Redes de Computadores 2022-21
Hands-on 4: Capa de red (IP Básico y fragmentos)

Profesor: David F. Celeita R.

Objetivos:

- Identificar detalles de IP
- Comprender el funcionamiento de traceroute
- Entender el proceso de fragmentación de datagramas e identificar adecuadamente segmentos.

Entrega:

- Fecha: Jueves 17 de Marzo (E-Aulas 23:59)
- Modalidad: Grupos.
- Metodología: Observar y aprender haciendo (Hands-on)

Contexto:

En este laboratorio, investigaremos el protocolo IP, centrándonos en el datagrama IPv4 e IPv6. Este laboratorio consta de tres partes. En la primera parte, analizaremos los paquetes en un rastro de datagramas IPv4 enviados y recibidos por el programa traceroute (el programa traceroute en sí se explora con más detalle en el laboratorio de Wireshark ICMP).Después, estudiaremos la fragmentación de IP.

Actividades:

Actividad 1: Captura de paquetes de una ejecución de traceroute

Actividad 2: Fundamentos IP

Actividad 3: Fragmentación

Actividad 1: Captura de paquetes de una ejecución de traceroute

Para generar un seguimiento de datagramas IPv4 para las dos primeras partes de este laboratorio, usaremos el programa traceroute para enviar datagramas a gaia.cs.umass.edu. Recuerde que traceroute opera enviando primero uno o más datagramas con el campo (TTL) en el encabezado IP; luego envía una serie de uno o más datagramas hacia el mismo destino con un valor TTL de 2; luego envía una serie de datagramas hacia el mismo destino con un valor TTL de 3, etc.

Recuerde que un enrutador debe disminuir el TTL en cada datagrama recibido en 1 (en realidad, RFC 791 dice que el enrutador debe disminuir el TTL en al menos uno). Si el TTL llega a 0, el enrutador devuelve un mensaje ICMP (tipo 11 - TTL excedido) al host de envío. Como resultado de este comportamiento, un datagrama con un TTL de 1 (enviado por el host que ejecuta traceroute) hará que el enrutador a un salto del remitente envíe un mensaje ICMP TTL excedido al remitente; el datagrama enviado con un TTL de 2 hará que el enrutador a dos saltos de distancia envíe un mensaje ICMP al remitente; el datagrama enviado con un TTL de 3 hará que el enrutador a tres saltos de distancia envíe un mensaje ICMP al remitente, y así sucesivamente. De esta manera, el host que ejecuta traceroute puede aprender las direcciones IP de los enrutadores entre él y el

destino mirando las direcciones IP de origen en los datagramas que contienen los mensajes ICMP TTL excedidos.

Instrucciones:

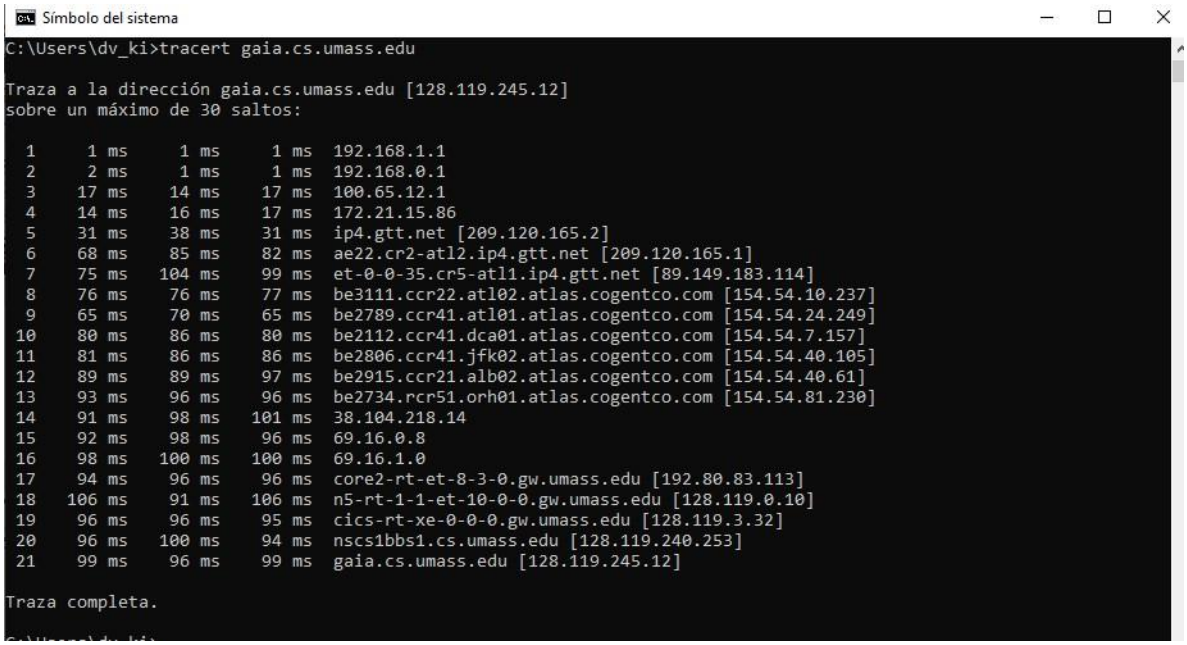
Ejecute traceroute y envíe datagramas. Si envía datagramas muy grandes, requerirá que los mensajes de traceroute se fragmenten en múltiples datagramas IPv4.

- **Linux / MacOS.** Con el comando traceroute de Linux / MacOS, el tamaño del datagrama UDP enviado hacia el destino final se puede establecer explícitamente indicando el número de bytes en el datagrama; este valor se ingresa en la línea de comando traceroute inmediatamente después del nombre o la dirección del destino. Por ejemplo, para enviar datagramas traceroute de 2000 bytes hacia gaia.cs.umass.edu, el comando sería el siguiente:

% traceroute gaia.cs.umass.edu 2000

- **Windows.** El programa tracert proporcionado con Windows no permite cambiar el tamaño del mensaje ICMP enviado por tracert. Por lo tanto, no será posible usar una máquina con Windows para generar mensajes ICMP que sean lo suficientemente grandes como para forzar la fragmentación de IP. Sin embargo, puede usar tracert para generar paquetes pequeños de longitud fija. En el símbolo del sistema de DOS, ingrese:

> tracert gaia.cs.umass.edu



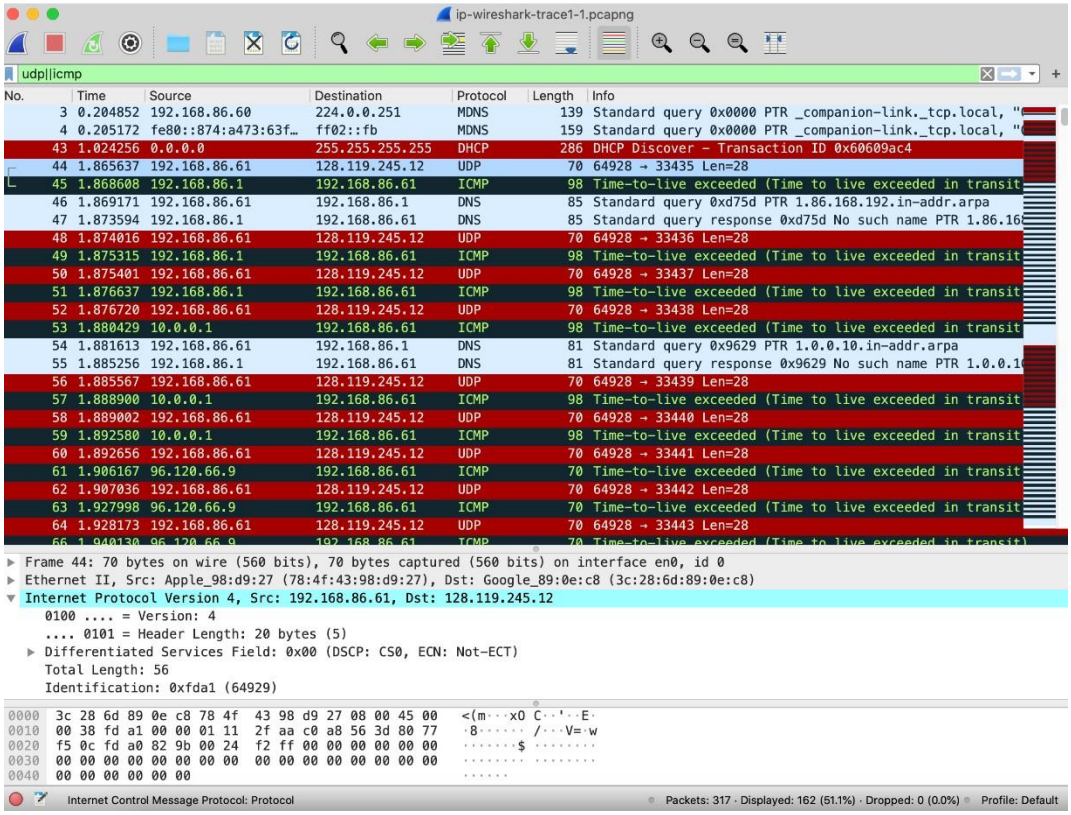
Pasos:

- Inicie Wireshark y comience la captura de paquetes. (Capturar-> Iniciar o hacer clic en el botón de aleta de tiburón azul en la parte superior izquierda de la ventana de Wireshark).
- Ingrese dos comandos de traceroute, usando gaia.cs.umass.edu como destino, el primero con una longitud de 56 bytes. Una vez que ese comando haya terminado de ejecutarse, ingrese un segundo comando traceroute para el mismo destino, pero con una longitud de 3000 bytes.
- Detenga el rastreo de Wireshark.

Nota: Para usuarios Windows, en E-Aulas se encuentra disponible una captura de Wireshark (ip-wireshark-trace1-1.pcapng).

Actividad 2: Fundamentos IP

En su rastreo, debería poder ver la serie de segmentos UDP (en el caso de MacOS / Linux) o mensajes ICMP Echo Request (Windows) enviados por traceroute, y los mensajes ICMP TTL excedidos regresados a su computadora por los enrutadores intermedios.



Wireshark: UDP + ICMP pkts del archivo ip-wireshark-trace1-1.pcapng

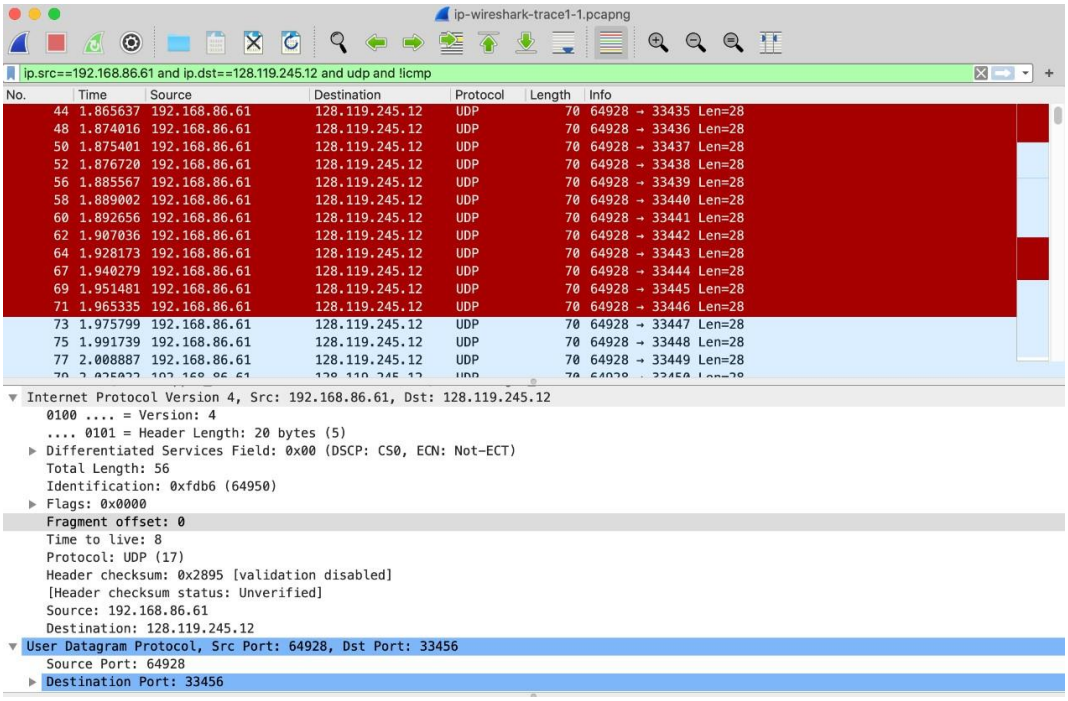
Redes de Computadores 2022-21
Hands-on 4: Capa de red (IP Básico y fragmentos)

Profesor: David F. Celeita R.

Preguntas:

1. Seleccione el primer segmento UDP enviado por su computadora a través del comando traceroute a gaia.cs.umass.edu. (Sugerencia: este es el paquete 44º en el archivo de seguimiento en el archivo ip-wirehark-trace1-1.pcapng). Expanda la parte Protocolo de Internet del paquete en la ventana de detalles del paquete. ¿Cuál es la dirección IP de la computadora?
2. ¿Cuál es el valor en el campo de tiempo de vida (TTL) en el encabezado de este datagrama IPv4?
3. ¿Cuál es el valor en el campo de protocolo de capa superior en el encabezado de este datagrama IPv4?
4. ¿Cuántos bytes hay en el encabezado IP?
5. ¿Cuántos bytes hay en la carga útil del datagrama IP? Explicar cómo determinar la cantidad de bytes del payload.
6. ¿Se ha fragmentado este datagrama de IP? Explicar cómo determinar si el datagrama se ha fragmentado o no.

A continuación, veamos la secuencia de segmentos UDP que se envían desde el origen a través de traceroute, destinados a 128.119.245.12. El filtro de pantalla que puede ingresar para hacer esto es “ip.src==192.168.86.61 and ip.dst==128.119.245.12 and udp and !icmp”. Esto le permitirá moverse secuencialmente fácilmente a través de los datagramas que contienen solo estos segmentos.



Wireshark: Segmentos ip-wireshark-trace1-1.pcapng usando el filtro ip.src==192.168.86.61 and ip.dst==128.119.245.12 and udp and !icmp

7. ¿Qué campos del datagrama IP siempre cambian de un datagrama al siguiente dentro de esta serie de segmentos UDP enviados por su computadora con destino a 128.119.245.12, vía traceroute? ¿Por qué?
8. ¿Qué campos de esta secuencia de datagramas IP (que contienen segmentos UDP) permanecen constantes? ¿Por qué?
9. Describa el patrón que ve en los valores del campo Identificación de los datagramas IP que envía su computadora.

Ahora echemos un vistazo a los paquetes ICMP que son devueltos a su computadora por los enrutadores intermedios donde el valor TTL se redujo a cero (y por lo tanto causó que el mensaje de error ICMP regresara a su computadora). El filtro de pantalla que puede usar para mostrar solo estos paquetes es “ip.dst == 192.168.86.61 and icmp”.

10. ¿Cuál es el protocolo de capa superior especificado en los datagramas IP devueltos por los enrutadores?
11. ¿Los valores en los campos de identificación (en la secuencia de todos los paquetes ICMP de todos los enrutadores) son similares en comportamiento a su respuesta a la pregunta 9?
12. ¿Son similares los valores de los campos TTL en todos los paquetes ICMP de todos los enrutadores?

Profesor: David F. Celeita R.

Actividad 3: Fragmentación

Ahora, veremos un segmento UDP grande (3000 bytes) enviado por el programa traceroute que está fragmentado en múltiples datagramas IP.

Utilizando el mismo archivo anteriormente mencionado, ordene la lista de paquetes de la Parte 1, con los filtros de visualización borrados, según la hora, haciendo clic en la columna Hora.

Preguntas:

1. Busque el primer datagrama IP que contenga la primera parte del segmento enviado a 128.119.245.12 enviado por su computadora a través del comando traceroute a gaia.cs.umass.edu, después de haber especificado que la longitud del paquete traceroute debe ser 3000. (Sugerencia: Este es el paquete 179 en el archivo de rastreo ip-wireharktrace1-1.pcapng en la nota al pie 2. Los paquetes 179, 180 y 181 son tres datagramas IP creados al fragmentar el primer segmento UDP de 3000 bytes enviado a 128.119.145.12) . ¿Ese segmento se ha fragmentado en más de un datagrama de IP?
2. ¿Qué información en el encabezado IP indica que este datagrama ha sido fragmentado?
3. ¿Qué información en el encabezado IP de este paquete indica si este es el primer fragmento frente a un último fragmento?
4. ¿Cuántos bytes hay en este datagrama IP (encabezado + payload)?
5. Ahora inspeccione el datagrama que contiene el segundo fragmento del segmento UDP fragmentado. ¿Qué información en el encabezado IP indica que este no es el primer fragmento de datagrama?
6. ¿Qué campos cambian en el encabezado IP entre el primer y segundo fragmento?
7. Ahora busque el datagrama IP que contiene el tercer fragmento del segmento UDP original. ¿Qué información en el encabezado IP indica que este es el último fragmento de ese segmento?

Redes de Computadores 2022-21
Hands-on 4: Capa de red (IP Básico y fragmentos)

Profesor: David F. Celeita R.

Entregables: Una carpeta con los siguientes elementos

Actividad 1 (0%):

- Toma de pantalla con resultado de traceroute

Actividad 2 (50%):

- Documento con respuestas + tomas de pantalla de Wireshark.

Actividad 3 (50%):

- Documento con respuestas + tomas de pantalla de Wireshark.