Tarea N° 3

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

En este laboratorio, se investiga el protocolo IP, centrándose en el datagrama IP. Se hará mediante el análisis de una traza de datagramas IP enviados y recibidos por una ejecución del programa traceroute. Se investiga los diversos campos en el datagrama IP, y estudia la fragmentación IP en detalle.

Antes de comenzar con esta práctica de laboratorio, es probable que usted desee revisar las secciones 1.4.3 en el texto (5° edición). Allí se describe el programa traceroute. En la sección 3.4 del RFC 2151 [ftp://ftp.rfc-editor.org/in-notes/rfc2151.txt] también se describe la operación del programa traceroute. También puede revisar la Sección 4.4 en el texto donde se describe el protocolo IP y puede consultar el estándar del protocolo IP en el RFC 791 [ftp://ftp.rfc-editor.org/in-notes/rfc791.txt].

1. Captura de paquetes con traceroute (no se pide entregar esta parte)

Con el fin de generar una traza de datagramas IP para esta tarea, se usará el programa traceroute para enviar datagramas de diferentes tamaños hacia algún destino, X. Recordar que traceroute funciona mediante el envío de uno o más datagramas con el campo time-to-live (TTL) del encabezado IP en 1; a continuación, envía uno o más datagramas hacia el mismo destino con un valor TTL de 2; a continuación, envía una serie de datagramas hacia el mismo destino con un valor TTL de 3; y así sucesivamente. Recordar que un router disminuye en 1 el TTL de cada datagrama recibido. Si el TTL llega a 0, el router retorna un mensaje ICMP de control (TTL excedido) al host donde traceroute corre. Como resultado de este comportamiento, datagramas con TTL de 1 hacen que el router - a un salto de distancia del emisor- envíe mensajes ICMP TTL excedido de vuelta al remitente; datagramas enviados con TTL de 2 harán que el router – a dos saltos de distancia- envíe mensajes ICMP al remitente; datagramas enviados con TTL de 3 harán que el router -a tres saltos de distancia- envíe mensajes ICMP al remitente; y así sucesivamente. De esta manera, el host ejecutando traceroute puede conocer la identidad de los routers entre él y el destino al ver las direcciones IP de origen en los datagramas que contienen los mensajes ICMP TTL excedido.

Se hará correr traceroute de manera que envíe datagramas de varios tamaños.

Caso Windows: El programa tracert proporcionado por Windows no permite cambiar el tamaño del mensaje de la solicitud de eco ICMP (ping). Una mejor versión de traceroute para Windows es el programa pingplotter, disponible tanto en versiones libres y shareware (con el entendimiento que se comprará si se sigue usando) http://www.pingplotter.com. Si usted trabaja en windows, descargue e instale pingplotter. El tamaño del mensaje eco ICMP de solicitud se puede configurar de forma explícita en pingplotter seleccionando la opción de menú *Edit-> Options-> Packet Options* [1]. El tamaño de paquete predeterminado es de 56 bytes. Una vez que pingplotter ha enviado una serie de paquetes con el aumento de los valores TTL, éste reinicia el proceso de envío con un TTL de 1 después de esperar un tiempo *Trace Interval*. El valor de *Trace Interval* y el número de re-inicios se puede configurar de forma explícita en pingplotter.

1 La última versión es de Marzo 2017, revise por posibles cambios en opciones del menú.

Caso Linux/Unix: Con el comando traceroute Unix, el tamaño del datagrama UDP enviado hacia el destino se puede definir de forma explícita en la línea de comando inmediatamente después del nombre o dirección del destino. Por ejemplo, para enviar datagramas de 2000 bytes hacia gaia.cs.umass.edu, el comando sería:

$ traceroute gaia.cs.umass.edu 2000

Para capturar los paquetes para esta tarea, haga lo siguiente:

- Corra Wireshark y comience la captura de paquetes (Capture-> Start),
- **Si está utilizando Windows**, corra pingplotter e introduzca el nombre de un destino en la ventana "Address to Trace Window.” Use 3 en el el campo "# of times to Trace". Seleccionar la opción de menú *Edit-> Advanced Options-> Packet Options* e ingrese 56 en el campo “*Packet Size*”. A continuación, presione *Trace*.

  A continuación, envíe un conjunto de datagramas con una longitud más larga, seleccionando *Edit-> Advanced Options -> Packets Options* e ingrese el valor 2000 en el campo *Packet Size*. A continuación, pulse el botón Reanudar.

  Detenga la captura de Wireshark.
- **Si está utilizando Linux o MacOS**, ejecute tres comandos traceroute, uno con tamaño de datagrama de 56 bytes y otro con tamaño de datagrama de 2000 bytes.

  Detenga la captura de Wireshark.

2. Análisis de los datagramas IP capturados (entregue sus respuestas)

En su traza, usted debería ver una serie de mensajes ICMP Echo Request (en el caso Windows) o segmentos UDP (en el caso Linux) enviados por el computador y mensajes ICMP TTL-Exceeded retornados a su equipo por los routers intermedios. **En las siguientes preguntas, se supone que usted está utilizando una máquina de Windows; las preguntas correspondientes para el caso de una máquina Linux usted las puede concluir por analogía, si tiene dudas pregunte al profesor.**

Cuando sea posible, al responder una pregunta su grupo debe entregar una impresión del paquete (s) que utilizó para responder a la pregunta. Agregue anotaciones en la impresión para aclarar de dónde usted obtuvo la información de su respuesta. Para imprimir un paquete, utilice *File -> Print*, elija *Selected packet only*, elija *Packet summary line* y seleccione la cantidad mínima de detalles del paquete(s) necesarios para responder.

1. Seleccione el primer mensaje ICMP Echo Request enviado por su computador, y expanda la parte de Internet Protocol del paquete en la ventana de detalles del paquete. ¿Cuál es la dirección IP de su computador?

2. Dentro de la cabecera del paquete IP, ¿cuál es el valor en el campo protocolo de nivel superior?

3. ¿Cuántos bytes tiene la cabecera IP? ¿Cuántos bytes tiene la carga útil (payload o datos transportados) del datagrama IP? Explique cómo determinó el número de bytes de carga útil.

4. ¿Se ha fragmentado este datagrama IP? Explicar cómo usted determina si el datagrama se ha fragmentado o no.

A continuación, ordenar los paquetes de la traza de acuerdo con la dirección IP de origen haciendo clic en la columna de encabezado *Source*; una pequeña flecha que apunta hacia abajo debe aparecer junto a la palabra *Source*. Si la flecha apunta hacia arriba, haga clic en la columna *Source* nuevamente. Seleccione el primer mensaje ICMP Echo Request enviado por el computador, y expanda la parte Internet Protocol en la ventana "details of selected packet header". En la ventana "listing of captured packets", debería ver todos los mensajes ICMP subsiguientes (tal vez con paquetes adicionales intercalados enviados por otros protocolos que se ejecutan en el computador) por debajo de este primer ICMP.

5. ¿Qué campos del datagrama IP **siempre** cambian de un datagrama al siguiente dentro de esta serie de mensajes ICMP enviados por su computador?

6. ¿Qué campos deben permanecer constante de un datagrama al siguiente en la serie ICMP enviados?

7. Describa el patrón que usted ve en la secuencia de valores del campo Identificación del datagrama IP.

Luego (con los paquetes ordenados por dirección de origen) encuentre la serie de respuestas ICMP TTL excedidos enviadas a tu computador por el router más cercano (primer salto).

8. ¿Cuál es el valor del campo Identificación y del campo TTL?

9. ¿Siguen estos valores siendo los mismos para todas las respuestas ICMP TTL-Exceeded enviadas a su computador por el router más cercano (primer salto)? ¿Por qué?

Fragmentación

Ordenar la lista de paquetes de acuerdo al tiempo haciendo clic en la columna *Time*.

10. Encuentre el primer mensaje ICMP Echo Request enviado por su computador después de cambiar el *Packet Size* en pingplotter a 2000. ¿Ha sido ese mensaje fragmentado en más de un datagrama IP?

11. Imprima el primer fragmento del datagrama IP original. ¿Qué información en la cabecera IP indica que el datagrama ha sido fragmentado? ¿Qué información en la cabecera IP indica si este es un fragmento o es el último fragmento? ¿Qué tamaño tiene este datagrama IP (el primer fragmento)?

12. Imprima el segundo fragmento del datagrama IP original. ¿Qué información en la cabecera IP indica que éste no es el primer fragmento de datagrama? ¿Hay más fragmentos? ¿Cómo lo puede saber?