Práctica 6: ARP, protocolo y análisis de trazas.

1. Sesión L6

Lectura previa: Kurose 5.4. : "Direccionamiento de la capa de enlace".

Trabajo previo a realizar antes de la sesión de laboratorio:

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

2. Introducción.

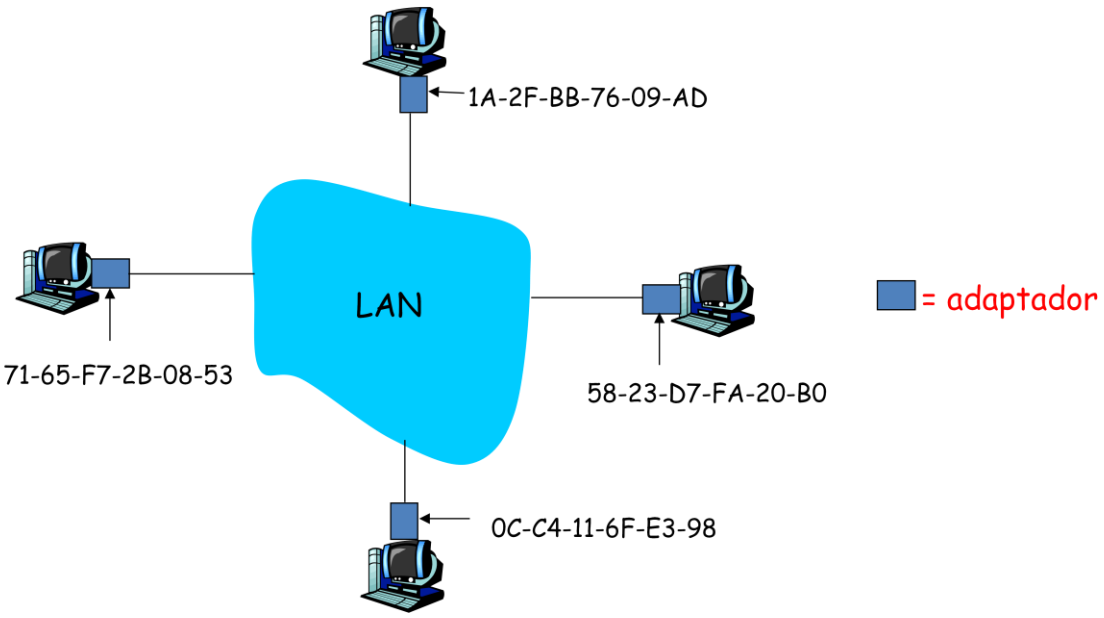
Cada uno de los hosts y routers que están conectados a Internet se identifica mediante una dirección del nivel de red: dirección IP. Pero además, cada adaptador de red instalado en cada nodo dispondrá de una dirección del nivel de enlace: dirección física.

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.

3. Direcciones MAC

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 MAC tiene 6 bytes de longitud, lo que nos da 2^{48} posibles direcciones MAC. 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 MAC 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 MAC, 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 una dirección MAC y dejando que la empresa diseñe combinaciones únicas de los últimos 24 bits para cada adaptador.

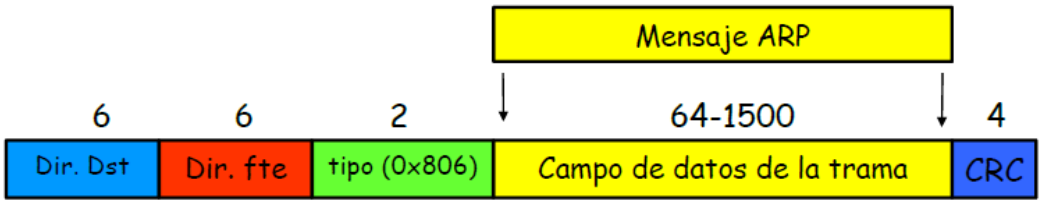
Cuando dos nodos pertenecientes a la misma red quieren comunicarse van a necesitar conocer no solo la dirección IP del otro sino también su dirección MAC. Un computador solo necesita averiguar la dirección física de otro si ambos comparten la misma red IP.

4. Protocolo ARP

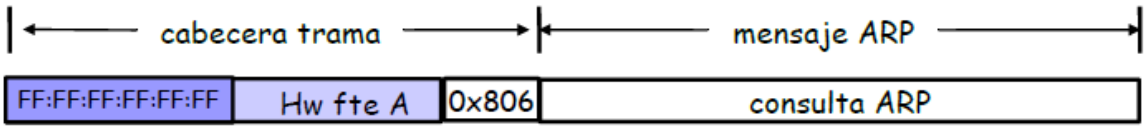
Para que un datagrama IP viaje por la red de área local, este debe encapsularse dentro de una trama (Ethernet en nuestro caso). Esa trama Ethernet contiene la dirección física del siguiente destino, que puede tratarse del computador final al que van dirigidos los paquetes (origen y destino en la misma 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 dentro de una trama, en el campo de datos. Un campo en la cabecera de la trama permitirá identificar el tipo de mensaje: 0x806 en el caso de Ethernet.

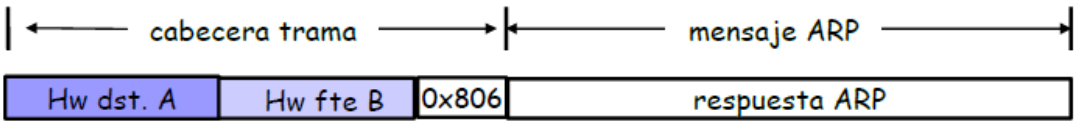


Para averiguar una dirección física, la capa de enlace enviará un paquete ARP de consulta que contendrá la siguiente información: dirección IP origen, dirección física origen y dirección IP destino. Este mensaje irá dirigido a toda la red por lo que la dirección destino será la de difusión: FF FF FF FF FF FF.



Esta consulta ARP llega a todos los nodos de la red con el objetivo de que cada uno de ellos compruebe si la dirección IP por la que se está consultando le pertenece. Sólo uno de ellos responderá a esta consulta y lo hará con un mensaje ARP de respuesta

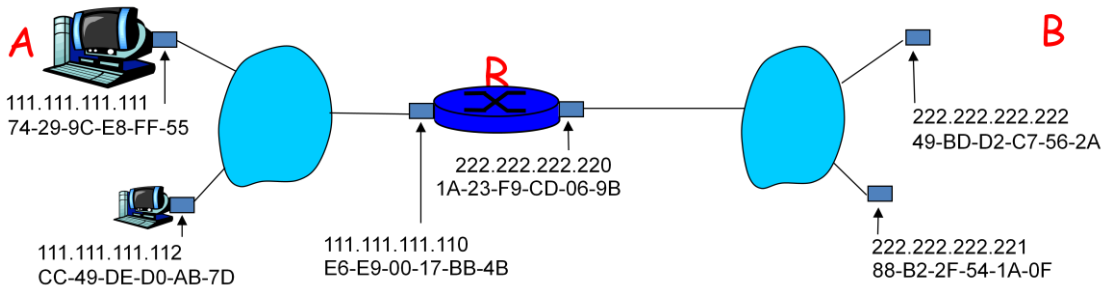
en el que añadirá su dirección física. Este mensaje ya no se enviará por difusión sino al nodo que ha realizado la consulta.



Cada nodo tiene en su memoria una tabla ARP donde va guardando las correspondencias entre las direcciones IP y direcciones MAC que va obteniendo, así como un valor de tiempo de vida (TTL), que indica cuándo se eliminará cada correspondencia 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 MAC, consultará siempre primero en su tabla ARP antes de lanzar la consulta ARP a la red.

Hasta ahora hemos considerado el caso de un nodo que quiere enviar un datagrama a otro perteneciente a la misma subred. Pero ¿qué ocurre cuando el nodo destino pertenece a otra subred? Estudiemos esta situación basándonos en la siguiente figura.



Tenemos dos redes: 111.111.111/24 y 222.222.222/24 conectadas mediante un router R. Como vemos el router tiene dos adaptadores, cada uno de ellos con sus correspondientes direcciones MAC a IP. Supongamos que el nodo A quiere enviar un datagrama al nodo B. Esta es la secuencia de acciones que sucederá:

1. El nodo A generará un datagrama con dirección IP origen 111.111.111.111 y dirección IP destino 222.222.222.222 y lo pasará a su nivel de enlace.
2. A generará 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 perteneciente a su misma subred (E6-E9-00-17-BB-4B). Para averiguar esta dirección destino es posible que el nodo A haya necesitado realizar una consulta ARP en su subred. El campo de datos de la trama contendrá el datagrama generado en el nivel de red.
3. Una vez la trama llega al router R la cabecera de la trama se elimina y pasa el datagrama al nivel de red. Consultando su tabla de reenvío el router determina que para alcanzar el destino el datagrama ha de salir por la interfaz

222.222.222.220. Esta interfaz pasa el datagrama a su adaptador de red: el nivel de enlace.

4. El datagrama es encapsulado en una nueva trama que tiene como dirección MAC origen 1A-23-F9-CD-06-9B y como dirección MAC destino la del nodo B: 49-BD-D2-C7-56-2A. Nuevamente habrá sido necesaria la actuación del protocolo ARP para que el router averigüe la dirección física del nodo B.
5. 5.- Una vez la trama llega al nodo B, el nivel de enlace extraerá el datagrama y lo pasará al nivel de red.

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. Para trabajar en Internet disponen de la dirección IP 197.8.4.0/24, que está organizada en 5 subredes correspondientes a cada una de las redes Ethernet. Cada subred tiene menos de 30 hosts, entre los cuales destacamos los hosts A1, D1 y E1.

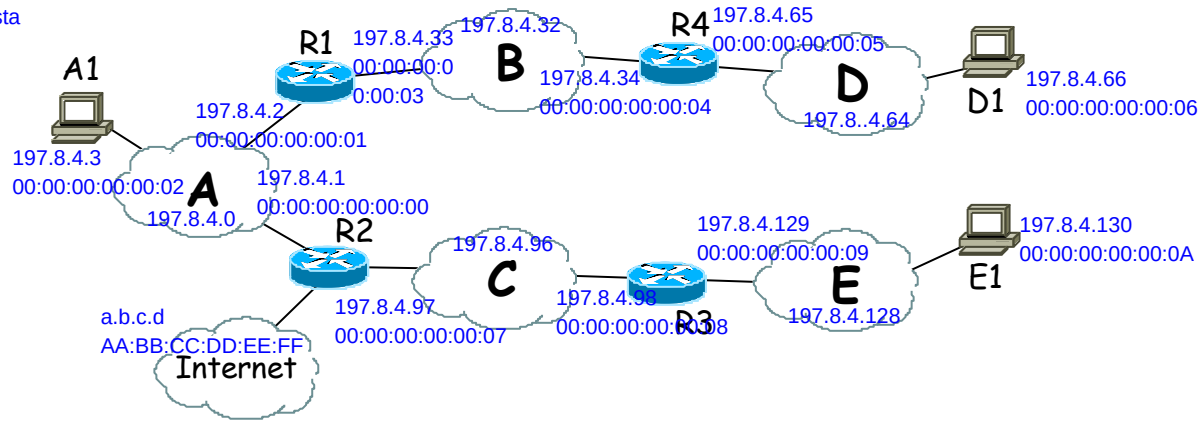
a) Asigna direcciones IP y direcciones MAC a todos los adaptadores de red que aparecen.

b) 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.

todos tendrian guardado en su cache el siguente salto desde A1 hasta D1 y al reves

c) Si a continuación, E1 envía un mensaje a D1, ¿cómo quedan las cachés ARP

De E1 hasta R1 ocurriria igual que antes, de R1 hasta D1 se quedaria igual



5. Análisis de tráfico

En esta práctica vamos a utilizar el analizador de protocolos que ya conocemos, *Wireshark*, para analizar el tráfico ARP que generaremos a través de diferentes acciones en la red.

Pero antes es interesante conocer algo más de la máquina con la que estamos trabajando.

Ejercicio 2.- Mediante el comando ***ifconfig*** averigua cuántos adaptadores de red tiene la máquina con la que estás trabajando. Anota la dirección MAC de cada uno de ellos y observa si son del mismo fabricante. ¿Todos los adaptadores tienen direcciones

2 eth0--> 10:c3:7b:94:e5:1f
eth1--> 00:1b:21:82:71:b2

no son del mismo fabricante porque los primeros 24 bits son diferentes.

IP asignadas? ¿De qué tipo es cada una de las direcciones IP que te aparece (cableada, inalámbrica, loopback,…)?

todos tienen una ip asignada

las dos son cableadas aunque tambien hay una loopback que no hemos comentado antes porque no tiene direccion MAC pero si tiene ip asignada

En las prácticas anteriores hemos estado analizando información con el Wireshark, centrándonos siempre en los niveles superiores de la pila de protocolos: aplicación, transporte y red. Ahora vamos a empezar a ver la información que se genera en el nivel de enlace de datos.

Ejercicio 3.- Realiza una captura con el Wireshark mientras cargas en el Navegador la página web de la Universidad de Valencia: www.uv.es. Utiliza el filtro adecuado para poder quedarte con el tráfico HTTP. Selecciona el primer mensaje HTTP de petición que transporta el GET y analiza en la ventana intermedia la pila de protocolos TCP/IP.

puertos
ip
10:c3:7b:94:e5:1f
2c:fa:a2:2d:10:95
El router de nuestra red que nos encamina hacia internet

- ¿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? ¿A quién piensas que pertenece esta última dirección MAC?

los 6 primeros digitos identifican al fabricante
F. Origen: 10:c3:7b
F. dest: 2c:fa:a2

- Observa que las direcciones MAC se están expresando de dos formas. ¿Qué dígitos identifican al fabricante del adaptador? ¿Qué código identifica a los fabricantes que te aparecen?

0x800 que significa que viene del nivel superior IP

- Observamos también que 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?

Céntrate ahora en el primer mensaje HTTP de repuesta. ¿A quién pertenecen las direcciones físicas que aparecen como origen y destino?

origen: el router de nuestra red
dst: nuestra targeta de red

Por último, en esta captura vamos a ver cómo el Wireshark nos permite visualizar solamente información de determinados niveles TCP/IP. En este caso nos interesará centrarnos en los dos niveles inferiores: enlace y físico. Para ello abrimos la ventana *Analize->EnabledProtocols* y deseleccionamos 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.

Ahora observamos las direcciones fisicas

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>** o **arp –d * :** 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.

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?

Aparecen diferentes host de nuestra red ademas del router de la red
Que es el router que nos ha redirigido hacia internet y hacia la pagina de la uv

A continuación, realiza una captura con el Wireshark mientras ejecutas la orden **ping 158.42.180.62** (dirección de la máquina zoltar.redes.upv.es) y examina nuevamente el contenido de la caché ARP. ¿Cuál es la dirección física de zoltar?

00:16:3e:1d:09:01

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. Si seleccionamos la consulta ARP:

Solo el de enlace porque se genera a nivel de enlace
se encapsulan en la targeta de red

- ¿Qué niveles de la pila de protocolos TCP/IP aparecen en la ventana intermedia? ¿Por qué? ¿Dónde se encapsulan los mensajes ARP?

ori: nuestra
dst: zoltar
tipo: 806
identifica que viene de enlace

- Mirando la cabecera Ethernet indica los valores de las direcciones origen y destino, así como el campo de Tipo. ¿Qué identifica este último campo?

nuestra mac y ip
Target ip addres
la 00:...:00 porque no la sabemos

- Observa los diferentes campos del paquete ARP. ¿Qué información proporciona la consulta ARP al resto de nodos de la red? ¿En qué campo indica la dirección IP consultada? ¿Qué dirección aparece como MAC de zoltar?

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

ori: zoltar
dst: nuestra
si

- Indica qué direcciones origen y destino aparecen en la cabecera Ethernet. ¿A quién pertenece la dirección física origen? Comprobamos que el campo Tipo identifica nuevamente al protocolo ARP.

en Sender MAC addres

Opcode: reply(2)

- Si nos centramos en el paquete ARP de respuesta ¿qué direcciones aparecen en el interior del paquete ARP? ¿A quién pertenecen? En concreto, ¿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 tenemos los mensajes ICMP que se generan por la ejecución de la orden ping. Es decir, una vez obtenida la dirección física de zoltar, nuestra máquina ya puede hacer el ICMP Request a zoltar. ¿A qué otro protocolo del nivel de aplicación nos puede recordar el protocolo ARP? dns

Ejercicio 5.- Ejecuta la orden **ping www.uji.es** y comprueba si ha aparecido en la caché la dirección IP del servidor www.uji.es. ¿A quién pertenece la otra dirección que aparece? No aparece, porque el protocolo arp trabaja en el nivel de enlace dentro de la misma red por tanto solo necesitamos la MAC del router que nos redirige al exterior

Como sabes, antes de la ejecución de la orden ping, se ha realizado una consulta al servidor DNS para resolver el nombre **www.uji.es**. ¿Por qué no aparece la dirección de este servidor en la caché ARP?

Ejercicio 6. Realiza ahora una captura con el Wireshark mientras realizas un ping a la dirección de difusión de la red en la que estás: **ping –b 158.42.181.255** .

- Consulta la caché ARP. ¿Cuántas entradas se han añadido? Copia las entradas nuevas que han aparecido. Identifica algunas de las máquinas sobre las que has obtenido información. se añaden todas las maquinas de nuestra red ya que necesitamos sus mac para comunicarnos con ellos
- Aplica un filtro "ARP" para quedarte sólo con los mensajes ARP en la pantalla de visualización del Wireshark. Localiza una consulta ARP que algún otro nodo haya realizado para obtener información sobre tu MAC. ¿Cuál es la dirección IP y física del nodo que consulta? ¿Y la dirección destino es la de tu máquina? ¿Quién contesta a esta consulta? ¿Qué información aporta la respuesta?

158.42.181.249 - 00:1e:e5:c1:79:e0

solo contestamos nosotros
nuestra tarjeta de red

nuestra MAC y IP

- ¿Cuántos nodos han realizado consulta sobre tu dirección física? Comprueba si estos nodos quedaron registrados en tu caché. 2
si que quedaron registrados

Ejercicio 7.- Por último, intenta averiguar la dirección física de 3 máquinas del laboratorio que estén conectadas. 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 (por ejemplo, porque tenga un cortafuegos configurado para desechar este tipo de peticiones).