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`. 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 calculo 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 tomado 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, se puede deber a diversas anomalías (*missing links*, *false links*, *loops and circle* y *diamonds*). Este tipo de anomalías surgen a partir del balanceo de carga por paquete que realizan los routers.

Por otro lado, el calculo 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, 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 ultimo 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)
- Universidad de Sydney (Australia)
- Universidad de Ghana (Africa)

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 balanceaos de carga de los routers.

Para identificar los saltos intercontinentales 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. Siendo los candidatos a saltos intercontinentales los pares de hops con ΔRTT mayor al resto. A partir de este calculo, tendremos en cuenta la detección de falsos positivos y negativos contrastando nuestra inferencia con herramientas de geolocalización de direcciones IP, (**ref a geolookip o lo que sea**).

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

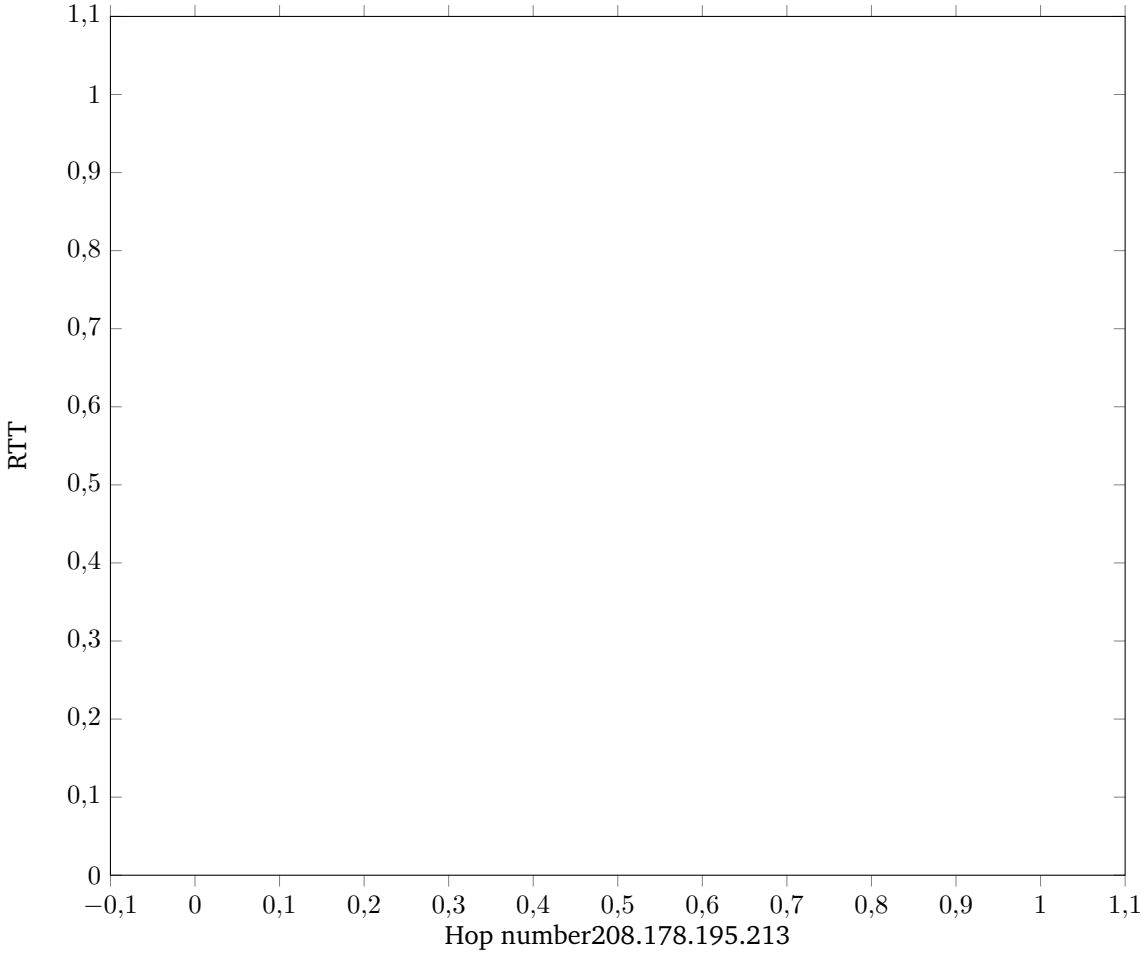
2.1. Universidad de Oxford

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

Hop #	IP	RTT (ms)	Δ RTT (%)	Ubicacion
1	192.168.0.1	1.61	-	IP privada
2	10.27.128.1	9.35	-	IP privada
3	10.242.1.61	10.83	-	IP privada
4	208.178.195.214	12.40	-	Estados Unidos
5	208.178.195.213	10.80	-	Estados Unidos
6	67.17.99.233	137.77	-	Estados Unidos
7	*	-	-	-
8	*	-	-	-
9	212.187.139.166	239.16	-	Gran Bretaña
10	146.97.33.2	238.03	-	Gran Bretaña
11	146.97.37.194	238.17	-	Gran Bretaña
12	193.63.108.94	245.87	-	Gran Bretaña
13	193.63.108.98	238.36	-	Gran Bretaña
14	193.63.109.90	248.00	-	Gran Bretaña
15	*	-	-	-
16	*	-	-	-
17	192.76.32.62	234.21	-	Oxford, Inglaterra, Gran Bretaña
18	129.67.242.154	241.62	-	Oxfordshire, Gran Bretaña

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

Una vez mandados los paquetes y realizados los promedios, procederemos a graficar los tiempos resultantes.



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 para False RTT.

- Entre 4 y 5. Asimétricos.
- Entre 9 y 10. Asimétrico.
- Entre 12 y 13. Asimétrico.
- Entre 14 y 17. Lo contamos porque 15 y 16 corresponden a hops perdidos. Es Asimétrico.

Por otro lado, tenemos los que no tuvieron respuesta. Esta anomalía es conocida como Missing Hops. Se produce en general cuando un router está protegido por un firewall o de configurado otro modo para no generar errores excesivos ICMP TTL. En nuestro caso tenemos 7, 8, 15, 16.

El hops 6 pertenece a Estados Unidos pero el 9 pertenece a Gran Bretaña. Pensamos que a la hora de establecer el enlace continental se lo hizo primero con dos hops que nunca darán respuestaNetherland-sambién se pierden hops entre una IP de Estados Unidos y la de Gran Bretaña. Como hipótesis alternativa podríamos pensar que esto ocurre por culpa del enlace continental.

En el caso de 15 y 16 ocurre algo parecido, puesto que 14 pertenece a Gran Bretaña(sin ubicar region ni ciudad) mientras que 17 pertenece a Oxford. En este caso es más probable que se trate de un caso aislado ya que no existe un salto continental, solamente regional.

Además tenemos identificado un posible salto continental en 208.178.195.213 - 67.17.99.233. Sin embargo esto es incorrecto ya que ambas IP pertenecen al dominio de Estados Unidos(Aunque la primera no puede estar ubicada en ese lugar por razones que explicaremos más adelante). El salto continental se produce entre 6 y 9, aunque si vemos el gráfico de RRTs podemos apreciar que la diferencia no es muy grande.

También podemos observar la anomalía de False Link en los hops 4 y 5 ya que muestran como ubicación a Estados Unidos , sin embargo los RTT de ambos no corresponden con la distancia que tuvieron que recorrer entre 3 y 4. El número 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 hops 6 también sufra de esta anomalía ya que usando herramientas alternativas de geolocalización de IP nos dio de resultado Netherlands. Aunque creemos que es poco probable porque el RTT que existe entre Londres y este sería demasiado grande.

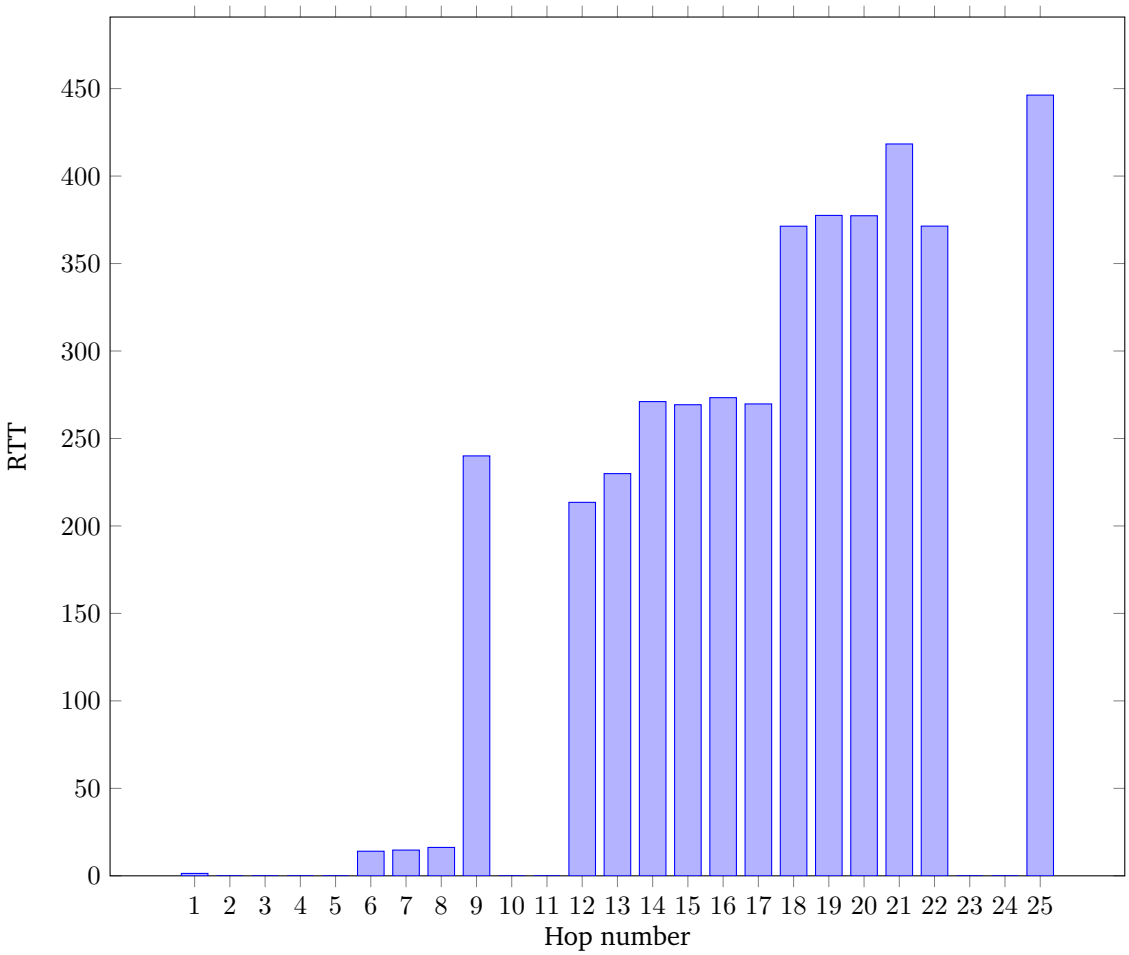
2.2. Universidad de Syndney

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

Hop #	**IP**	**RTT (ms)**	**Δ RTT**	**Ubicacion (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	10.33	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	371.39	-46.96	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)

Graficamos los RTT en un histograma para lograr una mayor claridad en los cambios en los tiempos entre los hops:



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. Por otro lado entre los hops 9-12 también encontramos una inconsistencia entre los valores de `RTT` de ambos hosts, independientemente de que no sean hosts consecutivos.
- *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 ($\Delta RTT = 223{,}81$) por abrumadora diferencia. Otro candidato es el enlace entre los hops 17-18 ($\Delta RTT = 101{,}59$). En menor medida podríamos especular con el enlace entre los hops 13-14 ($\Delta RTT = 41{,}17$) y el enlace entre los hops 20-21 ($\Delta RTT = 41{,}03$), sin embargo nos resulta inverosímil la existencia de 4 enlaces intercontinentales en la ruta de un paquete entre Argentina y Australia.

Contrastando nuestra hipótesis contra las ubicaciones arrojadas por la aplicación de geoubicación, 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, por lo cual estamos en presencia de un falso positivo. Este falso positivo es producto de la gran distancia entre ambos países. Por otro lado el enlace entre los hops 17-18 es un enlace entre Estados Unidos e Australia, lo que si representa un enlace intercontinental.

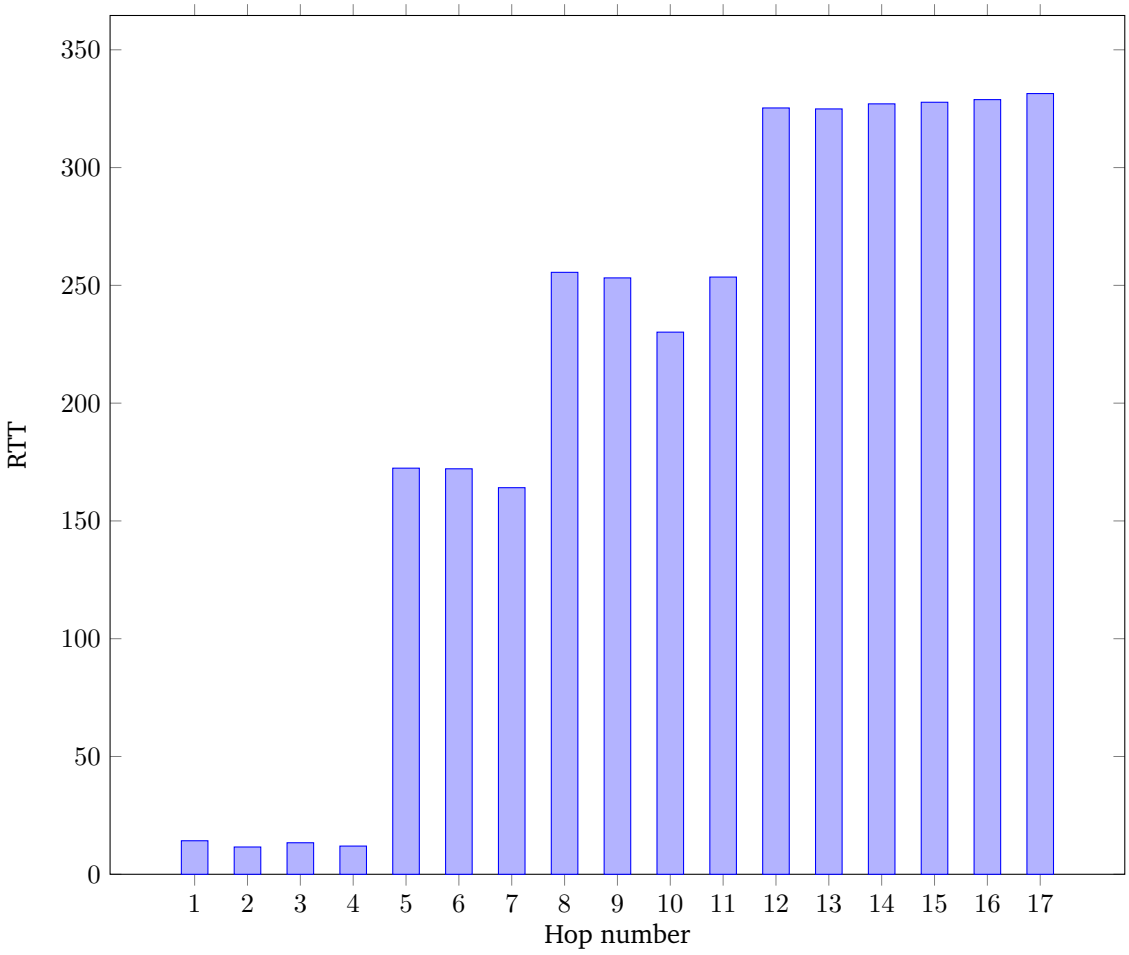
2.3. Universidad de Ghana

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

Hop #	IP	RTT (ms)	Δ RTT (%)	Ubicacion
1	10.27.64.1	14.23	-	Prov. Buenos Aires, Argentina
2	10.242.1.149	11.58	-	Prov. Buenos Aires, Argentina
3	195.22.220.33	13.38	-	Italia
4	195.22.220.32	11.97	-	Italia
5	195.22.206.92	172.40	-	Italia
6	195.22.206.92	172.13	-	Italia
7	216.6.87.202	164.11	-	Delaware, Estados Unidos
8	216.6.87.169	255.53	-	Delaware, Estados Unidos
9	216.6.57.1	253.17	-	Delaware, Estados Unidos
10	66.198.70.174	230.14	-	Delaware, Estados Unidos
11	80.231.76.121	253.52	-	Reino Unido, Europa
12	195.219.195.238	325.31	-	Reino Unido, Europa
13	41.21.232.70	324.90	-	Sudafrica
14	41.204.60.149	327.05	-	Ghana
15	41.204.60.150	327.73	-	Ghana
16	197.255.127.2	328.85	-	Ghana
17	197.255.125.10	331.42	-	Ghana

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

A continuación analizamos la anomalias encontradas:

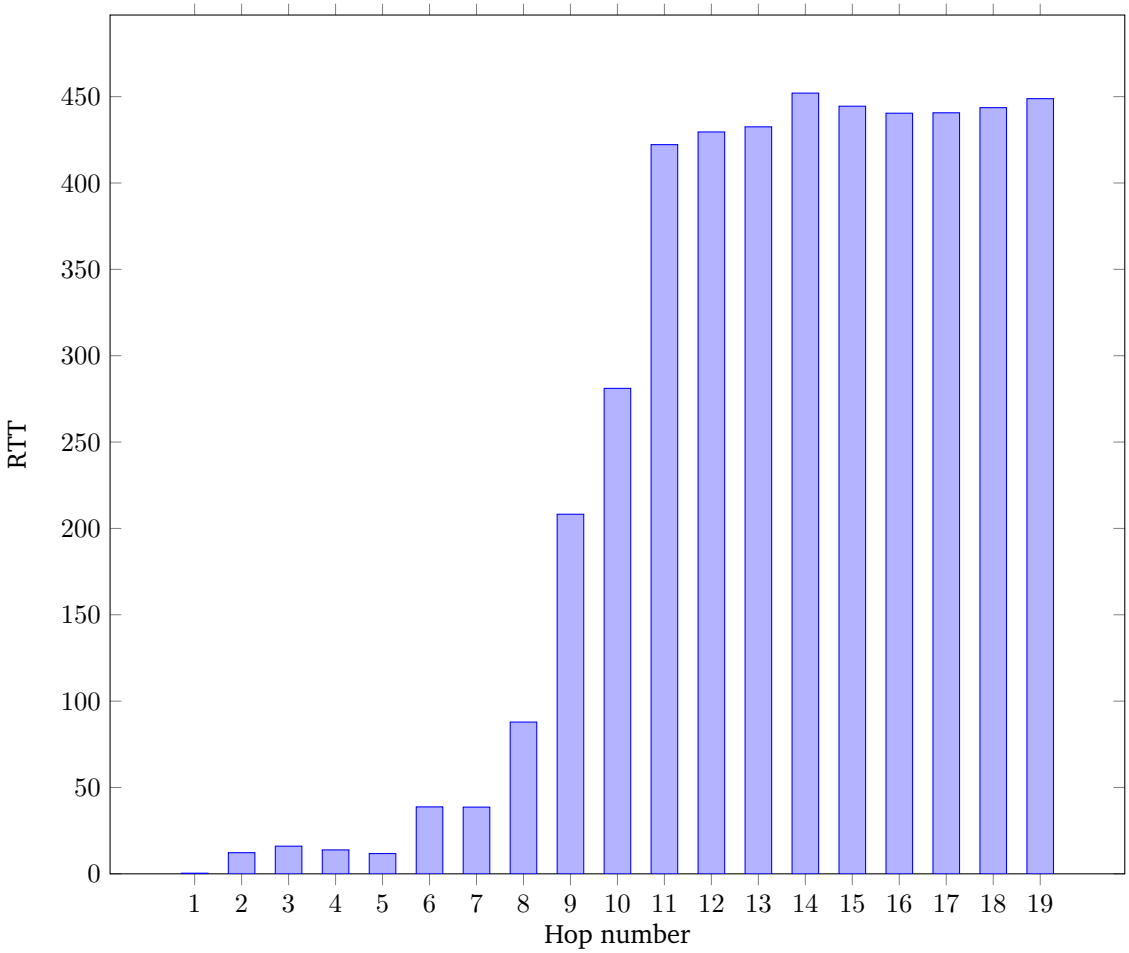


2.4. Universidad de Hong Kong de Ciencia y Tecnologia (HKUST)

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

Hop #	IP	RTT (ms)	Ubicacion
1	192.168.1.1	0.36	Local
2	200.3.60.192	12.24	Entre Ríos Province, AR
3	181.88.108.18	16.01	Entre Ríos Province, AR
4	190.225.252.166	13.85	Entre Ríos Province, AR
5	195.22.220.213	11.73	Italia
6	195.22.219.3	38.76	Italia
7	195.22.219.3	38.63	Italia
8	149.3.181.65	87.87	Italia
9	129.250.2.227	208.21	Colorado, US
10	129.250.4.13	281.09	Colorado, US
11	129.250.2.38	422.20	Colorado, US
12	129.250.5.134	429.55	Colorado, US
13	129.250.6.115	432.51	Colorado, US
14	203.131.246.154	452.04	Hong Kong
15	115.160.187.110	444.46	Hong Kong
16	202.130.98.102	440.41	Hong Kong
17	203.188.117.130	440.65	Hong Kong
18	202.14.80.153	443.62	Hong Kong
19	143.89.14.2	448.84	Hong Kong

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


RTT
0
50
100
150
200
250
300
350
400
450
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
Hop number

3. Conclusiones