DEPARTAMENTO
DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico II

Teoría de las Comunicaciones
Primer Cuatrimestre de 2016

Integrante	LU	Correo electrónico
Iván Arcuschin	678/13	iarcuschin@gmail.com
Federico De Rocco	408/13	fede.183@hotmail.com
Martín Jedwabny	885/13	martiniedva@gmail.com
José Massigoge	954/12	jmmassigoge@gmail.com

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2160 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (54 11) 4576-3359
http://www.fcen.uba.ar

Índice

1. Introducción

En el presente Trabajo Práctico nos propusimos experimentar con herramientas y técnicas frecuentemente utilizadas a nivel de red. En particular implementamos una herramienta cuya funcionalidad replica la de `traceroute`. A partir de la misma nos enfocamos en medir los `Round-Trip delay Time (RTT)` entre diversos hosts en búsqueda de obtener una mínima noción de la topología de la red global, en particular intentando detectar los enlaces entre diversos continentes.

Nuestra implementación de `traceroute` se baso en el intercambio de mensajes de tipo `echo request /reply` y `time exceeded` del protocolo `ICMP`[3]. Concretamente, utilizando la librería scapy, armamos varios paquetes de tipo `echo request`, variando el campo `Time To Live (TTL)` de los mismos entre 1 y un valor lo suficientemente grande tal que nos permita llegar a cualquier host, siendo 30 ese valor. Una vez enviados los paquetes, cuando recibimos respuesta, estas fueron de tipo `time exceeded` o `echo reply`.

El cálculo de la ruta entre dos hosts consistió en realizar varias iteraciones de nuestro `traceroute` a la dirección destino, y, con esa información, obtener la ruta habitual entre nuestro host fuente y destino. Por habitual nos referimos a aquella ruta tomada por los paquetes en la mayoría de los casos. Tuvimos que determinar una ruta habitual debido al hecho que los paquetes no siguieron siempre un mismo camino, lo cual, siguiendo la terminología propuesta por Jobst[1], se puede deber a diversas anomalías (*missing links*, *false links*, *loops and circle* y *diamonds*). Una de las principales razones por la cual surgen este tipo de anomalías es debido al balanceo de carga por paquete que realizan los routers.

Por otro lado, el cálculo del `RTT` entre los diversos hosts consistió en tomar el timestamp en el cual fue enviado el paquete y el timestamp de cuando se recibió la respuesta al mismo. Tomando como muestra aquellos tiempos correspondientes a la ruta habitual entre dos hosts, previo descarte de los outliers utilizando la metodología propuesta por Cimbala[2], definimos el `RTT` entre dos hosts como la media muestral. Nuevamente, en diversos casos, nos encontramos con una anomalía denominada *false RTT*. La misma consiste en la aparición de valores de `RTT` que no son consistentes, por ejemplo valores menores para hosts que se encuentran a distancias mayores que otros mas cercanos. La aparición de esta anomalía se puede deber a dos razones, rutas de paquete asimétricos o enrutamiento MPLS. Cuando los respectivos caminos hacia y desde el destino son asimétricos, es decir, los paquetes se encaminan por senderos diferentes desde y hacia el objetivo, los tiempos de ida y vuelta pueden no reflejar el tiempo real que tarda un paquete para llegar al destino. MPLS es un caso similar al anterior y podría verse en que los tiempos de ida y vuelta casi equivalentes para varios saltos en el resultado de traceroute.

Por último es importante mencionar que no obtuvimos respuesta de todos los router, este fenómeno se debe a la anomalía *missing hop*. Anomalía que puede ser producto de la existencia de un firewall en el router o una configuración del mismo para no generar respuesta a paquetes cuyo `TTL` es 0.

2. Experimentación

En esta sección desarrollaremos y mostraremos los resultados de los experimentos para las siguientes universidades:

- Universidad de Oxford (Reino Unido, Europa)
- Universidad de Sydney (Australia, Oceanía)
- Universidad de Ghana (Ghana, África)
- Universidad de Hong Kong de Ciencia y Tecnología (China, Asia)

Para llevar adelante los experimentos utilizamos la herramienta descripta en la introducción. La cantidad de veces que ejecutamos nuestra versión de `traceroute` para cada universidad fue de **50**. Con esa cantidad lo que buscamos es minimizar las oscilaciones en las rutas y tiempos fruto de balanceos de carga de los routers.

Para identificar los saltos intercontinentales, primero calculamos la variación en los RTT entre cada par de hops consecutivos, ΔRTT_i, de la siguiente manera: $\Delta RTT_i = RTT_i - RTT_{i-1}$, donde $2 \leq i \leq$ cantidad de hops. Luego tomamos estos ΔRTT como input para la técnica de estimación de outliers propuesta por Cimbala[2]. Los outliers detectados por la técnica serán nuestros candidatos a enlaces intercontinentales. A partir de este cálculo, tendremos en cuenta la detección de falsos positivos y negativos contrastando nuestra inferencia con herramientas de geolocalización de direcciones IP, (**ipinfo.io o ip2location.com**).

Por último, propondremos hipótesis para los casos de comportamiento anómalo.

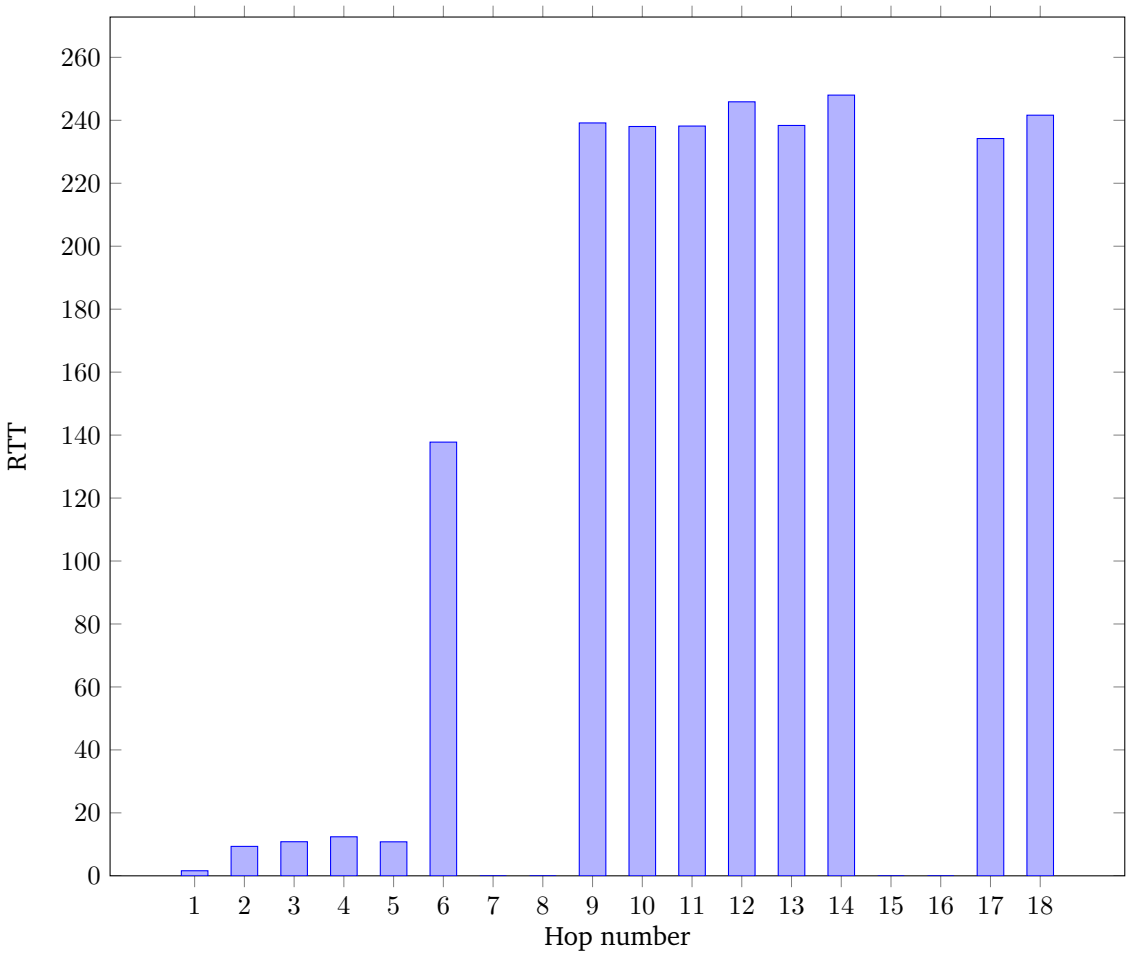
2.1. Universidad de Oxford

Los resultados de este experimento pueden resumirse en el siguiente cuadro:

Hop #	IP	RTT (ms)	Δ RTT (ms)	Ubicación (ipinfo.io)
1	192.168.0.1	1.61	-	IP privada
2	10.27.128.1	9.35	7,74	IP privada
3	10.242.1.61	10.83	1,48	IP privada
4	208.178.195.214	12.40	1,57	Estados Unidos
5	208.178.195.213	10.80	-1,6	Estados Unidos
6	67.17.99.233	137.77	126,97	Estados Unidos
7	*	-	-	-
8	*	-	-	-
9	212.187.139.166	239.16	-	Reino Unido
10	146.97.33.2	238.03	-1,13	Reino Unido
11	146.97.37.194	238.17	0,14	Reino Unido
12	193.63.108.94	245.87	7,7	Reino Unido
13	193.63.108.98	238.36	-7,51	Reino Unido
14	193.63.109.90	248.00	9,64	Reino Unido
15	*	-	-	-
16	*	-	-	-
17	192.76.32.62	234.21	-	Oxford, Inglaterra, Reino Unido
18	129.67.242.154	241.62	7,41	Oxfordshire, Reino Unido

Cuadro 1: Ruta Universidad de Oxford (ox.ac.uk - IP 129.67.242.154)

A continuación graficamos los RTT en función de los hops para analizar más fácilmente las anomalías detectadas.



Con este gráfico podemos claramente observar los saltos negativos y en los que no hubo respuesta(estos últimos los notamos con RTT -1).

Daremos nuestras hipótesis sobre que casos son los que identificamos como anomalías False RTT.

- El enlace entre los hops 4 y 5. Es asimétrico ya que la diferencia entre los RTTs de los hops mencionados y los anteriores es demasiado grande para ser causado por MPLS.
- El enlace entre los hops 9 y 10. Igual al caso anterior.
- El enlace entre los hops 12 y 13. Igual al caso anterior.
- El enlace entre los hops 14 y 17. Igual al caso anterior, con la particularidad de que los hops 15 y 16 son *missing hops*.

Los hops para los cuales no tuvimos respuesta fueron: 7, 8, 15, 16.

La herramienta de geolocalización nos dice que el hop 6 pertenece a Estados Unidos y el 9 pertenece a Reino Unido. Dado que el ΔRTT entre estos dos hops es significativamente grande, inferimos que hay entre ambos un salto intercontinental, aunque no hayamos obtenido respuesta de los hops 7 y 8.

Probando con la universidad de Cambridge (también en Reino Unido) obtuvimos un resultado similar: dos hops perdidos, lo cual nos sugiere que el enlace intercontinental entre Estado Unidos y Reino Unido tiende a caer en esta situación.

Como hipótesis alternativa podríamos pensar que esto ocurre por culpa del enlace intercontinental, ya sea por una cuestión de excesivo transito o por causas más puntuales sobre las configuraciones o protecciones de este.

En el caso de los hops 15 y 16 ocurre algo parecido, puesto que el hop 14 parece pertenecer al Reino Unido (sin ubicar región ni ciudad) mientras que el hop 17 pertenece a Oxford. En este caso es más probable que se trate de una situación aislada ya que no existe un salto intercontinental, solamente regional.

También podemos observar que los hops 4 y 5 se muestran como ubicación a Estados Unidos, aunque los RTT de ambos no corresponden con la distancia que tuvieron que recorrer entre los hops 3 y 4. El hop 6 posee un RTT más propio del primero ubicado en Estados Unidos. Una posible explicación para esta anomalía es que los servidores intermedios entre Argentina y Estados Unidos(posiblemente ubicados en Brasil) pertenecen a una compañía estadounidense y nuestra herramienta de ubicación utiliza este dato para aproximar su ubicación. Es posible que el hop 6 también sufra de este error de aproximación ya que usando herramientas alternativas de geolocalización de IP nos dio como resultado Holanda. Creemos que ésta ubicación es la más acertada ya que el salto intercontinental que habría entre Estados Unidos y Londres debería tener un ΔRTT bastante más grande. Sin embargo, el salto que separa a Holanda de Londres es demasiado grande, por lo tanto no terminamos de estar seguros.

Además nuestra herramienta identifica como posible salto intercontinental al enlace entre las IPs 208.178.195.213 - 67.17.99.233 (hops 5 y 6). Sin embargo esto podría ser incorrecto ya que la aplicación de geolocalización nos dice que ambas IP pertenecen al dominio de Estados Unidos. Aunque, podemos concluir que el salto mostrado es efectivamente intercontinental ya que, como mencionamos antes, el hops 6 podría ser de Holanda en vez de Estados Unidos.

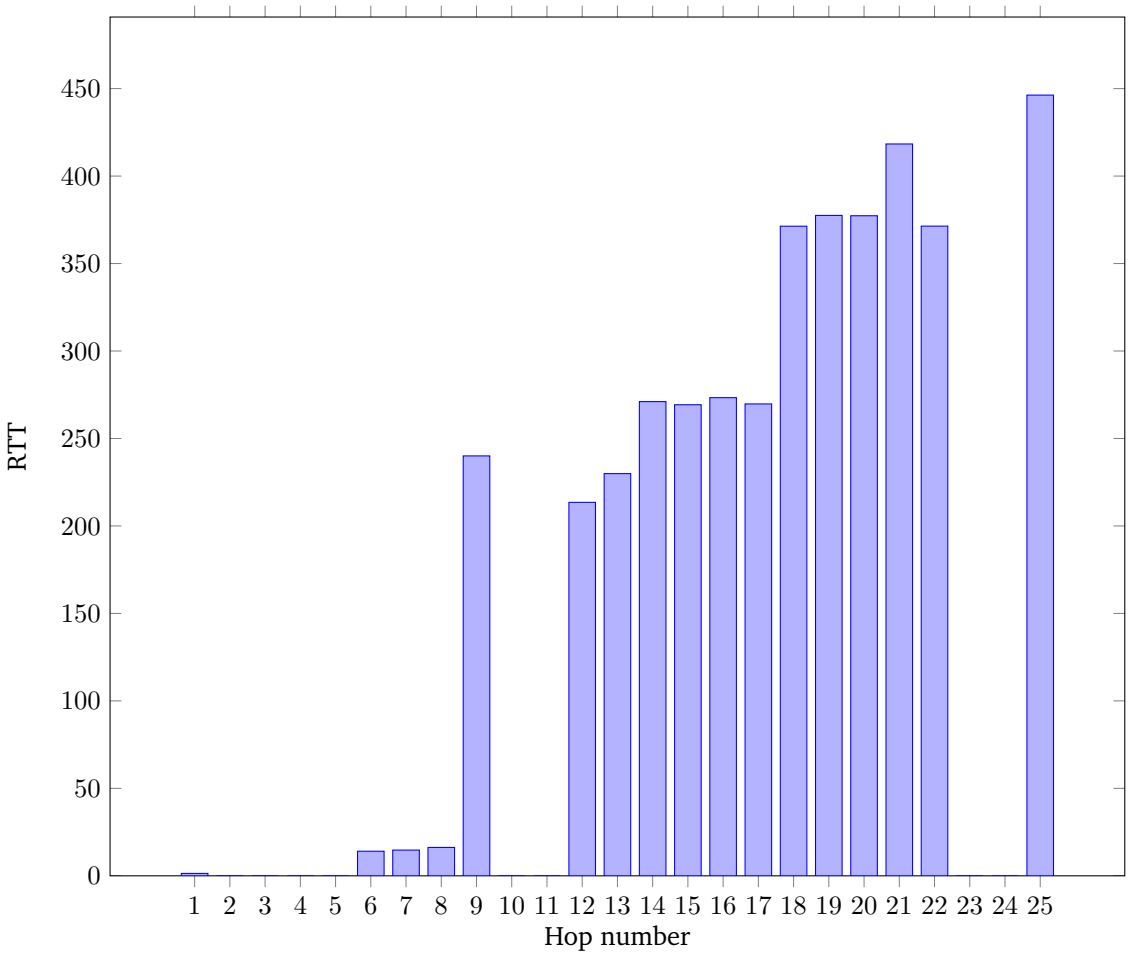
2.2. Universidad de Sydney

Los resultados de este experimento pueden resumirse en el siguiente cuadro:

Hop #	IP	RTT (ms)	Δ RTT (ms)	Ubicación (ipinfo.io)
1	192.168.0.1	1.38	-	IP privada
2	*	-	-	-
3	*	-	-	-
4	*	-	-	-
5	*	-	-	-
6	200.89.165.9	14.06	-	Argentina
7	200.89.165.250	14.71	0.65	Argentina
8	190.216.88.33	16.23	1.52	Ciudad de Buenos Aires, Argentina
9	67.17.94.249	240.04	223.81	Estados Unidos
10	*	-	-	-
11	*	-	-	-
12	4.68.127.54	213.49	-	Estados Unidos
13	129.250.4.250	229.91	16.48	Colorado, Estados Unidos
14	129.250.2.219	271.08	41.17	Colorado, Estados Unidos
15	129.250.7.69	269.29	-1.79	Colorado, Estados Unidos
16	129.250.3.123	273.33	4.04	Colorado, Estados Unidos
17	204.1.253.166	269.75	-3.58	Colorado, Estados Unidos
18	202.158.194.172	371.34	101.59	Canberra, Australia
19	113.197.15.68	377.51	6.17	Canberra, Australia
20	113.197.15.66	377.32	-0.19	Canberra, Australia
21	113.197.15.152	418.35	41.03	Canberra, Australia
22	138.44.5.47	391.39	-26.96	Victoria, Australia
23	*	-	-	-
24	*	-	-	-
25	129.78.5.8	446.28	-	Sydney, Australia

Cuadro 2: Ruta Universidad de Sydney (sydney.edu.au - IP 129.78.5.8)

A continuación graficamos los RTT en función de los hops para analizar más fácilmente las anomalías detectadas.



A continuación enumeramos las anomalías encontradas:

- *Missing hops*: de los hops 2, 3, 4, 5, 10, 11, 23 y 24 no obtuvimos respuesta.
- *False RTT por rutas asimétricas*: entre los hops 14-15, 16-17, 19-20, 21-22 obtuvimos valores negativos en el ΔRTT, valores no consistentes. En particular el caso de los hops 21-22 es el más significativo, especulamos que en este caso la ruta de vuelta de los paquetes difiere considerablemente con respecto a la ida. Por otro lado entre los hops 9-12 también encontramos una inconsistencia considerable entre los valores de `RTT` de ambos hosts, independientemente de que no sean hosts consecutivos. Nuevamente especulamos con rutas de ida y vuelta que difieren significativamente.
- *False RTT por MPLS routing*: la cercanía de los valores de `RTT` de los hops 14, 15, 16 y 17 y, por otro lado, los hops 18, 19 y 20, nos inducen a pensar que estos valores pueden caer dentro de la descripción de esta anomalía.

Con respecto a la detección de los enlaces intercontinentales, nuestra herramienta arroja como principal candidato al enlace entre los hops 8 y 9 ($\Delta RTT = 223{,}81$). El otro candidato es el enlace entre los hops 17-18 ($\Delta RTT = 101{,}59$).

Contrastando nuestra hipótesis contra las ubicaciones arrojadas por la aplicación de geolocalización, vemos que el enlace entre los hops 8 y 9 es un enlace entre Argentina y Estados Unidos, lo cual, geográficamente, no es un cambio de continente, pero si es un enlace submarino. Con respecto al enlace entre los hops 17-18 es un enlace entre Estados Unidos e Australia, lo que si representa un enlace intercontinental.

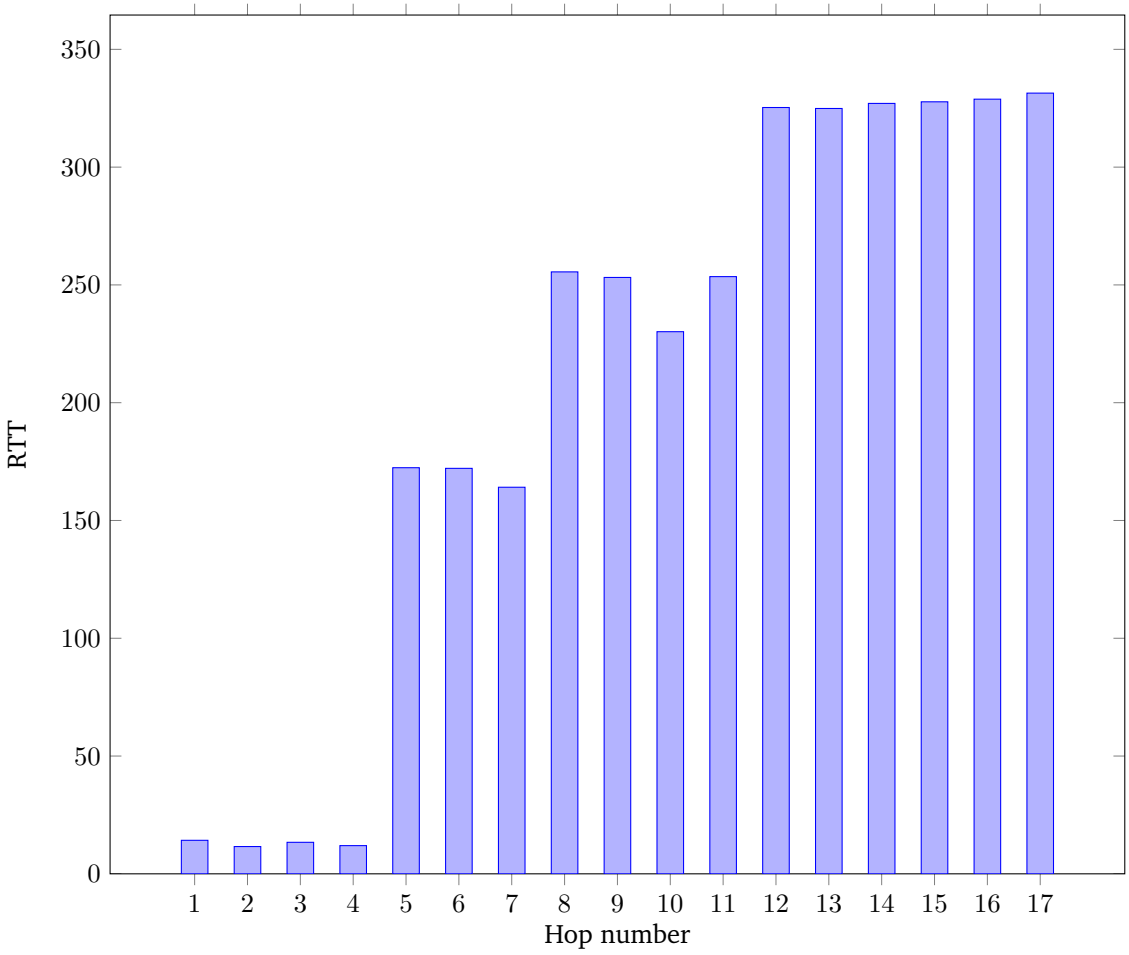
2.3. Universidad de Ghana

Los resultados de este experimento pueden resumirse en el siguiente cuadro:

Hop #	IP	RTT (ms)	Δ RTT (ms)	Ubicación (ipinfo.io)
1	10.27.64.1	14.23	-	IP privada
2	10.242.1.149	11.58	-2.65	IP privada
3	195.22.220.33	13.38	1.8	Italia
4	195.22.220.32	11.97	-1.41	Italia
5	195.22.206.92	172.40	160.43	Italia
6	195.22.206.92	172.13	0.27	Italia
7	216.6.87.202	164.11	-8.02	Delaware, Estados Unidos
8	216.6.87.169	255.53	91.42	Delaware, Estados Unidos
9	216.6.57.1	253.17	-2.36	Delaware, Estados Unidos
10	66.198.70.174	230.14	-23.03	Delaware, Estados Unidos
11	80.231.76.121	253.52	23.38	Europa
12	195.219.195.238	325.31	71.79	Europa
13	41.21.232.70	324.90	-0.41	Sudáfrica
14	41.204.60.149	327.05	2.15	Ghana
15	41.204.60.150	327.73	0.68	Ghana
16	197.255.127.2	328.85	1.12	Ghana
17	197.255.125.10	331.42	2.57	Ghana

Cuadro 3: Ruta Universidad de Ghana (ug.edu.gh - IP 197.255.125.10)

A continuación graficamos los RTT en función de los hops para analizar más fácilmente las anomalías detectadas.



En primer lugar es interesante notar que los primeros dos hops muestran IPs privadas. Aunque no

encontramos una explicación clara, podemos especular que estas corresponden a dos routers de un mismo proveedor de internet, quien les asignó IPs privadas para ahorrar IPs públicas.

Pasamos a analizar las anomalías encontradas:

- *Loop/Cycle*: en los hops 5 y 6, que tienen la misma IP. Esto podría suceder por diversas razones:
  - Debido a que el hop 5 fowardea paquetes con TTL 0.
  - Un ciclo que termina en la IP en cuestión, y que no deja ver cual es la IP verdadera del hop 5.
- *False RTT por rutas asimétricas*: en los hops 2, 4, 10 y 13 por tener incremento negativo en los saltos. El único salto de estos que podría llegar a ser debido a MPLS es el del hop 13 ($\Delta RTT = -0{,}41$), pero no fue posible confirmarlo.

Mostramos ahora los enlaces candidatos a salto continental que arroja nuestra herramienta, contrastándolos con las ubicaciones arrojadas por la aplicación de geolocalización:

1. Enlace entre los hops 4 y 5 ($\Delta RTT = 160{,}43$): Por la diferencias entre RTTs es claro que este enlace es un salto continental. Sin embargo, la aplicación de geolocalización nos dice que las IPs de los hops 3, 4, 5 y 6 corresponden a Italia, por lo que entonces estaríamos en un caso de falso positivo.

   Pero, dado que los ΔRTT entre los hops 3 y 4, y 5 y 6 son chicos, y que todas estas IPs tienen asociada la organización "AS6762 TELECOM ITALIA SPARKLE S.p.A.", concluimos que:

   - Los hops 3 y 4 corresponden en realidad a routers en Argentina, con IPs asignadas a Italia.
   - Los hops 5 y 6 corresponden efectivamente a routers en Italia, con IPs asignadas a Italia.
   - El enlace entre los hops 4 y 5 es efectivamente un salto continental.

2. Enlace entre los hops 7 y 8 ($\Delta RTT = 91{,}42$): Por la diferencias entre RTTs es claro que este enlace es un salto continental. Sin embargo, la aplicación de geolocalización nos dice que las IPs de los hops 7 y 8 corresponden a Estados Unidos, por lo que entonces estaríamos en un caso de falso positivo.

   Pero, dado que el ΔRTT entre los hops 6 y 7 es chico, y el hop 6 corresponde a Italia, podemos concluir que:

   - El hop 7 corresponde en realidad a un router en Italia, con IP asignada a Estados Unidos.
   - El enlace entre los hops 7 y 8 es efectivamente un salto continental.

3. Enlace entre los hops 11 y 12 ($\Delta RTT = 71{,}79$): Las diferencias entre RTTs nos inducen a pensar que este enlace es un salto continental, aunque la aplicación de geolocalización no nos provee información acerca de la posible ubicación de estas IPs.

   Sin embargo, debido a que el hop 10 corresponde a Estados Unidos, y el 13 a Sudáfrica concluimos que el enlace es efectivamente un salto continental, y que el hop 11 corresponde un router en Estados Unidos y el hop 12 a un router en Sudáfrica.

4. Enlace entre los hops 10 y 11 ($\Delta RTT = 23{,}38$): en base a lo concluido para el enlace entre los hops 11 y 12, este caso sería un falso positivo.

5. Enlace entre los hops 9 y 10 ($\Delta RTT = -23{,}03$): este enlace parecería ser un falso positivo, por varias razones:

   - La aplicación de geolocalización informa que ambas IPs están asignadas a Delaware, Estados Unidos.
   - El salto es negativo, lo cual podría implicar un congestionamiento en algún router.

6. Enlace entre los hops 6 y 7 ($\Delta RTT = -8{,}02$): en base a lo concluido para el enlace entre los hops 7 y 8, este caso sería un falso positivo.

2.4. Universidad de Hong Kong de Ciencia y Tecnología (HKUST)

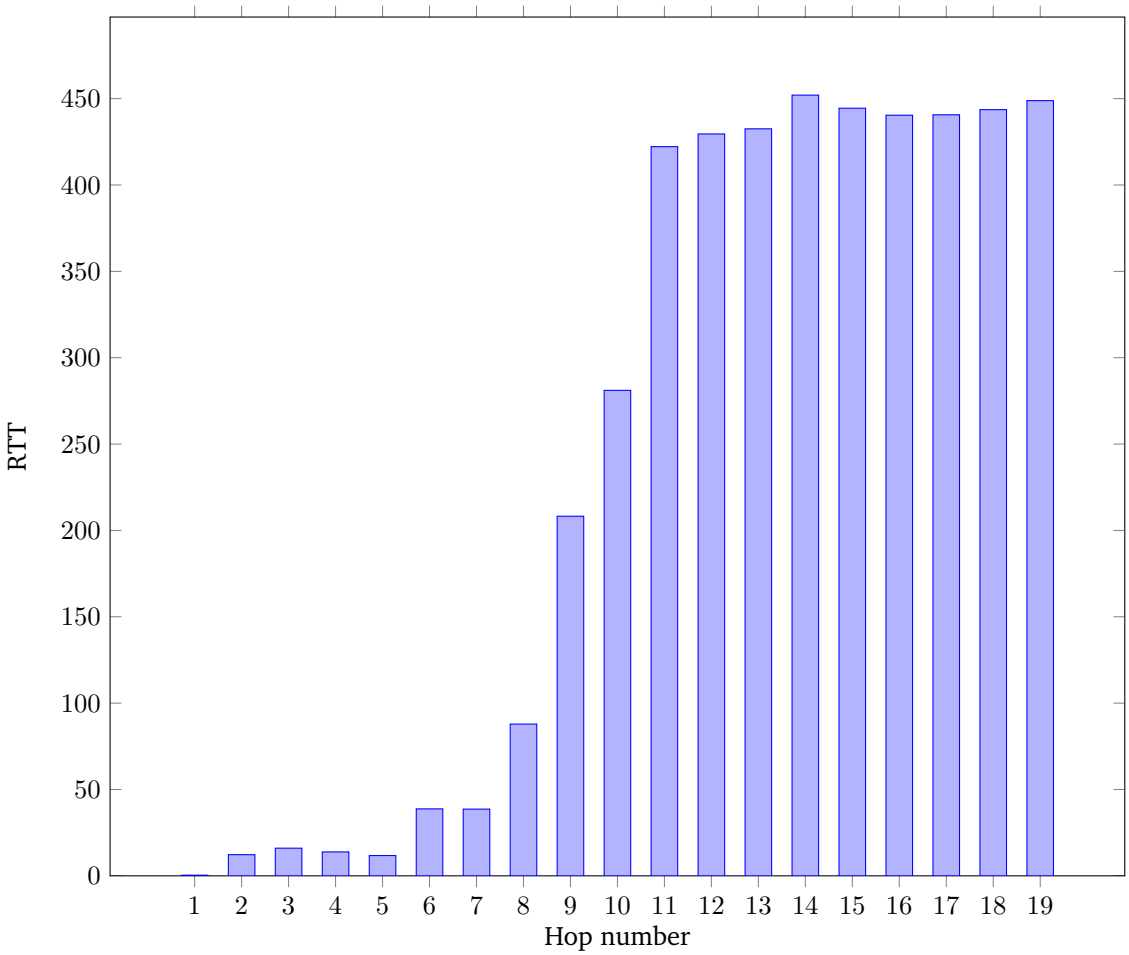
En este caso buscamos analizar los resultados de traceroute a una universidad de Hong Kong. Dada su ubicación en Asia, esperamos un gran aumento del RTT a medida que nos acercamos al destino, así como una gran cantidad de Hops y uno o varios saltos continentales.

Los resultados de este experimento pueden resumirse en el siguiente cuadro:

Hop #	IP	RTT (ms)	Δ RTT (ms)	Ubicación (ip2location.com)
1	192.168.1.1	0.36	-	Local
2	200.3.60.192	12.24	11.88	Buenos Aires
3	181.88.108.18	16.01	3.77	Buenos Aires
4	190.225.252.166	13.85	-2.16	Buenos Aires
5	195.22.220.213	11.73	-2.11	Buenos Aires
6	195.22.219.3	38.76	27.02	Italia
7	195.22.219.3	38.63	-0.13	Italia
8	149.3.181.65	87.87	49.24	Brasil
9	129.250.2.227	208.21	120.33	Nueva York, US
10	129.250.4.13	281.09	72.87	Washington, US
11	129.250.2.38	422.20	141.11	Tokyo, Japón
12	129.250.5.134	429.55	7.34	Hong Kong
13	129.250.6.115	432.51	2.96	Hong Kong
14	203.131.246.154	452.04	19.52	Hong Kong
15	115.160.187.110	444.46	-7.57	Hong Kong
16	202.130.98.102	440.41	-4.05	Hong Kong
17	203.188.117.130	440.65	0.24	Hong Kong
18	202.14.80.153	443.62	2.97	Hong Kong
19	143.89.14.2	448.84	5.21	Hong Kong

Cuadro 4: Ruta Universidad de Hong Kong de Ciencia y Tecnología (www.ust.hk - IP 143.89.14.2)

A continuación graficamos los RTT en función de los hops para analizar más fácilmente las anomalías detectadas.



Como podemos ver, a gran escala los `Round Trip Times` parecen obedecer nuestra suposición de que iba a escalar fuertemente a medida que nos acercamos al destino. La cantidad de hops en total fue 19, algo bastante grande y lógico dada la distancia entre el origen (Argentina) y el destino (Hong Kong).

Con respecto a las otras anomalías, nos sorprendió no detectar Missing Hops en ningún momento. Entre los hops 1 a 3, 11 a 13 y 16 a 19, los RTTs incrementaron gradualmente. Sin embargo tenemos las siguientes anomalías:

- `False RTTs`: entre los hops 3 y 4, 4 y 5, 14 y 15, 15 y 16. Esto se puede deber a rutas asimétricas que hacen que la diferencia entre los RTTs de hops sucesivos sea negativa porque en el segundo hop, el traceroute vuelve por una ruta más rápida.
- *Loop/Cycle*: entre los hops 6 y 7, esto se puede deber a que hay un ciclo en la topología y cuando el TTL es 7, el traceroute toma una ruta para llegar al mismo router que con TTL 6 que pasa por un router más que cuando el RTT es 6 pero llegan al mismo router porque hay un ciclo donde una ruta es más grande que la otra.

Con respecto a la detección de los enlaces intercontinentales, nuestra herramienta arroja como principal candidato al enlace entre los hops 10 y 11 ($\Delta RTT = 141{,}11$). El siguiente candidato es el enlace entre los hops 8 y 9 ($\Delta RTT = 120{,}33$). El último candidato detectado es el enlace entre los hops 9 y 10 ($\Delta RTT = 72{,}87$).

Por otro lado, la aplicación de geolocalización utilizada en este caso, ip2location.com, estipula varios saltos continentales, siendo los mismos:

- Argentina (Sudamérica) - Italia (Europa) entre hops 5 y 6.
- Italia (Europa) - Brasil (Sudamérica) entre hops 7 y 8.
- Brasil (Sudamérica) - Estados Unidos (Norteamérica) entre hops 8 y 9.

- Estados Unidos (Norteamérica) - Japón (Asia) entre hops 10 y 11.

Vemos una correspondencia entre los primeros dos candidatos que predice nuestra herramienta y el resultado de la aplicación de geolocalización. Es decir, tanto el enlace entre los hops 10 y 11 como el enlace entre los hops 8 y 9 corresponden a enlaces intercontinentales, (Estados Unidos-Japón y Brasil - Estados Unidos respectivamente). Por otro lado, el enlace entre los hops 9 y 10 sería un falso positivo según la ubicación dada por la aplicación de geolocalización, ya que este correspondería a una conexión entre dos ciudades de Estados Unidos, en particular especulamos que el mismo debe ser un enlace que une la costa este con la costa oeste de este país.

Queda por analizar la supuesta presencia de dos falsos negativos, los enlaces entre los hops 5 y 6 y los hops 7 y 8, que, según la aplicación de geolocalización, corresponden a enlaces entre Argentina e Italia e Italia y Brasil, respectivamente. Sin embargo los valores de RTT de los hops 6 y 7, (ambos hops corresponden al mismo host), nos inducen a pensar que este host no esta ubicado en Italia. Hipótesis que se encuentra reforzada por el hecho que la dirección de IP corresponde al ISP "AS6762 TELECOM ITALIA SPARKLE S.p.A.", organización que opera tanto en Argentina como en Italia.

Entonces para concluir, vemos que de los posibles candidatos el único enlace que es efectivamente intercontinental es el de los hops 10 y 11 (Estados Unidos - Japón).

3. Conclusiones

Como conclusión queremos mencionar que la implementación de nuestro `traceroute` nos resultó sencilla, fruto de las facilidades que nos otorgó la librería `scapy` a la hora de armar, enviar y recibir paquetes utilizando el protocolo `ICMP`. Sin embargo, nos hubiera gustado llegar a implementar un `traceroute` utilizando los flags Option de los paquetes `IP`, cuyas ventajas sobre una implementación basada en `ICMP` es la menor cantidad de paquetes que necesita para funcionar y el hecho que establece una ruta única al destino. Ésta limitación se debió a la, prácticamente, inexistente documentación de la librería scapy, razón por la cual nos resultó muy dificultoso la implementación mediante prueba y error.

Por otro lado, nos parece importante mencionar, a partir de los resultados de nuestros experimentos, lo común que resultan las diversas anomalías en la red. En particular los *false RTT* y los *missing hops* fueron las anomalías con mayor frecuencia de aparición. Entendemos que esta problemática dificulta mapeos de la red y dificulta la detección y solución de diversos problemas, como los mencionados por Jobst en su artículo[1].

Por último, nos resultó curioso las discrepancias entre la ubicación posible de los host inferida a partir de los valores de `RTT` del mismo y la ubicación de los mismos dadas por herramientas de geolocalización. Concluimos que estas diferencias se deben a como están implementadas las herramientas de geolocalización, las cuales parecería que relacionan ubicación de un host con los prefijos en su dirección IP, sabiendo que rango de direcciones pertenecen a que organización.

4. Referencias

[1] http://www.net.in.tum.de/fileadmin/TUM/NET/NET-2012-08-1/NET-2012-08-1_02.pdf.

[2] http://www.mne.psu.edu/cimbala/me345/Lectures/Outliers.pdf.

[3] Internet Control Message Protocol. RFC 792, March 2013.