes de volver a transmitir. Esto no evita por completo que al transmitir nuevamente esas tramas vuelvan a colisionar. En este caso, los nodos involucrados deberán ejecutar nuevamente el algoritmo de back-off. Esto se repetirá en cada nodo hasta que pueda transmitir la trama de manera exitosa o hasta que de error después de una cantidad de intentos fallidos. Esta aleatoriedad, no poder garantizar quien será el próximo en transmitir, es lo que convierte a Ethernet en un protocolo no determinístico.

Si la trama es transmitida exitosamente, sin colisiones, arribará a un nodo o varios nodos destino. Al recibir la trama, cada nodo primero debe verificar la integridad de la misma, lo que realiza mediante el cálculo del CRC. Si éste es correcto, la trama es aceptada; en caso contrario, es descartada y lo hace en modo silencioso, sin avisar nada al emisor. Algún protocolo de la capa superior en el nodo emisor deberá encargarse de detectar la pérdida de los datos e iniciar una retransmisión. A continuación, el receptor controla que la MAC destino de la trama coincida con la MAC asignada a la interface de red por donde se la recibió. Si coincide, la aceptará para su procesamiento, caso contrario, la descartará. También aceptará tramas con dirección MAC destino de tipo broadcast o multicast, en este último caso solo si el nodo está escuchando en la correspondiente dirección multicast.

En el modo full-duplex, las estaciones se comunican usando un medio de transmisión dedicado, punto a punto. Cuando un nodo quiere transmitir no debe esperar para hacerlo ni tiene que quedarse "sensando" el medio por una posible colisión una vez que lo hizo. No hay posibilidad de colisiones en un medio de este tipo. Consecuentemente, tampoco es necesario ejecutar un algoritmo de acceso al medio, como CSMA/CD, debido a que no hay contención por la utilización de un medio compartido. Si se quiere tener una red LAN de tipo full-duplex es necesario contar con un switch y conectar un único

dispositivo a cada uno de sus puertos. No es posible, en estos casos, utilizar un hub o repetidor. De hacerlo, el funcionamiento de la misma pasaría a ser half-duplex.

ARP

Si bien Ethernet es la tecnología de LAN más utilizada en la actualidad, no es la única. Como se explicó en la introducción del capítulo, un paquete IP puede pasar por distintos tipos de redes físicas con sus propios formatos de trama y direccionamiento en su capa de enlace. Este funcionamiento podría requerir, entre otras cosas, realizar una conversión entre las direcciones utilizadas en la capa de red (direccionamiento lógico) y las de la correspondiente capa de enlace (direccionamiento físico). En nuestro caso nos referimos específicamente al procedimiento de mapear direcciones IP de 32 bits en direcciones MAC de 48 bits. Este método es común para todos los estándares que utilicen direcciones MAC, como sucede con las redes Ethernet o WI-FI. El protocolo de capa de enlace encargado de realizar esta tarea es ARP (Address Resolution Protocol) definido en la RFC-826. Si bien este protocolo puede ser usado para otras finalidades, como la detección de direcciones duplicadas, en este capítulo nos vamos a enfocar en la funcionalidad de mapear direcciones IP en direcciones MAC.

> Algunos autores suelen ubicar a ARP en el medio de las capas de red y enlace indicando que pertenece a la capa 2.5 (dos y medio).

Aunque es un protocolo presente en prácticamente todas las redes LANs su uso es transparente tanto para los usuarios de la red, inclusive el administrador de la misma, como para las aplicaciones. ARP realiza todo su trabajo de forma dinámica, no necesita ninguna configuración ni administración. El mapeo de una dirección IP a la correspondiente dirección MAC se va haciendo a medida que se necesita, lo que posibilita que la red se adapte a los cambios que vayan sucediendo. Esto implica que si un nodo cambia su placa de red, y en consecuencia su dirección MAC, el administrador de la red no deberá hacer nada para que los demás nodos de la LAN se den cuenta de este cambio.

> ARP funciona únicamente con IPv4. En IPv6, en su reemplazo, se utiliza una de las funciones provistas en el protocolo Neighbor Discovery.

ARP no está definido para ningún tipo de direccionamiento en particular, es un protocolo genérico desarrollado para mapear direcciones de diferentes protocolos de capa de red en direcciones físicas de distintos tamaños, pero en la RFC-826 se habla específicamente de direcciones físicas de 48 bits de una red Ethernet. Y en cuanto a la capa de red, raramente se la utiliza con direcciones distintas a IPv4. Es un protocolo con un funcionamiento muy simple que solo define dos tipos de mensajes, ARP Request y ARP Reply, que al enviarse son encapsulados en el campo Datos de una trama Ethernet. En el análisis de esos paquetes ARP solo nos vamos a enfocar en los campos "Hardware Address", que se corresponden con las direcciones MAC, y "Protocol Address", que lo hacen con las direcciones IPv4.

Cuando un host tiene un mensaje para enviar va a necesitar, entre otra información, 4 direcciones: IP Origen e IP Destino, como parte de su capa de red, y MAC Origen y MAC Destino, como parte de su capa de enlace. De estas 4 direcciones el host conoce 3, sus propias direcciones, IP Origen y MAC

Origen; y la IP Destino, que es la dirección del host al que se quiere llegar (la sabe porque se indica en el propio comando, por ej. ping 163.10.5.66, o porque la deduce usando el servicio de DNS). Lo que el emisor no conoce y necesita determinar es la dirección MAC Destino, la cual le permitirá completar la trama Ethernet. Esta dirección es la que indica a qué host va dirigida la trama. Pero que dirección aprenderá va a depender de si el host destino se encuentra en la misma red que el host origen o no.

Lo primero que hará el host origen será chequear su tabla de ruteo para determinar si el host destino pertenece a su propia red, es decir, si son "vecinos". Si es así, enviará un mensaje de tipo ARP Request solicitando la dirección MAC asociada a la IP Destino. La dirección MAC corresponderá al nodo final al que se está queriendo acceder. Por el contrario, si no son vecinos, el ARP Request preguntará por la dirección MAC del default gateway del host origen. Como se indicó más arriba, ARP se encapsula en Ethernet y los mensaje ARP Request se envían en tramas Ethernet de tipo broadcast. El límite de estas tramas son los routers, que, como se sabe, dividen los dominios de broadcast y, en consecuencia, no reenvían los broadcasts. De esto último se puede inferir que un host no puede utilizar ARP para averiguar la dirección MAC de un host que no se encuentre en su misma red.

> Aunque no sea un router, un host tiene su propia tabla de ruteo, generalmente con dos entradas: una que indica la red a la que pertenece el host y otra con la ruta default con su default-gateway. Esta información puede ser configurada estáticamente o aprendida por el protocolo DHCP

Indistintamente de a quien se envía el ARP Request, la respuesta vendrá en un mensaje ARP Reply siempre que esté disponible el nodo por el cual se consulta. Estas respuestas serán de tipo unicast y también viajarán en tramas Ethernet.

Caso práctico

Resumiendo lo visto hasta ahora, una vez que se ingresa la URL:`http://www.unlp.edu.ar` en el navegador del host *n11-client* lo primero que se dispara es la resolución de nombres, descubrir la dirección IP asociada al servidor de esa página. El resolver local de este host genera una consulta DNS que es enviada, de forma recursiva, al servidor de nombres que tiene configurado. Para esto utiliza un protocolo de capa de transporte, UDP, que al bajar en el stack TCP/IP se transforma en el payload de un paquete IP. Este paquete IP sigue bajando por el stack y es pasado a la capa de enlace, que en nuestro caso es Ethernet. Acá se deberá formar la correspondiente trama que el host *n11-client* enviará por su interfaz llamada `eth0`, cuya configuración podemos ver en la figura 7.3. Para esto el host *n11-client* necesitará conocer la dirección MAC del dispositivo al cual le tiene que enviar esa trama. Es en este momento donde se recurre al protocol ARP para averiguar esa dirección. Obviamente, esto será necesario si es que el host no tiene esa información de algún intercambio anterior en su tabla ARP. Asumiendo que esto último es cierto, es que se analizará cómo se realiza este procedimiento. Si el host ya tiene esa información no sería necesario utilizar ARP.

De acuerdo a la configuración que el host *n11-client* aprendió mediante DHCP, su servidor de DNS es el host llamado *n18-dns-local-resolver*, que tiene la dirección IP 40.0.0.53, lo que ubica a ambos hosts en redes diferentes. Esto nos lleva a la siguiente pregunta, ¿podemos averiguar la dirección MAC

```
root@n11-client:/tmp/pycore.35177/n11-client.conf# ip addr show eth0
47: eth0@if48: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:00:00:aa:00:11 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.0.0.20/24 brd 10.0.0.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::200:ff:feaa:11/64 scope link
       valid_lft forever preferred_lft forever
```

Figura 7.3: Configuración interface eth0 de *n11client*

```
root@n11-client:/tmp/pycore.35177/n11-client.conf# ip route show
default via 10.0.0.1 dev eth0
10.0.0.0/24 dev eth0 proto kernel scope link src 10.0.0.20
root@n11-client:/tmp/pycore.35177/n11-client.conf#
```

Figura 7.4: Tabla ruteo del host *n11client*

asociada a esa dirección IP?. Como se explicó anteriormente, esto no es posible debido a que ambos hosts se encuentran en redes diferentes. Entonces, ¿qué dirección MAC debe aprender el host *n11-client* para terminar de armar la trama? La respuesta es simple, la de su default gateway. Entre la información aprendida mediante DHCP, el host también recibirá cual es su default gateway, el router al que le deberá enviar toda la información que no vaya dirigida a hosts dentro de su misma red. Esto lo puede saber consultando su propia tabla de ruteo, que se puede observar en la imagen 7.4, y que tiene solo dos entradas (podría tener más de dos). La línea que empieza con default es la que nos indica la ruta default y contiene la dirección IP, 10.0.0.1, correspondiente al default gateway. En el gráfico de la red esa dirección se corresponde con la interface `eth1` del router *n10*, cuya configuración se puede ver en la figura 7.5. Es por la dirección MAC asociada a esta dirección IP que se debe realizar la consulta.

Una vez que se sabe que dirección MAC se debe consultar, comienza el proceso. Obviamente, no se puede consultar directamente a un host con una dirección IP asignada cuál es su dirección MAC, esta información es la que se está intentando determinar. Como el host no sabe a quién consultar para obtener lo que necesita, consulta a todos los hosts en su red mediante el envío de un mensaje de tipo broadcast. Todos los hosts en su misma red recibirán ese mensaje, inclusive el router en la interface conectada a esa red, quien no lo retransmitirá hacia otras redes. Ese mensaje es un ARP Request que se puede ver en figura 7.6.

Como se explicó anteriormente, estos mensajes viajan en tramas Ethernet de tipo broadcast, que se ve en el campo *Destination* de la trama. La MAC origen, campo *Source*, corresponde al host *n11-client* que es quien hizo el envío (comparar este dato con el del ether/link de la figura 7.3). También, es posible deducir que se está utilizando el estándar Ethernet II y no el IEEE 802.3 porque tiene el campo *Type* que, en este caso, indica que se está transportando un paquete ARP. A continuación, se puede ver el contenido de este paquete, particularmente los campos *Sender MAC* y *Sender IP*, que contienen

```
root@n10:/tmp/pycore.35177/n10.conf# ip addr show dev eth1
45: eth1@if46: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:00:00:aa:00:10 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.0.0.1/24 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::200:ff:feaa:10/64 scope link
       valid_lft forever preferred_lft forever
```

Figura 7.5: Configuración interface eth1 del router *n10*

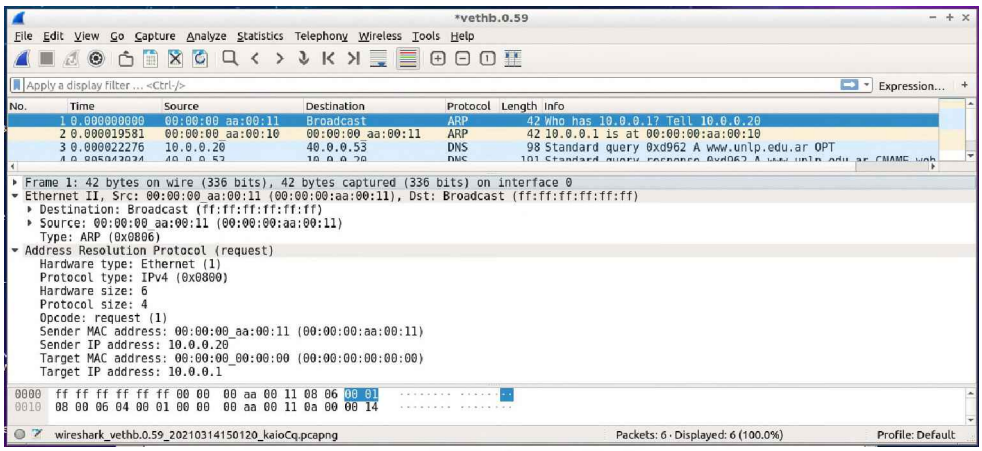

Figura 7.6: ARP Request

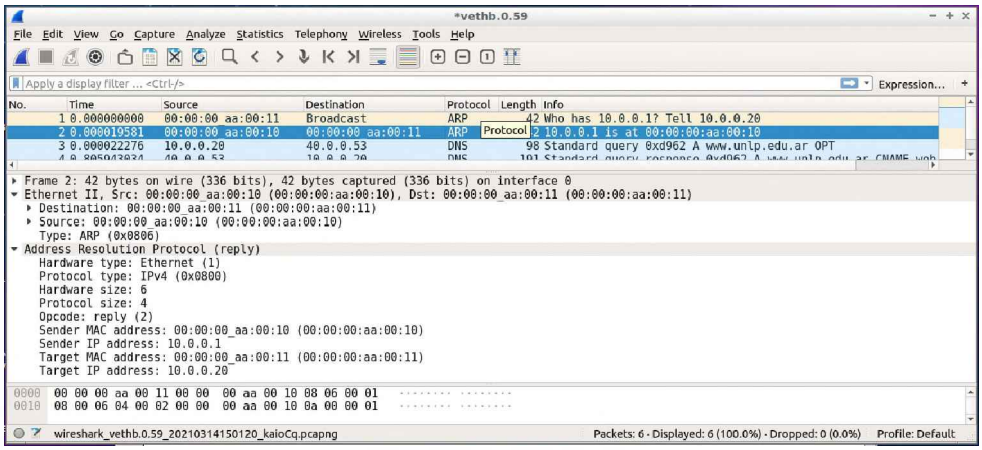

Figura 7.7: ARP Reply

las direcciones MAC e IP respectivamente del host que envió el mensaje, y *Target MAC* y *Target IP*. *Target MAC* contiene todos 0 (ceros) debido a que es la información que se está averiguando y *Target IP* la dirección IP del nodo del cual intentamos conocer su dirección MAC.

Después que la trama broadcast fue enviada será recibida por el switch *s20* que, al ver que es una trama de tipo broadcast, la reenviará por todos sus puertos activos menos por el que la recibió. Todos los hosts dentro de la red recibirán esta trama y la procesarán, pero solo responderá aquel que tenga configurada la dirección IP igual a la que está en el campo Target IP. En nuestro ejemplo, ese nodo será el router *n10* que tiene configurada esa IP en su interface `eth1` (ver la figura 7.5). Este responderá con un mensaje de tipo ARP Reply, que podemos ver en la figura 7.7, y que, a diferencia del ARP Request, es de tipo unicast. Esto implica que la respuesta solo será recibida por el nodo cuya dirección MAC se encuentra el campo *Destination* en la trama Ethernet.

Al observar el paquete ARP Reply, y compararlo con el correspondiente ARP Request, se puede ver que los valores de los campos *Sender* y *Target* están invertidos y todos completos. En el campo Sender MAC viaja la dirección MAC que hace falta para completar la trama Ethernet. A partir de este momento, el host *n11-client* tiene todo la información que necesita para enviar la trama correspondiente, que en este caso llevará un mensaje DNS Query como datos de la capa de aplicación.

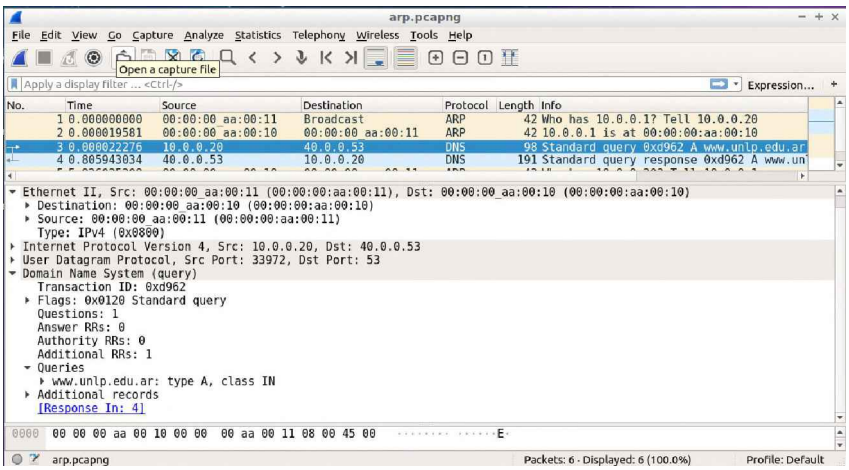

Figura 7.8: Mensaje DNS Query

Para hacer más eficiente el proceso, el router *n10* aprende la dirección MAC del host *n11-client* del ARP Request que recibió de éste. Esto evita que si *n10* le tiene que responder al host *n11-client* deba ejecutar el proceso ARP nuevamente. Además, la información aprendida se mantiene en una tabla ARP por un tiempo determinado, que es configurable. Cada vez que se referencia una entrada en esa tabla su tiempo de vida asociado se vuelve a regenerar. Si una entrada no es referencia por un determinado tiempo, se elimina de la tabla. Si esto sucede, al volver a necesitar esa dirección MAC se deberá ejecutar nuevamente el proceso ARP. Es posible definir una entrada en la tabla de manera permanente.

> Un dispositivo con más de una interfaz, como el caso de un router, tendrá una tabla ARP por cada interfaz que tenga IP configurado)

Es importante comprender que, en este ejemplo, la dirección MAC Destino de la trama Ethernet que transporta el DNS Query no indica el mismo destino que la dirección IP Destino del paquete IP. Esto se debe a que, si bien el paquete IP va destinado al host *n18-dns-local-resolver*, la trama Ethernet va dirigido a la interfaz `eth1` del router *n10*. Si se observa la figura 7.8 se puede ver que la dirección MAC destino de la trama Ethernet indica la interfaz `eth1` del router *n10*, pero la dirección IP destino del paquete IP referencia al host *n18-dns-local-resolver*.

Una vez que la trama llega al router *n10* y éste la acepta, es destruida y el contenido de su campo Datos, que es un paquete IP, se pasa a la capa correspondiente. El router hará lo que sabe hacer, rutear el paquete comparando la dirección IP Destino del paquete contra su tabla de ruteo. En nuestro ejemplo, reenviará el paquete por la interfaz `eth0`, por lo tanto, pasará ese paquete a la capa de enlace que, al ser también una red de tipo Ethernet, deberá ejecutar nuevamente el proceso ARP si es que no tiene la información necesaria en la tabla ARP. En resumen, el proceso ARP se ejecutará por cada red Ethernet que atraviese el mensaje entre un origen y un destino, siempre que no tenga la información necesaria para terminar de armar la correspondiente trama Ethernet.

De manera similar, si desde el host *n11-client*, con dirección IP 10.0.0.20, se quiere acceder a un host vecino, digamos que se envía un mensaje ICMP con el comando `ping(8)` a la dirección IP

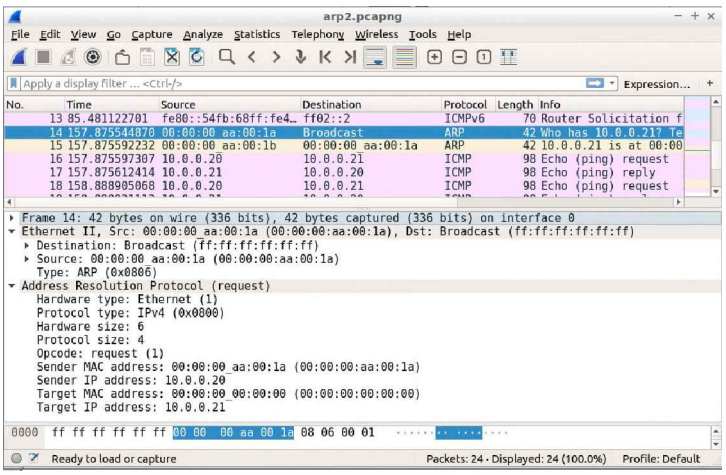

Figura 7.9: ARP Request - Host origen y destino en la misma LAN n11client

10.0.0.21 del host *n21-client*, también sería necesario ejecutar el proceso ARP. En este caso, el ARP Request no consultará por la dirección MAC de su default-gateway sino que lo hará por la dirección MAC correspondiente a la dirección IP que tiene *n21-client* asignada, que es la dirección que se indicó en el comando ping, lo que se puede ver en la figura 7.9. Y, a diferencia del ejemplo anterior, cuando se forme la trama Ethernet para enviar el mensaje del ping, tanto la dirección MAC Destino de la trama como la dirección IP Destino dentro del paquete IP harán referencia al mismo host destino.

Switching

Por último, para terminar de entender todo el proceso detallado hasta el momento, es necesario conocer el trabajo que realiza un switch y, en este caso, el que realiza en particular el switch *s20*. A medida que las tramas pasan por él, un switch, a diferencia de un hub que trabaja en la capa física, va aprendiendo donde se encuentran cada uno de los hosts de su red local, lo que le permitirá decidir que puerto debe utilizar para reenviar una trama dirigida a un host determinado, pero no aprenderá nada de los dispositivos fuera de la red en la que se encuentra. Esto hace que tenga una mínima inteligencia para decidir por donde reenviar una trama en forma eficiente. La información necesaria para tomar esas decisiones la almacenará en una tabla CAM, Content Addressable Memory, que se irá actualizando dinámicamente.

Usando el intercambio de mensajes ARP del ejemplo visto y asumiendo que tiene su tabla CAM vacía cuando reciba el ARP Request enviado por el host *n11-client*, el switch *s20* hará dos cosas: por un lado, agregará en su tabla CAM una nueva entrada en la que indicará que la MAC Origen de la trama, la perteneciente al host *n11-client*, se encuentra en el puerto e0 del switch; por el otro, reenviará la trama, que al ser de tipo broadcast la reenviará por todos los puertos menos por el que la recibió. Luego, cuando reciba el ARP Reply proveniente del router *n10* procederá de la misma manera: agregará una entrada en la tabla CAM que indique que la MAC Origen de la trama, la perteneciente a la interfaz `eth1` del router *n10*, se encuentra en el puerto e2. Y, para reenviarla, como la trama es de tipo unicast lo que hará será comparar la dirección MAC Destino de la trama contra la tabla CAM. En este caso esa dirección coincidirá con una de las entrada de la tabla, la que le indicará que la trama debe ser

reenviada únicamente por el puerto e0 del switch (un hub no tiene esta tabla por lo que todas las tramas que recibe las retransmite por todos los puertos menos por el que la recibió). Si no se encuentra una coincidencia en la tabla CAM, aunque la dirección destino de la trama sea de tipo unicast, la reenviará por todos los puertos menos por el que la recibió, como un hub. En la tabla 7.1 se puede ver como quedaría la tabla CAM del switch *s20* luego del intercambio descrito.

Cuadro 7.1: Tabla CAM del switch *s20*

Puerto	MAC
e0	00:00:00:aa:00:11
e2	00:00:00:aa:00:10

REFERENCIAS

[Plu82] David C. Plummer. «Rfc 826: An ethernet address resolution protocol (arp)», 1982.

[SZ14] Charles E. Spurgeon y Joann Zimmerman. «Ethernet: The definitive guide». OReilly, 2014. ISBN: 9780321336316.