PROTOCOLOS ETHERNET Y ARP – LABORATORIO WIRESHARK

En el presente laboratorio estudiaremos los protocolos Ethernet y ARP. Esto con el fin de reforzar los conceptos que se estudiaron en clases pasadas.

CAPTURA DE PAQUETES

Emplearemos una captura de una navegación a una página web para analizar las tramas Ethernet. Para este propósito:

- Limpie el caché de su navegador.
- Abra Wireshark, e inicie la captura por el adaptador de red adecuado.
- Acceda a la siguiente URL en su navegador: http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html
- Detenga la captura.
- Filtre ahora por la dirección IP del servidor remoto. Averigüe la dirección ejecutando el siguiente comando en consola: `nslookup gaia.cs.umass.edu`
- Haga clic derecho sobre uno de los paquetes de la captura, y elija la opción Follow -> TCP Stream
- Wireshark desplegará los paquetes correspondientes a la conexión al servidor y a la descarga de la página web.

ANÁLISIS DE LAS TRAMAS ETHERNET

En este punto, emplee la trama que contiene el comando HTTP GET (suele ser la cuarta trama, selecciónela y verifique en el panel inferior de la ventana, donde aparece el CONTENIDO de los paquetes, que aparezca la orden GET).

Ahora, vaya al panel intermedio de la ventana (que muestra la jerarquía de protocolos) y despliegue el encabezado Ethernet. Empleando dicha trama, conteste las siguientes preguntas:

1. ¿Cuál es la dirección Ethernet (48 bits) fuente? ¿A cuál equipo corresponde? ¿Cómo puede comprobarlo?
2. ¿Cuál es la dirección Ethernet de destino? ¿Corresponde a la dirección Ethernet de gaia.cs.umass.edu? En caso negativo, ¿a qué equipo corresponde esta dirección Ethernet?
3. ¿Cuál es el valor del tipo de trama? ¿Qué indica este valor?
4. ¿A cuántos bytes del inicio de la trama aparece la “G” de “GET”?
5. Revise la estructura de una trama Ethernet, en sus apuntes o mediante una búsqueda en la web. ¿Por qué Wireshark no muestra el campo de FCS?

Busque ahora la trama que contiene el texto “HTTP/1.1 200 OK” en el panel inferior de CONTENIDO. Con base en dicha trama, conteste las siguientes preguntas:

6. ¿Cuál es la dirección fuente Ethernet? ¿A qué equipo corresponde?
7. ¿Cuál es la dirección destino Ethernet? ¿A qué equipo corresponde?
8. ¿Cuál es el valor del tipo de trama? ¿Qué indica este valor?
9. ¿A cuántos bytes del inicio de la trama aparece la “O” de “OK”?

EL PROTOCOLO ARP

10. ¿Cuál es la función del protocolo ARP?

Recuerde que el protocolo ARP conserva un caché de equivalencias entre direcciones IP y Ethernet. El comando `arp` se puede emplear para manipular el contenido de dicha tabla.

Consulte la tabla ARP de su equipo, ejecutando el siguiente comando:

- `arp -a` (en Windows y Mac)
- `arp -n` (en Linux)

11. Tome una línea cualquiera del informe e interprétela. Por favor escriba dicha interpretación.

Para poder capturar tramas ARP, es necesario borrar el contenido de esta tabla. Proceda a borrarla ejecutando el siguiente comando:

- `arp -d *` (en Windows, como administrador)
- `sudo ip -s -s neigh flush all` (en Linux)
- `sudo arp -d -a` (en Mac)

Ahora haga lo siguiente:

- Limpie el caché de su navegador.
- Abra Wireshark, e inicie la captura por el adaptador de red adecuado.
- Acceda a la siguiente URL en su navegador: http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html
- Detenga la captura.
- Filtre las tramas del protocolo ARP (escriba `arp` en el campo de filtro y presione ENTER).

Busque la trama que envía su computador cuando está buscando el enrutador de su red. La trama estará identificada como “Who has (dirección IP del enrutador)? Tell (dirección IP de su computador). Conteste las siguientes preguntas:

12. ¿Cuáles son los valores de las direcciones fuente y destino de la trama Ethernet que contiene la solicitud ARP?
13. ¿Cuál es el valor del tipo de trama? ¿Qué indica este valor?
14. Estudie la siguiente descripción del protocolo ARP: https://erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.
    a. ¿Cuántos bytes hay entre el inicio de la trama Ethernet y el campo opcode de ARP?
    b. ¿Cuál es el valor del campo opcode? ¿Qué indica?
    c. ¿Contiene el mensaje ARP la dirección IP del equipo que lo envía?
    d. ¿En qué posición del mensaje ARP aparece la “pregunta”? (o sea, la dirección Ethernet de la máquina cuya dirección Ethernet está siendo averiguada).

15. Ahora, encuentre la trama que contiene la respuesta ARP a la solicitud anterior.
    a. ¿Cuál es el valor del campo opcode? ¿Qué indica?
    b. ¿En qué posición del mensaje ARP aparece la “respuesta”? (o sea, la dirección Ethernet de la máquina cuya dirección Ethernet está siendo averiguada).
16. ¿Cuáles son los valores de las direcciones fuente y destino de la trama Ethernet que contiene la respuesta ARP?