Tarea N° 4

"Dime y lo olvido, enséñame y lo recuerdo, involúcrame y lo aprendo." Proverbio Chino.

En esta tarea usted investigará el protocolo Ethernet y el protocolo ARP (Address Resolution Protocol). ARP fue estandarizado el año 1982 (como alguno de ustedes, yo estaba en mi cuarto año de universidad). El documento está en http://www.ietf.org/rfc/rfc826.txt. Usted no requiere leerlo para esta tarea, es interesante ver el contexto de esa época. ARP es el protocolo usado por un nodo para conocer la dirección Ethernet (o MAC) de un computador cuya dirección IP es conocida.

Par cada pregunta, acompañe la impresión del paquete analizado usando File->Print, elija Selected packet only, elija Packet summary line, y "Output to file:" para guardar su contenido en un archivo. Adjunte la mínima cantidad de líneas del archivo generado para generar sus respuestas.

1.- Borre el cache de su navegador. Corra Wireshark y acceda a la siguiente página con su navegador: http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html

Detenga la captura de Wireshark. Usted debería haber capturado los paquetes de la consulta GET de su navegador. Seleccione el paquete que contiene el requerimiento GET. Para estudiar sólo las tramas de capas inferiores a IP, en Wireshark vaya al menú Analyze-> Enabled Protocols y desactive la celda IPv4.

a) ¿Cuál es la dirección Ethernet de 48-bits de su computador?

b) ¿Cuál es la dirección Ethernet destino en el requerimiento GET? ¿A quién pertenece esa dirección Ethernet? ¿Cómo puede usted comprobar su respuesta?

2.- Para analizar la tabla ARP en DOS y Linux (y MacOS) se dispone del comando de igual nombre que el protocolo, comando arp. Usted puede ver el contenido de la tabla ARP con:

$ arp

Para observar el envío y recepción de paquetes ARP, borre cada una de las entradas de la tabla ARP de su computador con el comando:

$ arp -d <dirección IP o nombre de host correspondiente a la MAC a borrar>

-d es para borrar la dirección Ethernet (MAC) asociada a la dirección IP indicada. En linux usted debe correr este comando como super usuario.

Borre el cache de su navegador, corra Wireshark y cargue la misma página web de la pregunta previa.

a) ¿Qué valores tienen los campos de dirección Ethernet origen y destino en los paquetes ARP de requerimiento y respuesta?

b) ¿Qué valor tiene el campo tipo de trama Ethernet de dos bytes? Señale a qué protocolo capa superior corresponde.