Práctica 6: El protocolo ARP.

Lectura previa: Kurose2017, apartado 6.4.1

Videos:

https://www.youtube.com/watch?v=2XdAXD3uS8c

https://media.upv.es/#/portal/video/8e5cbcf2-0f19-8740-988f-536217d4442a

Trabajo previo para realizar antes de la sesión de laboratorio:

- Lectura del apartado: **Introducción.**
- Estudio de los apartados: **Direcciones físicas** y **Protocolo ARP.**

1. Introducción.

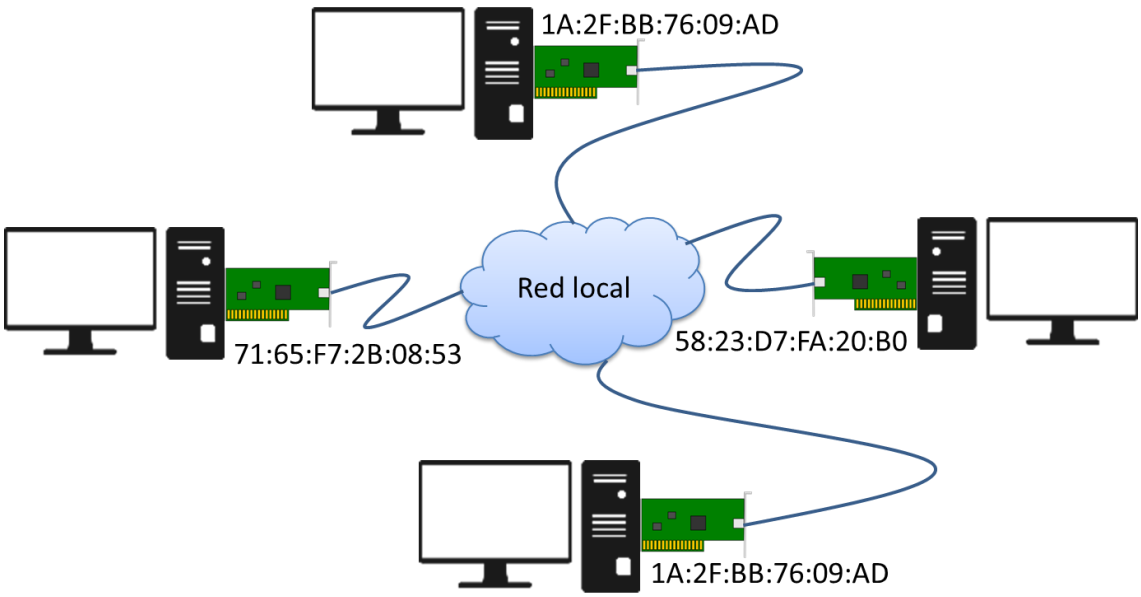
Cada uno de los hosts y routers que están conectados a Internet se identifica mediante una dirección del nivel de red: dirección IP. Pero, además, cada adaptador de red instalado en cada nodo dispondrá de una dirección del nivel de enlace: dirección física.

En esta práctica nos ocuparemos de estudiar el direccionamiento a nivel de enlace de red y también el Protocolo de Resolución de Direcciones (ARP, Address Resolution Protocol) que se encarga de traducir las direcciones IP en direcciones físicas.

2. Direcciones físicas

Las direcciones de la capa de enlace se asignan a los adaptadores de red y se les denomina de diversas formas: dirección LAN, dirección física o dirección MAC.

La dirección física tiene 6 bytes de longitud, lo que nos da 2^{48} posibles direcciones físicas. Estas direcciones se suelen expresar en notación hexadecimal, indicándose cada byte como una pareja de números hexadecimales. Lo podemos ver en la siguiente figura:



La dirección física de un adaptador tiene una estructura plana (no jerárquica como IP) y no variará, aunque el nodo al que pertenece cambie de red.

IEEE se encarga de gestionar el espacio de direcciones físicas, garantizando que dichas direcciones son únicas, independientemente de los fabricantes y de las redes. Cuando una empresa quiere fabricar adaptadores, debe comprar una parte del espacio de direcciones compuesto por 2^{24} direcciones. IEEE asigna el fragmento de 2^{24} direcciones fijando los primeros 24 bits de sus direcciones físicas y dejando que la empresa diseñe combinaciones únicas de los últimos 24 bits para cada adaptador.

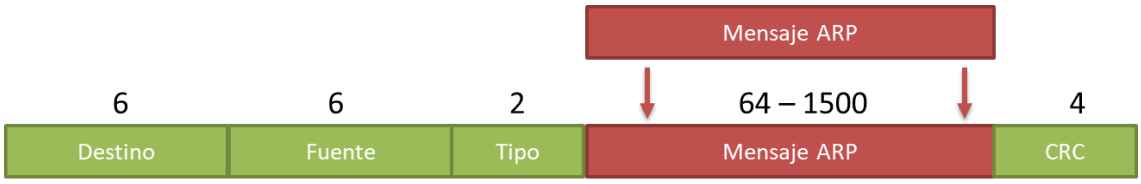
Cuando dos nodos pertenecientes a la misma red quieren comunicarse van a necesitar conocer no solo la dirección IP del otro sino también su dirección física. Un computador solo necesita averiguar la dirección física de otro si ambos comparten la misma red IP.

3. Protocolo ARP

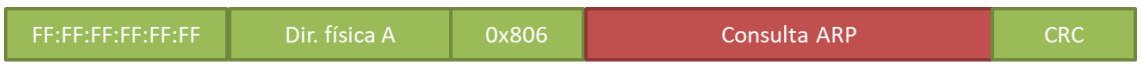
Para que un datagrama IP viaje por la red de área local, este debe encapsularse dentro de una trama (Ethernet en nuestro caso). Esa trama Ethernet contiene la dirección física del siguiente destino, que puede tratarse del computador final al que van dirigidos los paquetes (origen y destino en la misma red local) o del *router* que encaminará el paquete hacia el exterior (origen y destino en distintas redes).

En TCP/IP se utiliza un protocolo para la obtención de direcciones físicas a partir de direcciones IP dentro de una red de área local. Este protocolo se conoce con el nombre ARP (*Address Resolution Protocol*).

Los mensajes del protocolo ARP pertenecen al nivel de enlace y son encapsulados en el campo de datos de una trama. El campo **Tipo** en la cabecera de la trama permitirá identificar el tipo de mensaje: 0x806 identifica al protocolo ARP en el caso de Ethernet.



Para averiguar una dirección física, la capa de enlace enviará un paquete ARP de consulta que contendrá la dirección IP origen, dirección física origen y dirección IP destino. Este mensaje irá dirigido a todos los nodos de la red, empleando para ello la dirección de difusión: FF:FF:FF:FF:FF:FF como dirección destino.



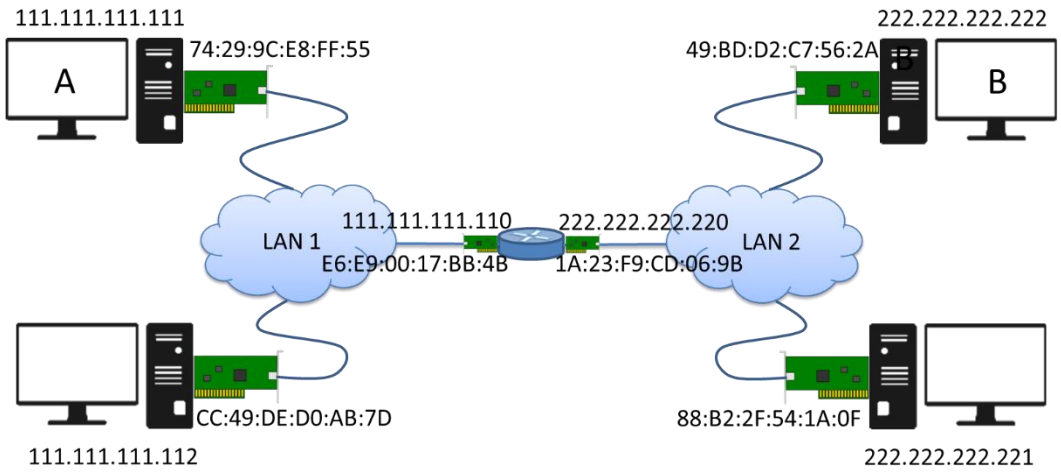
Esta consulta ARP llega a todos los nodos de la red. Cada uno de ellos comprueba si la dirección IP por la que se está consultando le pertenece. Aquel cuya dirección coincida con la pregunta responderá a esta consulta y lo hará mediante un mensaje ARP de respuesta en el que añadirá su dirección física. Este mensaje ya no se enviará por difusión, sino que será dirigido al nodo que ha realizado la consulta.

Dir. física A	Dir. física B	0x806	Respuesta ARP	CRC

Cada nodo tiene en su memoria una tabla ARP donde almacena temporalmente las correspondencias entre las direcciones IP y direcciones físicas que ha utilizado, y presumiblemente podría volver a utilizar. Cada entrada tiene asociado un valor de tiempo de vida (TTL), que indica cuándo se eliminará de la tabla. ARP se considera un protocolo *plug-and-play* porque la tabla ARP se construye automáticamente, no necesita ser configurada por el administrador del sistema.

Cuando un nodo necesite una correspondencia entre dirección IP y física, consultará en primer lugar su tabla ARP, y en caso de no disponer de la información, lanzará la consulta ARP a la red.

Este mecanismo es suficiente cuando dos computadores pertenecientes a la misma red desean intercambiar un datagrama IP. El origen averigua la dirección física del destino y encapsula en datagrama IP en una trama destinada al mismo. Sin embargo, cuando el nodo destino pertenece a otra red IP no es posible esta entrega directa. Estudiemos esta situación basándonos en la siguiente figura.



En la figura aparecen dos redes: 111.111.111.0/24 y 222.222.222.0/24, ambas conectadas mediante un *router* R. Como vemos, dicho *router* dispone de dos adaptadores, con sus correspondientes direcciones físicas e IP. Supongamos que el nodo A quiere enviar un datagrama IP al nodo B. La secuencia de eventos será la siguiente:

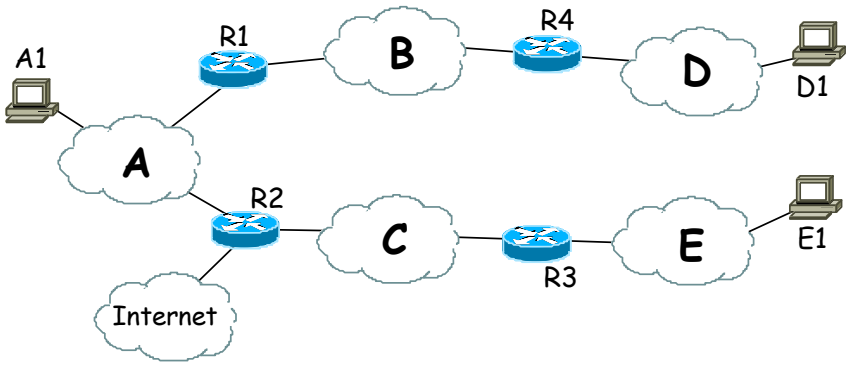
1. El nodo A generará un datagrama con dirección IP origen 111.111.111.111 y dirección IP destino 222.222.222.222. Al aplicar su algoritmo de reenvío, A decidirá que B no está en su red IP, por lo que consultará sus tablas de reenvío, que le indican que la puerta de enlace adecuada es el *router* R.
2. Indicando que el datagrama ha de entregarse a la IP 111.111.111.110 (*router* R), A lo pasará a su nivel de enlace.
3. El nivel de enlace necesita generar una trama con dirección MAC origen la del nodo A (74-29-9C-E8-FF-55) y como dirección destino la del adaptador del *router* R perteneciente a su misma subred (E6-E9-00-17-BB-4B). Para averiguar esta dirección física destino el nodo A consultará su caché ARP y, si es necesario, realizará una consulta ARP en su red. El campo de datos de la trama contendrá el datagrama generado en el nivel de red.

4. Cuando la trama llegue al *router* R, el datagrama IP pasará al nivel de red, desapareciendo la trama original. El *router* R consultará su tabla de reenvío para determinar qué interfaz ha de emplear para alcanzar el destino, y si éste puede hacer una entrega directa. Se decidirá que el datagrama ha de utilizar la interfaz 222.222.222.220, que pasa el datagrama a su el nivel de enlace.
5. El datagrama IP deberá ser encapsulado en una nueva trama que tiene como dirección física origen la del *router* R (1A-23-F9-CD-06-9B) y como dirección física destino la del nodo B (49-BD-D2-C7-56-2A). Nuevamente, será necesaria la consulta a la caché ARP, y quizá una nueva consulta ARP, para que el *router* R averigüe la dirección física del nodo B.
6. Una vez la trama llega al nodo B, el nivel de enlace extraerá el datagrama y lo pasará al nivel de red, que lo procesará convenientemente.

Por último, comentar que el protocolo ARP para Ethernet está definido en el documento RFC 826.

Ejercicio 1.- En la figura se muestra un conjunto de redes locales Ethernet (A, B, C, D y E) de una empresa conectadas entre sí por cuatro routers (R1, R2, R3 y R4). La red se conecta a Internet a través del router R2. Emplearemos la notación IP(D1) e IP(R4D) para denotar las direcciones IP del host D1 y el Router 4, adaptador conectado a la red D. Del mismo nodo, MAC(D1) y MAC(R4D) se refieren a las direcciones físicas correspondientes. Supondremos todas las máquinas correctamente configuradas y las resoluciones DNS en caché.

a) Si suponemos que inicialmente las cachés ARP asociadas a los adaptadores están vacías, indica cómo quedarán las cachés ARP de todos los adaptadores después de que A1 envíe un mensaje a D1 y después de que D1 le conteste a A1.
b) Si a continuación, E1 envía un mensaje a D1, ¿cómo quedan las cachés ARP?



4. Análisis de tráfico

En esta práctica utilizaremos el analizador de protocolos *Wireshark*, que ya conocemos, para analizar el tráfico ARP generado en la red. Para ello necesitamos conocer algo más de la máquina con la que estamos trabajando.

Ejercicio 2.- Mediante el comando ***ifconfig*** en Linux o ***ipconfig*** en Windows**,** averigua cuántos adaptadores de red tiene la máquina con la que estás trabajando. Anota la dirección física de cada uno de ellos y observa si son del mismo fabricante. ¿Todos los adaptadores tienen direcciones IP asignadas? ¿De qué tipo es cada una de las direcciones IP que te aparece?

Adaptador	Dirección Física	Dirección IP

En las prácticas anteriores hemos centrado el análisis de la información proporcionada por las capturas de *Wireshark* en los niveles superiores de la pila de protocolos: aplicación, transporte y red. En esta práctica, en cambio, estudiaremos la información relacionada con el nivel de enlace de datos.

Ejercicio 3.- Realiza una captura con el *Wireshark* mientras cargas en el navegador la página web: http://www.upv.es (no omitas el protocolo en la URL). Utiliza el filtro de captura "**`tcp port 80 and host www.upv.es`**" para poder quedarte con el tráfico HTTP. Selecciona el primer mensaje HTTP de petición que transporta el GET y analiza en la ventana intermedia las diferentes cabeceras de la pila de protocolos TCP/IP.

- ¿Qué tipo de direccionamiento se utiliza en el nivel de transporte? ¿Y en el nivel de red?
- Expande la información relacionada con el nivel de enlace (Ethernet) ¿Cuál es la dirección física origen? ¿Y la dirección física destino?
- Recordando los contenidos aprendidos en las sesiones teóricas. ¿A quién piensas que pertenece esta última dirección física?
- Observa que *Wireshark* expresa las direcciones físicas en dos formatos. ¿Qué dígitos identifican al fabricante del adaptador? ¿Qué código identifica a los fabricantes que te aparecen?
- En la cabecera de Ethernet aparece un campo más que indica el Tipo. ¿Qué se identifica con este campo? ¿Qué valor tiene en nuestro caso y a quién identifica?

El analizador *Wireshark* muestra, por defecto, información del nivel más alto posible. Sin embargo, es posible centrarnos en los niveles inferiores (enlace y físico). Para ello, a través de la opción *Analize->EnabledProtocols*, deshabilitaremos el protocolo IPv4. Observa cómo ha cambiado el aspecto de las ventanas del Wireshark, especialmente la superior. ¿Qué valores aparecen ahora en las columnas Origen, Destino y Protocolo? Vuelve a habilitar el protocolo IP para tener una visión completa de TCP/IP.

Recordemos que el protocolo ARP mantiene una caché con las últimas correspondencias *dirección IP-dirección MAC* averiguadas. El comando *arp* nos permite tanto ver como manipular los contenidos de esta caché:

- **`arp -a`**: nos permite visualizar el contenido de la caché local de ARP.
- **`arp -d <dir_IP>`**: nos permite eliminar entradas manualmente de la caché. Para ello el usuario ha de tener permisos de root.
- **`arp -s <dir_IP> <dir_Eth>`**: para añadir entradas manualmente a la caché. También necesitamos permisos de root.

A lo largo de la práctica podrás encontrar momentos en los cuales ya está disponible en caché ARP una dirección física, y por tanto no se producen los mensajes ARP que quieres obtener. En tal caso, puedes emplear la orden **`sudo arp -d <dirIP>`** (necesitarás ser administrador, por lo que, en Windows, debes ejecutar el "Símbolo del sistema" como administrador. En Linux, debes usar "sudo arp -d <dirIP>") para invalidar la entrada en la tabla, lo cual obliga a volver a consultar la dirección física empleando ARP cuando esta información es necesaria.

Ejercicio 4.- Desde una ventana de comandos ejecuta la orden **arp –a** para comprobar el contenido de la caché. Anota los resultados. ¿A qué máquina o máquinas pertenece la información que obtienes? ¿Qué relación tiene una de las direcciones obtenidas con el ejercicio anterior?

A continuación, realiza una captura con el *Wireshark* empleando el filtro "**`(arp or icmp) and host X.X.X.X`**", sustituyendo las X de la dirección IP por la dirección IP de tu ordenador.

Obtén mediante el comando "**`ipconfig /all`**" la dirección IP de tu router (aparece como puerta de enlace predeterminada). Y elimínala de la tabla arp con "**`arp -d <dirIP>`**"

Ejecuta la orden **ping** a tu router y examina nuevamente el contenido de la caché ARP.

Ahora mira la captura obtenida y localiza la consulta y respuesta ARP que se ha generado relacionada con la orden ping. Puedes utilizar el filtro *ARP* en la ventana de visualización. Tras seleccionar la consulta ARP, responde a las siguientes cuestiones:

- ¿Qué niveles de la pila de protocolos TCP/IP aparecen en el mensaje ARP? ¿Por qué? ¿Dónde se encapsulan los mensajes ARP?
- Evalúa la cabecera Ethernet de la petición ARP. Observa los valores de las direcciones origen y destino, así como el campo de Tipo. ¿Qué identifica este último campo?
- Observa los campos del mensaje ARP. ¿Qué información proporciona la consulta ARP al resto de nodos de la red? ¿En qué campo indica la dirección IP consultada? ¿Cuál es la dirección física de tu router?

Selecciona ahora el mensaje de respuesta ARP asociado a la consulta realizada:

- Observa las direcciones origen y destino de la cabecera Ethernet, e identifica a quién pertenece la dirección física origen. Comprueba que el campo Tipo identifica nuevamente al protocolo ARP.
- ¿Qué direcciones aparecen en el interior del mensaje ARP de respuesta? ¿A quién pertenecen? ¿Dónde aparece la información que nuestro equipo había solicitado?
- ¿Qué campo permite diferenciar una consulta ARP de una respuesta?

Si volvemos a la captura realizada podemos observar cómo inmediatamente después de la consulta ARP aparecen los mensajes ICMP que se generan por la ejecución de la orden **ping**. Es decir, una vez obtenida la dirección física del destino, nuestra máquina ya puede enviar el mensaje ICMP de petición de eco dentro de una trama dirigida al mismo. En este sentido, es similar al protocolo DNS.

Ejercicio 5.- Ejecuta la orden **ping www.upc.es** y comprueba si ha aparecido en la caché la dirección IP del servidor www.upc.es. ¿A quién pertenece la otra dirección que aparece?

Como sabes, antes de la ejecución de la orden ping, se ha realizado una consulta al servidor DNS para resolver el nombre **www.upc.es**. ¿Aparece la dirección del servidor DNS en la caché ARP? ¿Por qué? (en Windows puedes averiguar dirección IP del DNS con el comando ipconfig /all)

Con ARP sólo resulta posible averiguar las direcciones físicas de computadores que están en tu misma red IP.

Ejercicio 6.- Por último, intenta averiguar la dirección física de 3 dispositivos que se encuentren conectados a tu red y que estén en funcionamiento. Utiliza para ello la orden **ping** y consulta después el contenido de la caché ARP. Recuerda que las consultas ARP se realizan antes de la ejecución del ping, por eso el resultado ARP es independiente de si la máquina destino contesta al ping o no.