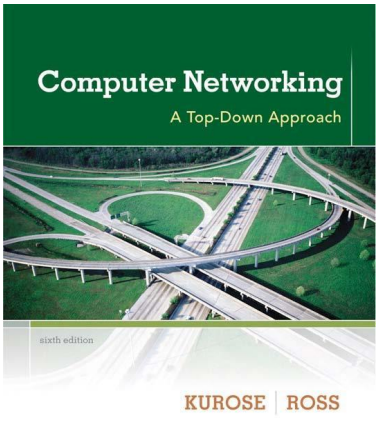
Wireshark Lab: IP v6.0

Supplement to *Computer Networking: A Top-Down Approach, 6th ed.,* J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb



En este laboratorio, investigaremos el protocolo IP, centrándonos en el datagrama IP. Lo haremos mediante el análisis de una traza de datagramas IP enviados y recibidos por una ejecución del programa `traceroute`. Investigaremos los diversos campos en el datagrama IP, y estudiaremos la fragmentación IP en detalle.

Antes de comenzar con esta práctica de laboratorio, es probable que desees 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`

Con el fin de generar una captura de datagramas IP para esta tarea, usaremos el programa `traceroute` para enviar datagramas de diferentes tamaños hacia algún destino, X. Recordemos 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. Recordemos que un router debe disminuir en 1 el TTL de cada datagrama recibido. Si el TTL llega a 0, el router retorna un mensaje ICMP (tipo 11 – TTL excedido) al host donde el traceroute corre. Como resultado de este comportamiento, un

datagrama con un TTL de 1 (enviado al ejecutar traceroute) hace que el router - a un salto de distancia del emisor- envíe un mensaje ICMP TTL excedido de vuelta al remitente; el datagrama enviado con un TTL de 2 hará que el router – a dos saltos de distancia- envíe un mensaje ICMP al remitente; el datagrama enviado con un TTL de 3 hará que el router -a tres saltos de distancia- envíe un mensaje ICMP al remitente; y así sucesivamente. De esta manera, el host ejecutando `traceroute` puede conocer la identidad de los routers entre el mismo y el destino X al ver las direcciones IP de origen en los datagramas que contienen los mensajes ICMP TTL excedido.

Ejecutaremos `traceroute` de manera que envíe datagramas de varios tamaños.

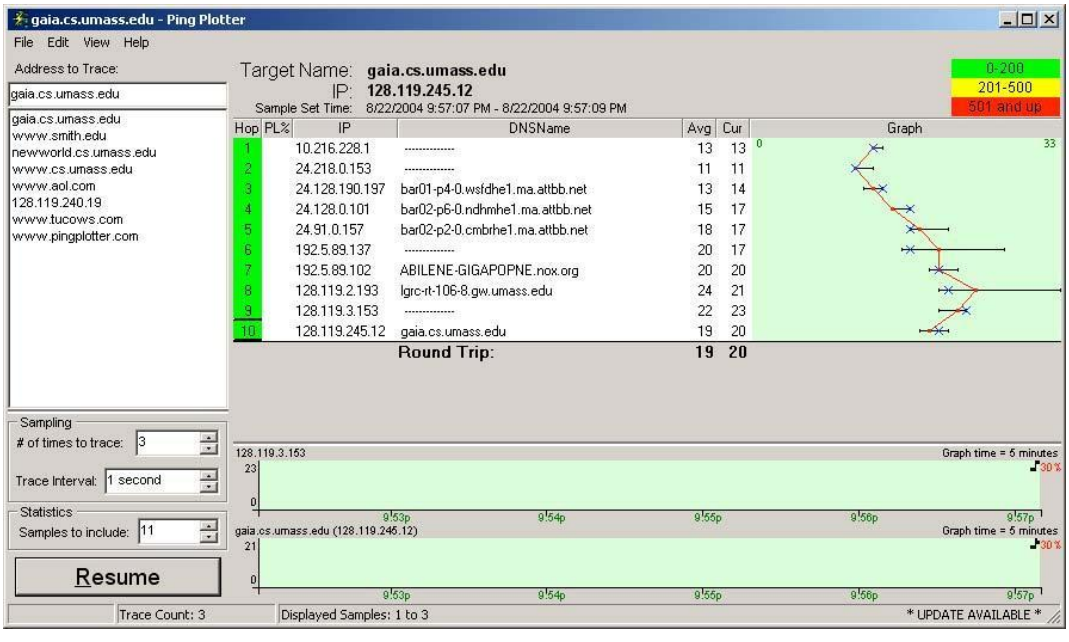
- **Windows.** El programa `tracert` proporcionado por Windows no permite cambiar el tamaño del mensaje de la solicitud de eco ICMP (ping). Una mejor versión de traceroute para Windows es el programa `pingplotter`, disponible tanto en versiones libres y shareware http://www.pingplotter.com. Si trabajáis en windows, descarga e instala `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*. 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 reinicios se puede configurar de forma explícita en `pingplotter`.

- **Linux/Unix/MacOS.** 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 traceroute de 2000 bytes hacia gaia.cs.umass.edu, el comando sería:

```
%traceroute gaia.cs.umass.edu 2000
```

Haz lo siguiente:

- Ejecute Wireshark y comience la captura de paquetes (Capture-> Start),
- Si está utilizando Windows, ejecuta `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*. Introduce 56 en el campo "*Packet Size*". A continuación, presiona *Trace.*
- A continuación, envía un conjunto de datagramas con una longitud más larga, seleccionando *Edit-> Advanced Options -> Packets Options.* Introduce el valor 3500 en el campo Packet Size. A continuación, pulse el botón Reanudar. Detenga la captura de Wireshark.
- Si está utilizando UNIX (aragorn.elo.utfsm.cl, por ejemplo), entre dos comandos `traceroute`, uno con tamaño de datagrama de 56 bytes, y otro con tamaño de datagrama de 3500 bytes. Detenga la captura de Wireshark.



Si no puedes ejecutar Wireshark en una conexión de red en vivo, puedes descargar el archivo de seguimiento de paquetes que fue capturado mientras seguía los pasos anteriores en una de las computadoras Windows del autor[2]. Puede que te resulte útil descargar esta captura, incluso si has capturado tu propio tráfico y lo has utilizado para responder a las siguientes preguntas.

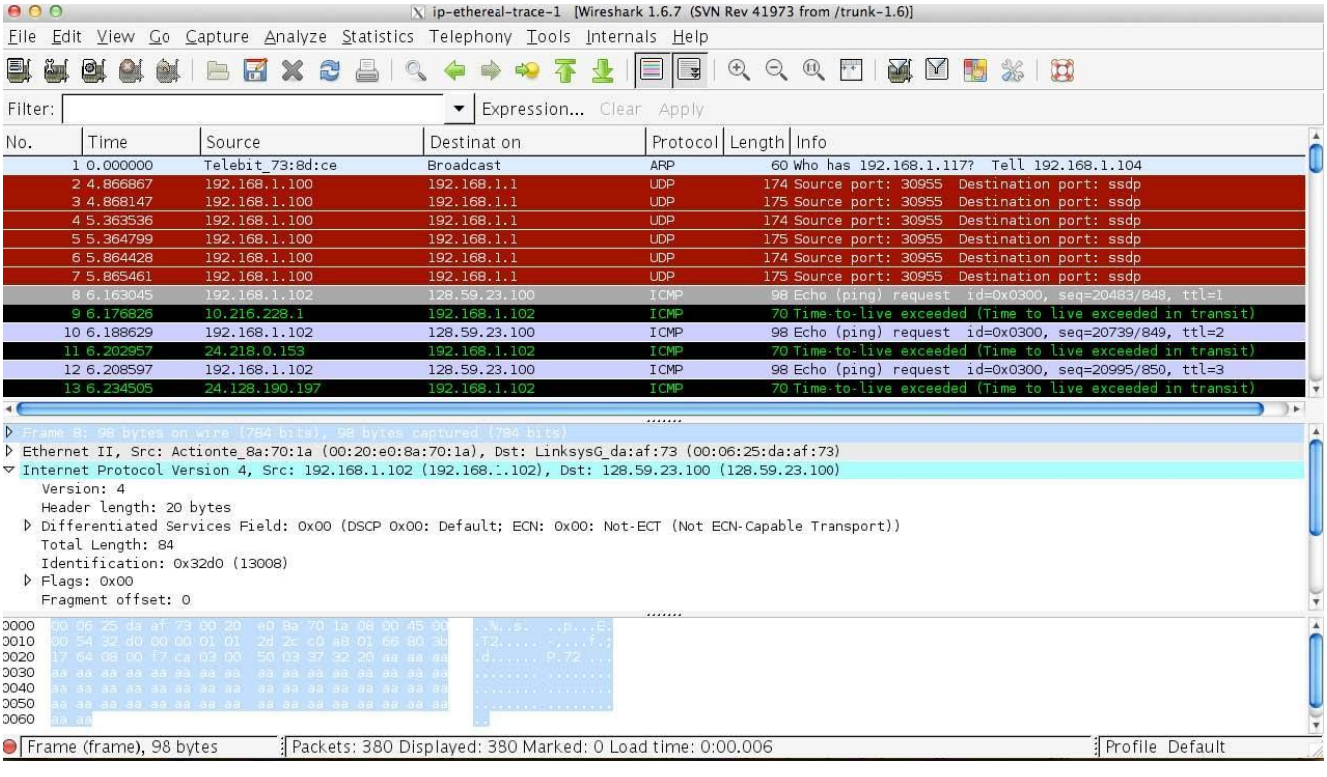
[2] Descargue el archivo zip http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip y extraiga el archivo ipethereal-trace-1. Wireshark recopiló los rastros en este archivo zip ejecutándose en una de las computadoras del autor, mientras realizaba los pasos indicados en el laboratorio de Wireshark. Una vez que haya descargado la traza, puede cargarla en Wireshark y ver la traza usando el menú desplegable Archivo, eligiendo Abrir y luego seleccionando el archivo de traza ip-ethereal-trace-1

2. Análisis de los datagramas IP capturados

En su traza, deberías ver una serie de mensajes ICMP Echo Request (en el caso Windows) o segmentos UDP (en el caso Unix) enviados por el computador y mensajes ICMP TTL-Exceeded retornados a su equipo por los routers intermedios. En las siguientes preguntas, se supone que estás utilizando una máquina de Windows; las preguntas correspondientes para el caso de una máquina Unix las puedes sacar por analogía, si tienes dudas pregunta al profesor.

Cuando sea posible, al responder una pregunta realiza una impresión del paquete (s) que utilizaste para responder a la pregunta. Agrega comentarios a la impresión para explicar tu 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? Explica cómo determinó el número de bytes de carga útil.
4. ¿Se ha fragmentado este datagrama IP? Explicar cómo identificas 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.

A continuación (con los paquetes aún ordenados por dirección de origen) busque la serie de respuestas ICMP TTL excedidas enviadas a su computadora por el router más cercano (primer salto).

5. ¿Qué campos en el datagrama IP siempre cambian de un datagrama al siguiente dentro de esta serie de mensajes ICMP enviados por tu computador?
6. ¿Qué campos se mantienen constantes? ¿Qué campos deben permanecer constantes? ¿Qué campos deben cambiar?
7. Describe el patrón que ves en la secuencia de valores del campo Identificación del datagrama IP.

Siguiente (con los paquetes todavía ordenados por dirección de origen) encontrar la serie de ICMP TTL excedido en las respuestas enviadas al ordenador por el router más cercano (primer salto).

8. ¿Cuál es el valor en el campo de Identificación y el 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?

3. 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? [[Nota: si encuentra que su paquete no se ha fragmentado, debe descargar el archivo zip http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip y extraer el rastreo de ipethereal-trace-1packet. Si su computadora tiene una interfaz Ethernet, un tamaño de paquete de 2000 debería causar fragmentación.[3]]
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?

Ahora busque el primer mensaje de solicitud de eco ICMP que envió su computadora después de cambiar el tamaño del paquete en el pingplotter a 3500.

13. ¿Cuántos fragmentos fueron creados a partir del datagrama original?
14. ¿Qué campos de la cabecera IP cambian entre los fragmentos?

[3]Los paquetes en el archivo de rastreo ip-ethereal-trace-1 en http://gaia.cs.umass.edu/wireshark-labs/wiresharktraces.zip tienen menos de 1500 bytes. Esto se debe a que la computadora en la que se recopiló el rastreo tiene una tarjeta Ethernet que limita la longitud del paquete IP máximo a 1500 bytes (40 bytes de datos de encabezado TCP / IP y 1460 bytes de carga útil del protocolo de capa superior). Este valor de 1500 bytes es la longitud máxima estándar permitida por Ethernet. Si su traza indica un datagrama de más de 1500 bytes y su computadora está usando una conexión Ethernet, entonces Wireshark está reportando la longitud incorrecta del datagrama IP; es probable que también muestre solo un datagrama IP grande en lugar de varios datagramas más pequeños. Esta inconsistencia en las longitudes informadas se debe a la interacción entre el controlador Ethernet y el software Wireshark. Recomendamos que, si tiene esta inconsistencia, realice esta práctica de laboratorio utilizando el archivo de seguimiento ip-ethereal-trace-1.