Tarea N° 4

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

En esta tarea primero se abordará el protocolo DHCP y luego usted investigará los protocolos Ethernet y ARP (Address Resolution Protocol).

ARP fue estandarizado el año 1982. El estándar está en http://www.ietf.org/rfc/rfc826.txt. Usted no necesita 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.

Para cada pregunta, acompañe la impresión del paquete analizado. Para esto usted deberíia hacer algo del tipo (depende de su versión de wireshark): 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 apoyar sus respuestas.

A. DHCP

En el sistema operativo Windows es posible liberar la dirección IP asignada por DHCP a su computador usando:

ipconfig /release

Como resultado la IP de su computador IP pasa a ser 0.0.0.0. Este programa lo puede ejecutar desde una consola de comandos de Windows.

Similarmente el comando:

ipconfig /review

pide a su computador obtener una nueva configuración de red incluyendo una dirección IP nueva.

En sistema operativo Linux los comandos equivalentes son:

$ sudo dhclient -r /* para liberar una dirección IP previamente asignada por DHCP.*/

$sudo dhclient /* para obtener una dirección IP nueva */

Nota: el comando dhclient debe ser ejecutado con permisos de super-usuario por ello se antepone aquí sudo ("Super User Do").

Inicie Wireshark, luego realice lo siguiente:

- libere la dirección IP asociada a su computador por DHCP.

- obtenga una IP para su computador usando el comando que corresponda a su sistema operativo. Repita el comando.

- Cuando la segunda vez haya concluido, libere nuevamente la dirección IP previamente asignada.

- Finalmente solicite una dirección IP nueva para su computador y detenga Wireshark.

Para ver los paquetes DHCP en Wireshark pruebe usar como filtro "bootp" (DHCP deriva de un protocolo más antiguo llamado BOOTP, por eso podría requerir ingresar "bootp" y no "dhcp" en el campo filtro de Wireshark). En Wireshark observe los 4 paquetes generador al obtener la IP: paquete DHCP Discover, paquete DHCP Offer, paquete DHCP Request, y

paquete DHCP ACK. Para cada pregunta incluya la porción del paquete mostrada por Wireshark destacando lo usado para responder.

a) ¿Los mensajes DHCP son enviados por UDP o TCP?

b) Dibuje un diagrama de tiempo que ilustre la secuencia de los primeros cuatro paquetes: DHCP Discover / Offer / Request / ACK entre el cliente y el servidor. Para cada paquete, indique los números de puerto de origen y destino.

c) ¿Cuál es la dirección IP de su servidor DHCP?

d) ¿Por cuánto tiempo fue asignada la dirección IP a su computador?

B. Ethernet y ARP

B1.- 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? (entregue resultado en hexadecimal)

b) ¿Cuál es la dirección Ethernet destino del paquete saliente del requerimiento GET? ¿A quién pertenece esa dirección Ethernet?

c) ¿Cuántos bytes hay desde el comienzo de la trama Ethernet hasta el código ASCII para la letra “G” en “GET”? Liste los protocolos de cada encabezado y sus tamaños en bytes.

d) ~~¿Cuál es el valor hexadecimal del campo CRC en esta trama Ethernet?~~

e) Indique el valor hexadecimal para el campo tipo de trama Ethernet.

B2.- 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 y a qué interfaz corresponden 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 para el paquete ARP? Señale a qué protocolo capa superior corresponde.

c) El comando arp:

arp -s dirección_IP EtherAddr

permite añadir manualmente una entrada en la caché ARP que resuelve la dirección IP a la dirección física EtherAddr. ¿Qué pasaría si, cuando se añade manualmente una entrada, usted introduce una dirección IP correcta, pero le asocia una dirección Ethernet distinta a la correspondiente a esa interfaz?

d) ¿Cuál es el lapso de tiempo predeterminado que una entrada permanece en la memoria caché ARP antes de ser removido? Se puede determinar empíricamente (mediante la observación del contenido de la caché). Indique brevemente los pasos que siguió para determinarlo.