**Práctica 5 (I): Ethernet y ARP[[1]](#footnote-0)**

**Descripción**

En esta práctica de laboratorio, investigaremos el protocolo Ethernet y el protocolo ARP.

**Objetivo**

Analizar tramas Ethernet

Observar el funcionamiento del protocolo ARP a través de Wireshark y del comando **arp**

**Información básica**

Revisa el Tema 5: Ethernet y ARP

**Tareas**

**Parte 1. Captura y análisis de tramas Ethernet**

Comencemos por capturar un conjunto de tramas Ethernet para estudiarlas. Haz lo siguiente:

* Primero, asegúrate de que la memoria caché de tu navegador está vacía. Para hacer esto en Firefox, selecciona **Historial-> Limpiar historial reciente** y selecciona todo el rango temporal.
* Inicia la captura de paquetes con Wireshark
* Introduce la siguiente URL en tu navegador: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>, debe mostrar la Declaración de Derechos de los Estados Unidos
* Detén la captura de paquetes y guardala en “prac5.1\_ethernet.pcapng”

Primero, busca los números de paquete (la columna más a la izquierda en la ventana superior de Wireshark) del mensaje HTTP GET que se envió desde tu pc al servidor Web, así como el comienzo del mensaje de respuesta HTTP enviado a tu computador por el servidor Web.

Dado que esta práctica trata sobre Ethernet y ARP, no estamos interesados en los protocolos IP o de capa superior. Así que podemos cambiar (es opcional) la ventana de "lista de paquetes capturados" de Wireshark para que muestre información solo sobre los protocolos debajo de IP. Para que Wireshark haga esto, selecciona **Analizar->Protocolos Activados**. A continuación, desmarca la casilla IPv4 y selecciona Aceptar.

Para responder a las siguientes preguntas, deberás examinar los detalles del paquete y las ventanas de contenido del paquete (las ventanas de visualización central e inferior de Wireshark).

* Selecciona la trama Ethernet que contiene el mensaje HTTP GET. (Recuerda que el mensaje HTTP GET se transporta dentro de un segmento TCP, que se transporta dentro de un datagrama IP, que se transporta dentro de una trama Ethernet).
* Expande la información de Ethernet II en la ventana de detalles del paquete. Ten en cuenta que el contenido de la trama de Ethernet (encabezado y carga útil) se muestra en la ventana de contenido del paquete.

Responde las siguientes preguntas, en función del contenido de la trama Ethernet que contiene el mensaje HTTP GET. Recuerda que si quieres puedes adjuntar una copia impresa del paquete(s) al responder una pregunta (**Archivo-> Imprimir**, selecciona *Solo paquete seleccionado*, elije *Línea de resumen de paquete* y seleccione la cantidad mínima de detalles de paquete que necesita para responder la pregunta.)

1. ¿Cuál es la dirección Ethernet de 48 bits de tu PC?
2. ¿Cuál es la dirección de destino de 48 bits en la trama Ethernet? ¿Es esta la dirección Ethernet de gaia.cs.umass.edu?No, es la del gateway (Pista: la respuesta es no). ¿Qué dispositivo tiene esta como su dirección de Ethernet?El gateway [Nota: esta es una pregunta importante, y una en la que los estudiantes más se equivocan. Revisa la información sobre Redes LAN en el Tema 5 y asegúrate de entender la respuesta aquí.]
3. Indica el valor hexadecimal para el campo *Tipo de trama* de dos bytes. ¿A qué protocolo de capa superior corresponde esto?A la capa de red (Protocolo IPv4)
4. ¿Cuántos bytes después del inicio de la trama de Ethernet, aparece el ASCII “G” en “GET” en la trama de Ethernet? La G es el Byte nº 54. Los 54 anteriores (0-53) corresponden a las cabeceras de enlace, red y transporte.

A continuación, responde las siguientes preguntas, basadas en el contenido de la trama Ethernet que contiene el primer byte del mensaje de respuesta HTTP.

1. ¿Cuál es el valor de la dirección de origen de Ethernet? ¿Es esta la dirección MAC de tu pc o del servidor web?Ninguno (Sugerencia: la respuesta es no). ¿Qué dispositivo tiene esta dirección como su dirección de Ethernet? El router que ha enviado el paquete al pc.
2. ¿Cuál es la dirección de destino en la trama de Ethernet? ¿Es esta la dirección Ethernet de tu PC? Si
3. Indica el valor hexadecimal para el campo *Tipo de trama* de dos bytes. ¿A qué protocolo de capa superior corresponde esto? IPv4 (Capa de red)
4. ¿Cuántos bytes después del inicio de la trama de Ethernet aparece la "O” ASCII en “OK” (es decir, ¿el código de respuesta HTTP) en la trama de Ethernet? El byte nº 54, igual que el GET.

**Parte 2. Protocolo de resolución de direcciones**

En esta sección, observaremos el protocolo ARP en acción.

**ARP Caching**

Recuerda que el protocolo ARP generalmente mantiene una caché de pares de traducción de direcciones IP a Ethernet en tu computador. El comando **arp** (tanto en MSDOS como en Linux / Unix) se usa para ver y manipular el contenido de esta caché. Dado que el comando **arp** y el protocolo ARP tienen el mismo nombre, es comprensible que sea fácil confundirlos. Pero ten en cuenta que son diferentes: el comando **arp** se usa para ver y manipular los contenidos de la caché ARP, mientras que el protocolo ARP define el formato y el significado de los mensajes enviados y recibidos, y define las acciones tomadas en la transmisión y recepción de mensajes.

Echemos un vistazo al contenido del caché ARP en tu pc, para ello ejecuta el comando[[2]](#footnote-1):

“**arp –a”**.

1. Copia el contenido de la caché ARP de tu computador. ¿Cuál es el significado de cada valor de columna? 1º: IP, 2º: MAC, 3º: TIPO

Interfaz: 192.168.56.1 --- 0x3

Dirección de Internet Dirección física Tipo

224.0.0.22 01-00-5e-00-00-16 estático

224.0.0.251 01-00-5e-00-00-fb estático

239.255.255.250 01-00-5e-7f-ff-fa estático

Interfaz: 172.19.31.138 --- 0x8

Dirección de Internet Dirección física Tipo

172.19.31.1 b0-c5-3c-60-d2-5f dinámico

172.19.31.99 0c-9d-92-12-08-3d dinámico

172.19.31.130 30-9c-23-87-d2-03 dinámico

172.19.31.131 30-9c-23-87-d1-e5 dinámico

172.19.31.132 30-9c-23-87-d1-f8 dinámico

172.19.31.134 30-9c-23-87-d1-f3 dinámico

172.19.31.137 30-9c-23-88-47-03 dinámico

172.19.31.169 70-85-c2-cc-83-3c dinámico

172.19.32.230 d8-67-d9-c3-42-23 dinámico

224.0.0.22 01-00-5e-00-00-16 estático

224.0.0.251 01-00-5e-00-00-fb estático

224.0.0.252 01-00-5e-00-00-fc estático

239.255.255.250 01-00-5e-7f-ff-fa estático

Interfaz: 192.168.88.1 --- 0x9

Dirección de Internet Dirección física Tipo

192.168.88.254 00-50-56-ec-b4-57 dinámico

224.0.0.22 01-00-5e-00-00-16 estático

224.0.0.251 01-00-5e-00-00-fb estático

239.255.255.250 01-00-5e-7f-ff-fa estático

Interfaz: 192.168.87.1 --- 0xb

Dirección de Internet Dirección física Tipo

192.168.87.254 00-50-56-f0-5e-99 dinámico

224.0.0.22 01-00-5e-00-00-16 estático

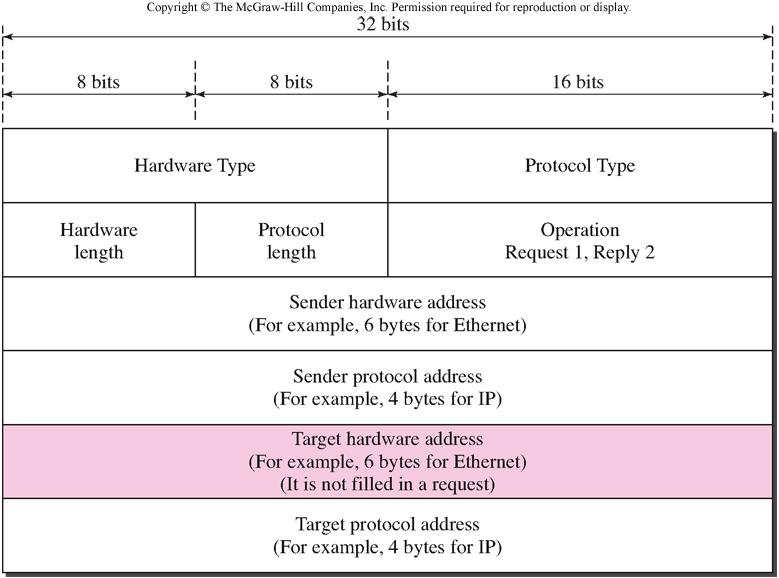
224.0.0.251 01-00-5e-00-00-fb estático

239.255.255.250 01-00-5e-7f-ff-fa estático

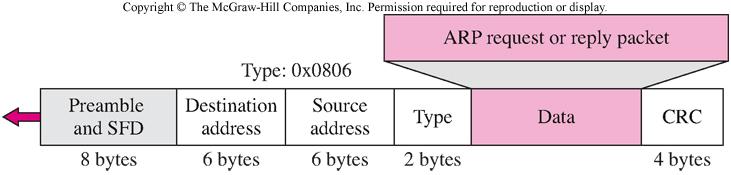
Para observar cómo tu pc envía y recibe mensajes ARP, debemos limpiar la caché ARP, de lo contrario es probable que encuentre un par de traducción de dirección IP-Ethernet en su caché y, por lo tanto, no necesite enviar un mensaje ARP. Para ello se utiliza el comando “**arp –d \***”. La marca –d indica una operación de eliminación, y el \* es el comodín que dice que se deben eliminar todas las entradas de la tabla.

**Observando ARP en acción**

En la Figura 1 se muestra el formato de la cabecera ARP y los campos que la forman, asci como el formato de una trama Ethernet en la que la carga útil es un paquete ARP.



(a) Formato paquete ARP



(b) Encapsulamiento paquete ARP en una trama Ethernet

Figura 1. Especificación ARP

Haz lo siguiente:

* Asegúrate de nuevo que la memoria caché de tu navegador está vacía.
* Copia la URL ya utilizada en tu navegador: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>, pero todavía no le des a Intro.
* Inicia la captura de paquetes con Wireshark
* Abre una ventana de comandos y borra la caché ARP.
* Ve al navegador y accede a la URL copiada.
* Detén la captura. (Si no has vuelto a habilitar el protocolo IPv4 en el menú **Analizar->Protocolos activados**, seguirá inhabilitado, déjalo así. Sino vuelve a inhabilitarlo)
* Busca una pareja solicitud/respuesta ARP en wireshark.

Responde las siguientes preguntas:

1. Indica el valor hexadecimal para el campo *Tipo de trama* de Ethernet de dos bytes. ¿A qué protocolo de capa superior corresponde esto? ARP
2. Teniendo en cuenta el formato de la cabecera ARP de la Figura 1:
   1. ¿Cuál es el valor del campo de código de operación en la cabecera de ARP?
   2. ¿El mensaje ARP contiene la dirección IP del remitente? Si
   3. ¿En qué lugar de la solicitud ARP aparece la "pregunta": la dirección Ethernet del pc cuya dirección IP correspondiente se está consultando?
   4. Completa la siguiente tabla con la cabecera del paquete de solicitud ARP.

| **Campo** | **Valor** |
| --- | --- |
| Dirección MAC del emisor |  |
| Dirección IP del emisor |  |
| Dirección MAC de destino |  |
| Dirección IP de destino |  |

1. ¿Cuáles son los valores hexadecimales para las direcciones de origen y destino en la trama Ethernet que contiene el mensaje de solicitud ARP?

Origen: 

Destino: 

1. Ahora encuentra el paquete de respuesta ARP que se envió en respuesta a la solicitud ARP.
   1. ¿Cuál es el valor del campo de código de operación en la cabecera de ARP?
   2. ¿En qué lugar del mensaje ARP aparece la "respuesta" a la solicitud ARP anterior: la dirección IP del pc con la dirección Ethernet cuya dirección IP correspondiente se está consultando?
   3. Completa la siguiente tabla con información de la cabecera del paquete de respuesta ARP

| **Campo** | **Valor** |
| --- | --- |
| Dirección MAC del emisor |  |
| Dirección IP del emisor |  |
| Dirección MAC de destino |  |
| Dirección IP de destino |  |

* 1. ¿Cuáles son los valores hexadecimales para las direcciones de origen y destino en la trama Ethernet que contiene el mensaje de respuesta ARP?

Origen: 

Destino: 

**Anexo**

A1. El comando arp: **arp -s InetAddr EtherAddr t**e permite agregar manualmente una entrada a la caché ARP que resuelve la dirección IP InetAddr a la dirección física EtherAddr. ¿Qué pasaría si, cuando se agrega manualmente una entrada, ingresa la dirección IP correcta, pero la dirección Ethernet incorrecta para esa interfaz remota?

A2. Examina la latencia de red que causa ARP

1. Borra la caché ARP.
2. Inicia una captura de Wireshark.
3. Haz un ping a un PC de tu red
4. Una vez finalizado el ping, deten la captura de Wireshark. Utiliza el filtro de Wireshark para mostrar solamente los resultados de ARP e ICMP. (En Wireshark, escribe **arp or icmp** en el área de entrada **Filter:**). Si no lo has hecho, habilita de nuevo el protocolo IPv4 en el menú **Analizar->Protocolos activados** .
5. Examina la captura de Wireshark. ¿Qué ocurre con el primer ICMP?

1. Adaptado de: Wireshark Labs v7.0 J.F. Kurose, K.W. Ross. [↑](#footnote-ref-0)
2. Ejecuta como administrador la aplicación de símbolo del sistema. Aunque no es necesario para consultar la tabla arp, si lo es para borrarla. [↑](#footnote-ref-1)