Protocolos Ethernet y ARP

Área de Arquitectura y Tecnología de Computadores – Versión 1.0.915, 24/03/2022

Objetivos

En esta sesión se van a estudiar el protocolo Ethernet y el protocolo ARP. Para ello se utilizará el analizador de paquetes de red *Wireshark* y el simulador *Packet Tracer*.

Conocimientos y materiales necesarios

Antes de comenzar esta práctica el alumno debe:

- Conocer la organización en capas de los protocolos de red.
- Acudir al laboratorio de prácticas con el libro de apuntes de la asignatura.
- Durante la sesión se plantearán una serie de preguntas que puedes responder en el correspondiente cuestionario en el Campus Virtual. Puedes abrir el cuestionario en otra pestaña del navegador pinchando en el enlace mientras mantienes pulsada la tecla `Ctrl`.

1. La capa de enlace. Protocolo Ethernet

Todas las tramas que contiene el archivo `6-peticionHTTPcorta.pcap` se han capturado en una red local formada por dos ordenadores y un enrutador, conectados entre sí por una red Ethernet. Por lo tanto, todas las tramas capturadas serán Ethernet y todos los protocolos de nivel superior estarán encapsulados dentro de una trama Ethernet.

Para analizar con más detalle el protocolo Ethernet necesitamos recordar cómo es una trama. En la figura 1 tenemos un esquema de la misma.

Preámbulo	Delimitador	MAC destino	MAC origen	Etiqueta 802.1Q	EtherType o tamaño	Carga útil	CRC
7 bytes 10101010	1 byte 10101011	6 bytes	6 bytes	4 bytes opcionales	2 bytes	46–1500 bytes	4 bytes

Figura 1. Formato de una trama Ethernet

De los elementos que conforman la trama Ethernet, *Wireshark* no nos puede presentar ni los 7 bytes del preámbulo, ni el byte delimitador, ni los 4 bytes del CRC ya que esos elementos solo le sirven a la capa física para identificar la información útil de la trama pero nunca son trasmitidos "hacia arriba" en la arquitectura de protocolos y no llegan al programa de captura. El resto de campos sí se pueden analizar dentro del programa. Vamos a ver una trama en detalle:

- Abre el archivo `6-peticionHTTPcorta.pcap` que se ha suministrado con el material de la práctica.
- Pulsa y selecciona la trama número 1. Oculta pulsando sobre `-` todos los campos que pudieran estar expandidos en el panel intermedio.
- En el panel intermedio, selecciona la segunda línea, la que comienza con la palabra `Ethernet`. Verás que en el tercer panel se seleccionan 14 bytes que corresponden a los datos de la cabecera de una trama Ethernet.
- Expande la información correspondiente al protocolo Ethernet pulsando en el símbolo `+` que hay a la izquierda de la palabra Ethernet. Comprobarás que han aparecido tres líneas más. Si pulsas sobre cualquiera de ellas verás en el panel inferior los bytes de la trama que se corresponden con esa información.
- Pulsa sobre la línea que comienza por la palabra `Type`. Verás que se seleccionan dos bytes en la trama del tercer panel con los valores `08 00`. En el segundo panel se nos informa del significado, en el protocolo Ethernet, de esos dos bytes: indican que los datos que se transportan en la trama Ethernet son del protocolo IP.
- Pulsa sobre la línea que empieza por la palabra `Destination`. Verás en el tercer panel que se seleccionan 6 bytes que son los que se corresponden con la dirección MAC de la interfaz de red de destino de la trama. ¿Qué valor tienen esos bytes? Responde en el cuestionario: pregunta 1. Puedes comprobar que también se puede obtener la dirección MAC del origen.
- Las direcciones Ethernet de las interfaces de red son únicas. A cada fabricante se le asigna un rango de direcciones para que las asigne a las tarjetas que fabrica. De esa manera, conociendo la dirección MAC de una interfaz se puede saber cuál ha sido el fabricante. ¿Sabrías decir quién es el fabricante de la tarjeta Ethernet origen de la trama? Responde en el cuestionario: pregunta 2. Para obtener este valor debes activar la resolución de direcciones MAC en las preferencias **Edit › Preferences › Name Resolution**.

2. El protocolo ARP

El *Address Resolution Protocol* (*ARP*) es un protocolo de comunicaciones de la capa de enlace. Su cometido es determinar cuál es la dirección física (dirección MAC si se usa el protocolo Ethernet a nivel de enlace) de un dispositivo a partir de su dirección IP. Como sabes, para poder establecer una comunicación entre equipos que se encuentran en diferentes redes, es necesario utilizar algún método de direccionamiento que sea inequívoco. A tal efecto se usa el protocolo *Internet Protocol* (*IP*), con el que ya estás familiarizado. Sin embargo, cuando la comunicación debe llevarse a cabo entre elementos dentro de una misma red, ésta se realiza a nivel de enlace, de tal manera que un dispositivo necesita conocer la dirección física de su interlocutor.

Los servicios y aplicaciones no operan en una capa inmediatamente superior a la de enlace, sino que se basan en el nivel IP y superiores. Por tanto, incluso en el ámbito de una red local Ethernet, necesitamos un procedimiento que permita hallar la equivalencia entre direcciones IP y MAC, y es ahí donde juega su papel el protocolo ARP.

Siempre que el sistema operativo de un elemento de la red no conozca la dirección MAC asociada a una dirección IP, se ejecutará el protocolo ARP. Esta información se consulta en una tabla cargada en memoria denominada tabla ARP. Por tanto, es un protocolo que tiende a aparecer en los estadios iniciales del funcionamiento de una red, o bien cuando un equipo pasa a formar parte de la misma (por ejemplo tras su arranque). Además, no importa dónde esté ubicado el destinatario de la comunicación (bien dentro o fuera de la red local), el protocolo se ejecutará siempre si la dirección MAC de destino no se conoce. Hay dos posibilidades:

- Si el destino está en la misma red que el emisor: el protocolo ARP se usará para obtener la dirección MAC de dicho elemento de la red.
- Si el destino no está en la misma red que el emisor: el protocolo ARP se usará para determinar la dirección MAC del elemento de red necesario para dirigir la comunicación hacia el destino, es decir, la dirección MAC de la puerta de enlace (gateway) de la red en la que se encuentra el emisor.

Vamos a ver cómo funciona el protocolo ARP:

- Ejecuta el simulador de red *Cisco Packet Tracer*. A continuación, accede al Campus Virtual, y descarga el recurso `Escenario5.pkt`. Abre dicho escenario en el simulador a través del menú **File › Open**. En este escenario realizaremos diversas comunicaciones desde el equipo denominado *Usuario*. Haz clic en dicho PC, y a continuación en **Desktop › Command Prompt**. En la ventana que se abre escribe el comando "arp -a" para ver la tabla ARP, donde se muestran equivalencias entre direcciones IP y direcciones MAC que este computador ya conoce. ¿Cuántas entradas aparecen en la tabla? Responde en el cuestionario: pregunta 3.
- Cierra las ventanas anteriores. Cambia al modo de simulación denominado *Simulation* y asegúrate que solo los filtros *ARP* e *ICMP* están activos. Haz clic en el sobre cerrado que aparece en el panel derecho en la ventana del simulador (*Add Simple PDU*). Recuerda que esta funcionalidad permitía realizar un ping (encapsulado en el protocolo ICMP) entre un origen y un destino. Haz clic en el PC *Usuario* como origen y en el PC *PC1* como destino.
- Han aparecido dos mensajes. Uno es el mensaje ICMP que encapsula el ping que acabamos de hacer, pero ha aparecido otro de color verde más oscuro, que se enviará antes, y que pertenece al protocolo ARP. Haz clic en dicho mensaje y fíjate en los campos de la capa de enlace (*Layer 2*). ¿Cuál es la dirección MAC del emisor de esa trama? Responde en el cuestionario: pregunta 4. ¿Cuál es la dirección MAC del destino de la trama? Responde en el cuestionario: pregunta 5. ¿Cuántos ordenadores de la red local recibirán y procesarán la trama? Responde en el cuestionario: pregunta 6.
- Haz clic dos veces en botón `Capture/Forward` hasta que el mensaje ARP llegue a su destino. Como ves, al tratarse de un mensaje broadcast, llega a todos los equipos de la red. Todos lo descartan menos el *PC1*, que es el destino del ping, mensaje que aún no ha salido del emisor porque falta resolver la dirección MAC.
- Haz clic en el sobre verde que está sobre *PC1*, y accede a la pestaña *Inbound PDU Details*. Esta trama Ethernet encapsula un mensaje de tipo ARP que se puede entender como la siguiente consulta: "*¿Quién tiene la dirección IP 192.168.2.107 Contestar a 192.168.2.20*". Vamos a ir analizando el significado de cada campo en el protocolo ARP. Observa el campo `Hardware Type`. ¿Qué valor tiene ese campo? Responde en el cuestionario: pregunta 7. Ese valor significa que el protocolo que se está utilizando en la capa de enlace es Ethernet. Fíjate ahora en `Protocol Type`. ¿Qué valor tiene ese campo? Responde en el cuestionario: pregunta 8.Ese valor indica que el protocolo de la capa de red es IP versión 4. Observa `HLEN` (*Hardware Size*). ¿Qué valor tiene? Responde en el cuestionario: pregunta 9. Ese valor indica que el tamaño de las direcciones físicas para el protocolo indicado en el campo *Hardware Type* es de 6 bytes. Finalmente el campo `PLEN` (*Protocol Size*). ¿Qué valor tiene? Responde en el cuestionario: pregunta 10. Ese valor significa que el tamaño de las direcciones del protocolo de capa de red indicado en el campo *Protocol Type* es de 4 bytes. ¿Qué valor tendría que tener este campo si la versión de IP usada fuera IPv6? Responde en el cuestionario: pregunta 11. El siguiente campo del protocolo, `OP CODE` (*Operation Code*), indica que es una solicitud de información y no una respuesta a una petición previa. ¿Qué valor tiene el campo? Responde en el cuestionario: pregunta 12.
- El resto del paquete ARP contiene la solicitud ARP propiamente dicha. En ARP se denomina *target* (objetivo) al destino del mensaje, en este caso una solicitud. ¿Cuál es la dirección IP del objetivo de esta trama? Responde en el cuestionario: pregunta 13. ¿Y la dirección MAC del objetivo? Responde en el cuestionario: pregunta 14. ¿Cuál es la razón del curioso valor de esa dirección MAC? Responde en el cuestionario: pregunta 15.
- ¿Cuál es la dirección IP de origen de esa trama? Responde en el cuestionario: pregunta 16. ¿Y su dirección MAC? Responde en el cuestionario: pregunta 17. Haz clic en el PC *PC1*, y a continuación en *Command Prompt*. Escribe el comando "arp -a" para ver la tabla ARP. ¿Cuántas entradas aparecen en la tabla? Responde en el cuestionario: pregunta 18. *PC1* ha aprovechado la recepción del mensaje ARP anterior para añadir en su tabla ARP una entrada a través de la cual puede comunicarse directamente con *Usuario*.
- Cierra las ventanas anteriores y haz clic dos veces en botón `Capture/Forward` hasta que la respuesta ARP llegue a su destino, *Usuario*. Como ves, al llegar la respuesta al PC *Usuario* este ya se dispone a enviar el ping puesto que conoce la dirección MAC de destino (el sobre que encapsula dicho mensaje ha aparecido a la derecha de la respuesta ARP). No obstante, vamos a analizar el ARP recibida.
- Haz clic en el sobre verde oscuro que está sobre *Usuario*, y accede a la pestaña *Inbound PDU Details*. La mayoría de campos no han cambiado respecto a la solicitud, salvo los siguientes. Fíjate en el campo `OP CODE` (*Operation Code*). ¿Qué valor tiene? Responde en el cuestionario: pregunta 19. Esto indica que es una respuesta ARP. ¿Cuál es la dirección IP del objetivo de esta trama? Responde en el cuestionario: pregunta 20. ¿Y la dirección MAC del objetivo? Responde en el cuestionario: pregunta 21. ¿Cuál es la dirección IP de origen de esa trama? Responde en el cuestionario: pregunta 22. ¿Y su dirección MAC? Responde en el cuestionario: pregunta 23. Si te das cuenta, son los campos que aparecían en la solicitud pero en orden inverso, puesto que el destino (*target*) de la respuesta ARP es el PC *Usuario*. Además, puedes apreciar como el origen, *PC 1*, ha incluido en el mensaje la dirección MAC por la que había sido consultado.
- Comprueba en el *Command Prompt* del PC *Usuario* que ahora dispone de una entrada en la tabla ARP para la dirección IP de *PC1*, y posteriormente avanza la simulación mediante el botón `Capture/Forward` hasta que el ping alcance al *PC1*. Haz clic en dicho mensaje. Analiza la direcciones de Origen y Destino en las capas 2 y 3 de las columnas *In Layers* (ping recibido por *PC1* desde el PC *Usuario*) y *Out Layers* (respuesta que va a enviar *PC1* al PC *Usuario*). Como puedes comprobar, son las direcciones que estuvieron involucradas en el diálogo ARP anterior.
- Pulsa el botón `Delete` en la zona inferior de la pantalla para finalizar esta simulación. Ahora, tras seleccionar el sobre cerrado, haz clic en el PC *Usuario* como origen, y en el *Servidor Web* como destino. Responde a las siguientes preguntas accediendo a la solicitud ARP que se ha generado. ¿Cuál es la dirección IP del objetivo de esta trama? Responde en el cuestionario: pregunta 24. ¿Qué elemento de la topología tiene esa dirección IP? Responde en el cuestionario: pregunta 25. ¿Por qué el mensaje ARP consulta la MAC de dicha IP si el destino del ping era el servidor Web? Responde en el cuestionario: pregunta 26.

3. Ejercicios adicionales

Supongamos que una máquina con la dirección IP `156.35.122.100` quiere solicitar la página web denominada `index.html` al servidor web cuya dirección IP es `129.168.1.100`. Además, supongamos que las direcciones MAC de cada una de esas máquinas y las de sus enrutadores son las que se muestran en la figura 2. Inicialmente las máquinas desconocen las direcciones MAC de las otras máquinas.

- Indica sobre la figura 2 el intercambio de paquetes entre dos máquinas. Indica con flechas su sentido y etiquétalos con números.
- Describe a continuación cada uno de los paquetes, los protocolos utilizados, y el valor de los campos más significativos usados en dichos protocolos. Indica también para qué se usa cada uno de los protocolos.

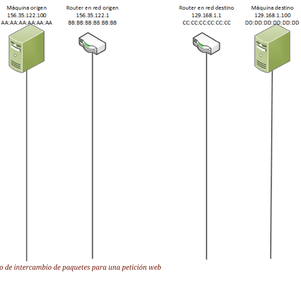

Figura 2. Ejercicio de intercambio de paquetes para una petición web