Traceroute

Axel J. Iglesias, Agustín Martinez Suñe, Nahuel Lascano

***Abstract*—En este trabajo vamos a implementar un traceroute y hacer un análisis de la rutas que realizan los paquetes por la red.**

I. Introducción

El primer paso para desarrollar el TP fue familiarizarse con las herramientas que íbamos a utilizar. Para esto, buscamos distintas implementaciones de traceroute con scapy y analizamos su funcionamiento.

Para los análisis decidimos utilizar 3 Universidades: Rusia (www.msu.ru), China (www.cuhk.edu.hk) y Cuba (www.uh.cu). Para cada caso encontramos interesantes resultados que vamos a explicar en su correspondiente punto.

II. Estimación de RTT

El primer punto fue hacer un análisis teórico del tiempo de respuesta entre las distintas universidades y el host local y compararlo con la implementación nuestra y la del Sistema Operativo.

A. Teórico

Para la estimación de los RTT's teóricos BLA BLA BLA
Obteniendo como resultado:

- Universidad Estatal de Moscú: 13500km / 67.435 ms
- Universidad de la Habana: 6900km / 34.507 ms
- Universidad China de Hong Kong: 18500km / 92.46 ms

B. Práctico

Para este análisis implementamos de distintas maneras el traceroute. Sin embargo, varias tenían algunas irregularidades como por ejemplo, que en los laboratorios devolvió resultados muy particulares que más adelante se detallan. La implementación que se encuentra en el TP se "cuelga" esperando respuestas que nunca llegan, pero se puede continuar arpetando ctrl+c.

El Sistema Operativo usado fue Mac OS X 10.9.

B.1 Implementación en Scapy

Como se observa en el código, se utiliza el protocolo TCP para hacer el análisis. La idea es sencilla, enviar los paquetes a destino aumentando el TTL hasta llegar al destino. Por cada paquete, identificamos el RTT, la IP que nos está respondiendo, si es el destino y un cálculo que nos servirá para buscar enlaces transatlánticos.

Por otro lado, se hicieron pruebas en 3 rangos horarios distintos.

Los resultados obtenidos fueron:

Hora	Rusia	China	Cuba
12Hs	277ms	361ms	No Responde
16Hs	546ms	626ms	No Responde
18Hs	354ms	402ms	No Responde

Es interesante ver que a las 19hs de Moscú (16hs de Bs As) es el momento donde mayor RTT hay. Sin embargo haya que tener en cuenta el detalle de que, al ser una comunicación transatlántica, posiblemente el paquete viaje por distintas zonas horarias y esto aumentará o disminuirá el RTT dependiendo del consumo de cada país.

El caso de Cuba nos desorientó bastante. No pudimos conseguir respuesta mediante un ping ni tampoco mediante un traceroute. En algunos casos, todos los paquetes tenían como origen de la respuesta el router local (192.168.0.1). No pudimos descifrar a que se debe este accionar.

B.2 Implementación del Sistema Operativo

Utilizando el traceroute del SO obtuvimos estos resultados:

Hora	Rusia	China	Cuba
12Hs	270ms	357ms	No Responde
16Hs	603ms	457ms	No Responde
18Hs	325ms	521ms	No Responde

C. Análisis

Luego de haber hecho las pruebas, vemos que la implementación del SO no tiene mayores diferencias a la que implementamos nosotros. Aunque si cuenta con más herramientas que las que nosotros hicimos. Como mencionamos antes, el horario en el que se realizan las pruebas influye en el rendimiento que obtenemos. Este rendimiento se verá afectado por el horario no solo actual sino también de los países de los enlaces que utilice el paquete para llegar a destino.

FALTA ANALIZAR Y GRAFICAR EL ULTIMO PUNTO DEL 3.1.1

III. Enlaces transatlánticos

En esta segunda parte, vamos a encontrar los enlaces transatlánticos que usa nuestro paquete.

A. Implementación

Para resolver este punto se modificó el código del traceroute para que vaya acumulando las mediciones y calcule el promedio, el desvío y la posibilidad de que el enlace sea transatlántico.

A su vez, implementaos un script que toma una lista de IP's y utiliza la web propuesta por la materia para buscar su geolocalización.

Utilizando estas dos herramienta, comparamos los resultados teóricos con los verdaderos saltos.

En términos generales, la heurística detectó algunos enlaces transatlánticos, pero para la gran mayoría no lo hizo. Hubo tanto falsos positivos como verdaderos negativos. Creemos que esto puede deberse no tanto al cálculo en si, sino al error general de la implementación que no pudimos resolver.

B. Análisis de geolocalización

Luego de realizar las pruebas, nos encontramos con que varias veces la heurística toma como enlace transatlántico al segundo enlace en un nuevo continente. A continuación damos un ejemplo:

IP	Geolocalización	Heurística
192.168.0.1	Router	False
181.167.38.1	Arg	False
200.89.165.49	Arg	False
200.89.165.6	Arg	False
200.89.165.150	Arg	False
64.214.130.253	EUA	False
67.17.74.46	EUA	True
146.82.54.2	EUA	True
194.85.40.129	Rusia	True
194.85.40.133	Rusia	True
194.190.254.118	Rusia	False
93.180.0.174	Rusia	False
188.44.33.41	Rusia	False
188.44.33.22	Rusia	False
93.180.0.18	Rusia	False

Esta situación se repite en cada uno de los casos. Creemos que puede deberse a la falta d información de algunos hops.

Por otro lado, aumentar m lo único que provocaría es menos falsos positivos pero no conseguiríamos encontrar los enlaces que de por si no encontramos. Disminuir m nos daría más falsos positivos.

Otra situación que nos llamó la atención en la ubicación de los enlaces transatlánticos. Observemos que para enviar el paquete a Rusia, el mismo debe pasar por EUA. En el caso de Cuba:

IP	Geolocalización
192.168.0.1	Argentina
181.167.38.1	Argentina
200.89.165.33	Argentina
200.89.165.2	Argentina
200.89.165.101	Argentina
200.89.165.86	Argentina
200.89.165.85	Argentina
200.89.165.1	Argentina
200.89.165.250	Argentina
64.209.94.97	EUA
67.16.139.65	EUA
67.16.139.65	EUA
213.140.53.109	España
176.52.255.6	España
94.142.118.33	España
94.142.118.45	España
200.0.16.73	Cuba

Nuevamente el recorrido cruza por EUA. Pero para el caso de Hong Kong:

Hop	IP	Geolocalización
1	192.168.0.1	Argentina
2	181.167.38.1	Argentina
5	200.89.165.49	Argentina
6	200.89.165.2	Argentina
9	200.89.165.101	Argentina
10	200.89.165.86	Argentina
11	195.22.220.128	Italia
12	195.22.223.164	Italia
13	195.22.223.142	Italia
14	115.160.187.102	Hong Kong
15	175.45.11.98	Hong Kong
16	203.188.117.34	Hong Kong
17	137.189.192.250	Hong Kong
18	137.189.9.57	Hong Kong
19	137.189.11.73	Hong Kong

Con esto llegamos a dos conclusiones. La primera es que en Argentina contamos con enlaces a distintos continentes que se utilizan de maneras diversas. Esto provoca que cruzar a Europa pueda hacerse directamente (Arg-Italia) o bien pasando por America del Norte (Arg-EUA-España). La segunda, más que una conclusión es un interrogante. Nos llama la atención que particularmente el paquete a Cuba pacer por EUA. Al saber que a nivel continental muchos enlaces no son simples algoritmos de routeo sino que están dirigidos, nos parece un dato importante el que obtuvimos con este análisis.

Por último, otra heurística que se podría llegar a utilizar en cierta medidas, es el análisis de los prefijos de IP. Creemos que podría ser bastante acertada dada la distribución de los números IP globalmente.