

Universidad de Buenos Aires  
Facultad de  
Ciencias Exactas y Naturales  
Departamento de Computación

Teoría de las Comunicaciones

Primer Cuatrimestre de 2015

Trabajo práctico

Rutas en Internet

Fecha de entrega: 17 de Junio

Integrante	LU	Correo electrónico
De Sousa Bispo, Germán	358/12	german_nba11@hotmail.com
De Sousa Bispo, Mariano	389/08	marian_sabianaa@hotmail.com
Raffo, Diego	423/08	draffo@dc.uba.ar
Tilli, Leonardo	511/00	leotilli@gmail.com

[Introducción](#)

[Contexto Teórico](#)

[Paquetes ICMP](#)

[Tiempo de propagación y tiempo de encolamiento](#)

[RTT estimado, probabilidad de pérdida de paquete, y throughput](#)

[Caracterizando rutas](#)

[Implementación](#)

[Modo de uso](#)

[Decisiones de diseño](#)

[Gráficos y análisis](#)

[Universidad de Auckland](#)

[Universidad de Cambridge](#)

[Universidad de Peking](#)

[Universidad de Rhodes](#)

[Universidad de Simon Fraser](#)

[Curiosidad: Universidad de Pretoria](#)

[Contrastando con la realidad](#)

[Universidad de Auckland](#)

[Universidad de Cambridge](#)

[Universidad de Rhodes](#)

[Universidad de Simon Fraser](#)

[Conclusiones](#)

[Referencias](#)

# Introducción

En el presente trabajo se realizó un estudio sobre distintas rutas que siguen los paquetes IP desde su dirección natal hasta alcanzar su dirección de destino. En particular nos enfocamos en los paquetes ICMP, y en los saltos que éstos realizan a través de los nodos de la red, para llegar y retornar de sitios públicos conocidos. Parte del trabajo consistió en implementar una herramienta propia de traceroute, para poder capturar información sobre estas rutas.

Dentro del marco teórico sobre el comportamiento de internet, se analizaron los resultados contrastando mediciones y geolocalizaciones.

## Contexto Teórico

### Paquetes ICMP

Los paquetes de tipo ICMP (*Internet Control Message Protocol*) son parte del protocolo IP, el cual no es considerado completamente confiable. Si bien los mensajes ICMP no atacan este punto de manera directa, nos proveen información acerca de los problemas que ocurren.

La siguiente tabla<sup>1</sup> muestra los tipos de mensajes ICMP; utilizamos en este trabajo únicamente los tipos 0, 3 y 8.

Numeric Type	Symbolic Name	Description
0	echo-reply	A ping response.
3	destination-unreachable	A general error status message; the destination host is unable to deliver the packet to the destination port or a router along the path to the destination is unable to deliver the packet to the next destination; used by traceroute.
4	source-quench	IP network layer flow control between two routers, or between a router and a host. The destination, or an intermediate router, uses the message to tell the sender that messages are being received faster than can be processed.
5	redirect	A routing message returned to the sender when a router determines that a shorter path exists.
8	echo-request	A ping request.
11	time-exceeded	An error message returned when a packet's maximum hop count (TTL) is exceeded and a router has discarded the packet in transit; used by traceroute.
12	parameter-problem	Unexpected values are found in the IP packet header.

---

<sup>1</sup> <http://www.informit.com/articles/article.aspx?p=26121&seqNum=6>

## Tiempo de propagación y tiempo de encolamiento

Llamamos RTT al tiempo que tarda un paquete en llegar a destino y volver al origen. Definimos al RTT como la sumatoria del tiempo que cada router, que recibe y redirige el paquete, necesita para encolar el paquete en el enlace sumado al tiempo que tarda un bit en llegar al siguiente router. A esto se le suma el mismo tiempo que el paquete tarda en volver del destino al origen.

Llamamos  $ZRTT_i$  al valor normalizado del RTT correspondiente al  $i$ -ésimo router en cierta ruta, y se calcula de la siguiente manera:

$$ZRTT_i = \frac{RTT_i * \overline{RTT}}{SRTT}$$

Donde  $\overline{RTT}$  representa la esperanza

$$\overline{RTT} = \frac{1}{n} \sum_{i=1}^n RTT_i$$

Y  $SRTT$  al desvío estándar

$$SRTT = \sqrt{\frac{1}{n} \sum_{i=1}^n (RTT_i - \overline{RTT})^2}$$

Este valor es muy útil para poder comparar si el RTT de algún router es mayor o menor a la media, ya que la media estaría en el cero.

## RTT estimado, probabilidad de pérdida de paquete, y throughput

Al enviar un mensaje de manera reiterada al mismo destino, podemos calcular el valor estimado de RTT utilizando la siguiente fórmula de manera iterativa:

$$EstimatedRTT = \alpha * EstimatedRTT + (1 - \alpha) * SampleRTT$$

donde  $\alpha$  puede variar durante la experimentación.

También podemos estimar la probabilidad de pérdida de paquete, mediante la siguiente fórmula

$$EstimatedPacketLossProbability = 1 - \frac{\#Echo\ reply}{\#Echo\ request}$$

dando lugar al cálculo de throughput, de acuerdo a la ecuación de Mathis

## Caracterizando rutas

La forma de comunicarse de una punta del mundo a otra descansa sobre una estructura jerárquica de nodos que redirigen paquetes.

Utilizando el comando *tracert* podemos ver los saltos entre *routers* que realiza el paquete entre la dirección origen y destino, como se muestra en el siguiente ejemplo.

```
C:\WINDOWS\system32>tracert www.facebook.com

Trazo a la dirección star.c10r.facebook.com [31.13.73.11]
sobre un máximo de 30 saltos:

  1  121 ms    3 ms    13 ms    192.168.1.1
  2  131 ms    49 ms    22 ms    1-118-167-181.fibertel.com.ar [181.167.118.11]
  3  *          *          *          Tiempo de espera agotado para esta solicitud.
  4  *          *          *          Tiempo de espera agotado para esta solicitud.
  5  *          *          *          Tiempo de espera agotado para esta solicitud.
  6  174 ms    351 ms    18 ms    9-164-89-200.fibertel.com.ar [200.89.164.91]
  7  67 ms     112 ms    21 ms    6-165-89-200.fibertel.com.ar [200.89.165.61]
  8  84 ms     21 ms     58 ms    150-165-89-200.fibertel.com.ar [200.89.165.150]

  9  21 ms     17 ms     17 ms    195.22.220.56
 10 150 ms    202 ms    147 ms    xe-3-0-1.miami15.mia.seabone.net [195.22.199.131]
 11 216 ms    196 ms    192 ms    xe-1-3-0.miami15.mia.seabone.net [195.22.199.111]
 12 160 ms    158 ms    170 ms    facebook.miami15.mia.seabone.net [89.221.41.151]
 13 *          *          *          Tiempo de espera agotado para esta solicitud.
 14 *          *          *          Tiempo de espera agotado para esta solicitud.
 15 147 ms    139 ms    227 ms    edge-star-shv-01-mia1.facebook.com [31.13.73.11]

Trazo completa.
```

Se puede ver cómo el paquete va pasando por distintos servidores hasta llegar a destino, que se muestran como una dirección IP junto a su respectivo nombre de dominio. Existen *routers* que descartan los paquetes ICMP, por lo tanto, ciertos nodos de la ruta, no podrán ser conocidos por nosotros.

# Implementación

Para la primera parte del presente trabajo práctico, se hizo una herramienta que permite hacer un *traceroute*. La herramienta va reenviando un paquete ICMP de tipo 8 a la dirección destino determinada, con TTLs crecientes. De manera incremental, los nodos intermedios van descartando el mensaje debido a que expira, y envían una respuesta ICMP de tipo 3. Finalmente, se envía el mensaje con un TTL suficientemente grande como para que llegue a destino, obteniendo una respuesta ICMP tipo 0, lo que permite reconstruir la ruta entera. Además de las IP de cada nodo de la ruta, se calculan los RTT de cada nodo, el ZRTT previamente mencionado, y el nombre de la red en donde se encuentra dicha IP.

Para la segunda, se hizo una herramienta que permite hacer *ping*; ésta envía paquetes ICMP a la dirección destino (cada una de las universidades analizadas). Por parámetro, se define un rango de *alphas* y un rango de cantidades máxima de pings con las que se realizará el análisis empírico. Por cada una de estas combinaciones, se genera una estadística. El programa al finalizar, imprime la colección de estadísticas con la siguiente información: IP, *alpha*, # total de paquetes enviados, # de paquetes no respondidos, # de paquetes respondidos, probabilidad de pérdida de paquetes, ERTT, tiempo promedio de *ping*, *throughput*. Veremos más adelante, que los tiempos fluctúan considerablemente entre distintas corridas. Por lo tanto, y para tener datos más confiables, todas las combinaciones de estadísticas se realizan sobre la misma ejecución de la tool *ping*. Queda claro que cada estadística analizará sólo la información contenida en su rango de *pings* a procesar.

Ambas herramientas, utilizan la librería de Python *scapy.py*

## Modo de uso

- **trace\_route.py:** python trace\_route.py [ip] [time to live] [times repeat]
  - **ip:** dirección de destino.
  - **time to live:** TTL máximo.
  - **times repeat:** # de paquetes que se envían con igual TTL.
- **ping.py:** python ping.py [ip] [alpha\_pace] [count\_pace] [timeout]
  - **ip:** dirección de destino.
  - **alpha\_pace:** define el paso del rango para *alpha*, entre [0,1] (i.e.: Un *alpha\_pace* de 0.25 generará los siguientes *alphas*: 0.00, 0.25, 0.50, 0.75, 1.00).
  - **count\_pace:** define el paso del rango para las cantidades máximas, entre [10, 150]
  - **time\_out:** tiempo máximo en segundos para esperar la respuesta del ping.

## Decisiones de diseño

A la hora de implementar el traceador de rutas, se tomaron las siguientes decisiones:

- **La hora de salida del mensaje y la hora de llegada se piden directamente a los mensajes IP.** De esta forma tratamos de evitar errores sujetos a la PC que ejecutaba el programa.

- Se decidió utilizar como mensaje de salida el de ICMP tipo 8, echo request, por su facilidad de implementación y por su amplia adopción.

## Gráficos y análisis

Para esta sección se escogieron 4 universidades en distintos puntos del planeta:

- University of Auckland, Auckland, Nueva Zelanda - [\*\*www.auckland.ac.nz/\*\*](http://www.auckland.ac.nz/).
- University of Cambridge, Cambridge, Inglaterra - [\*\*www.cam.ac.uk\*\*](http://www.cam.ac.uk).
- Peking University, Beijing, China - [\*\*www.pku.edu.cn\*\*](http://www.pku.edu.cn).
- Rhodes University, Grahamstown, Sudáfrica - [\*\*www.ru.ac.za\*\*](http://www.ru.ac.za).

Además se escogió una universidad dentro del continente, donde no hubiera necesidad de un enlace interoceánico, y así poder comparar los tiempos de propagación y los ZRTT obtenidos en cada caso. La universidad propuesta es: Simon Fraser University, Burnaby, Canada - [\*\*www.sfu.ca\*\*](http://www.sfu.ca)

Para cada una de las universidades propuestas, se realizó un rastreo de la ruta de paquetes ICMP de tipo ping-echo, realizando mapas de dichas rutas. Vale aclarar, los valores obtenidos de cada rastreo son valores promedio, ya que se enviaron múltiples paquetes a cada destino para minimizar el impacto de algún resultado inusual.

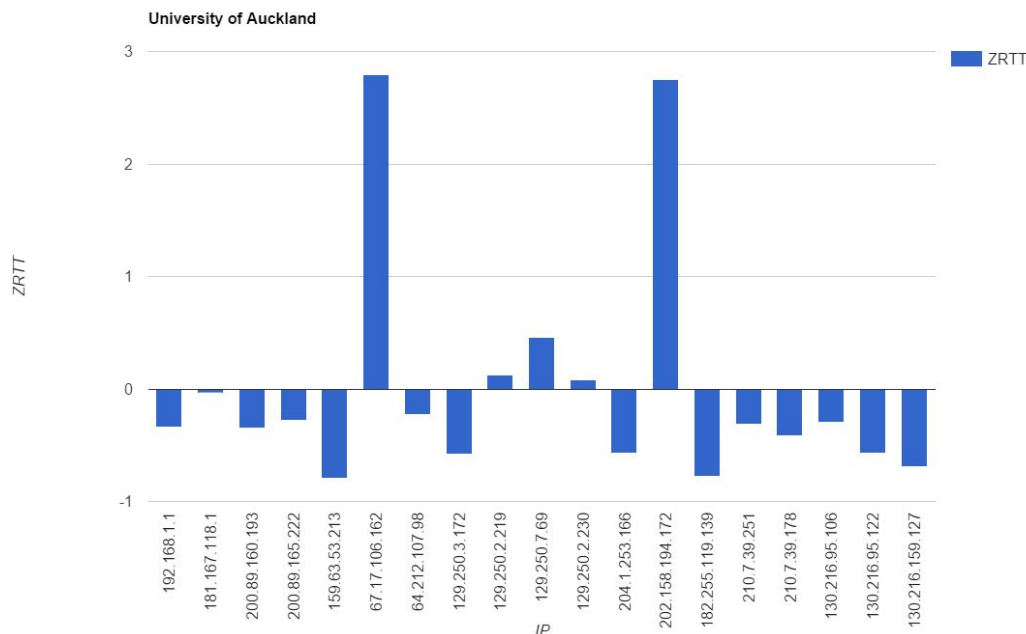
Las rutas se rastrearon utilizando el programa descrito en la sección *Implementación*, la cual nos proporcionó información muy similar a la que nos devuelve *tracert*.

Los puntos en los mapas se encontraron utilizando las herramientas de geolocalización que se encuentran en la sección de *Referencias*, a partir de las IP que se listaron en cada ruta encontrada.

Todas las mediciones se realizaron con PC's con Fibertel como proveedor de internet, con lo que las rutas encontradas no necesariamente son únicas, ya que esto depende de los enlaces que cada proveedor contrate.

## Universidad de Auckland

Primero se analizará la relación IP - ZRTT, explicado previamente en la sección “*Tiempo de propagación y tiempo de encolamiento*”. En el siguiente gráfico se representará esta relación. A partir del mismo, se realizarán hipótesis acerca de los posibles enlaces subacuáticos existentes en la ruta.



Recordando que el ZRTT se relaciona con el RTT promedio, podemos observar como la IP 67.17.106.162 y la IP 202.158.194.172 poseen un valor de ZRTT significativamente mayor que el del resto de las direcciones. Esto implica que el valor promedio de cada RTT de estas dos IP está por encima de los demás. Esto nos da a entender que la distancia que recorrió un paquete desde el router precedente al de la dirección es mucho mayor que la distancia promedio, por lo que podemos inferir que para llegar a ambas direcciones se tuvieron que recorrer largas distancias.

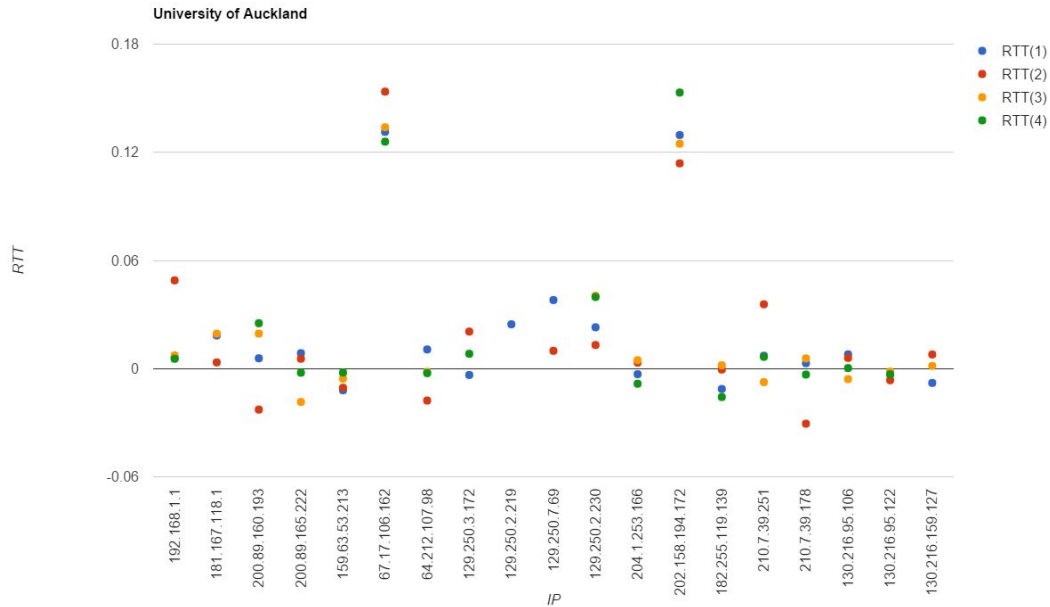
Una segunda posible explicación para un ZRTT alto, es que el tiempo de encolamiento del ICMP en el *router* sea alto. Esto podría suceder si se encuentra congestionado, y por lo tanto, le da poca prioridad a los mensajes de control.

La mayoría de las IP están por debajo de la media se aprecian con valores negativos. Esto nos muestra que los picos de ZRTT son muy significativos, llevando la media a estar por encima de la mayoría.

Sería pertinente preguntarnos si estos datos son representativos, y si no sería posible que la congestión de un *router* en un momento determinado nos esté dando falsos positivos a



la hora de buscar picos de ZRTT. Para responder a esta pregunta realizamos cuatro corridas idénticas de la misma ruta, y graficamos los distintos RTT para cada router dentro de la misma.



Como primera observación, vemos que las tendencias se respetan en ambos graficos. Los picos de ZRTT se corresponden con los RTT más grandes. También podemos apreciar que no todas la direcciones IP tienen valores para todos los intentos, es decir, no toda IP tiene puntos de todos colores. Esto es debe a que en algunas corridas, algunos routers rechazaron los paquetes ICMP u obtuvimos time-out y en otras no.

Como siguiente observación, podemos ver que aún efectuando experimentos idénticos, el promedio varía para cada *router* en distinta medida.

No obtuvimos rutas alternativas luego de haber efectuado varias corridas. No tuvimos casos donde para un mismo TTL obtengamos dos direcciones IP distintas.

Veamos ahora el mapa con las ubicaciones geográficas de los nodos obtenidos en el *traceroute* de la Universidad de Auckland y tratemos de mapear las direcciones IP a los saltos en el mundo.

Tener en cuenta que las rutas son marcadas con líneas rojas en los mapas y comienzan desde Buenos Aires, Argentina, lugar desde donde se realizó el traceroute. Los puntos negros corresponden a las ciudades que fueron distinguidas por las herramientas de geolocalización ya mencionadas.



Como se puede visualizar en el mapa, las mayores distancias por tramo entre ciudad y ciudad se pueden ver entre Argentina y Estados Unidos, y entre Estados Unidos y Australia, a través del océano pacífico. También podemos observar un enlace subacuático entre Australia y Nueva Zelanda, aunque la longitud del mismo no sea tan extensa como la de llegada a Oceanía.

Veamos a partir de los datos obtenidos de la experimentación qué relación se puede realizar entre los mayores ZRTT mostrados en el gráfico de barras y la visualización del camino en el mapa.

TTL	IP	Locación	Router	Empresa
1	192.168.1.1	Buenos Aires, ARG	-	-
2	181.167.118.1	Buenos Aires, ARG	1-118-167-181.fibertel.com.ar	Cablevision SA
3	Desconocido	-	-	-
4	Desconocido	-	-	-
5	Desconocido	-	-	-

6	200.89.160.193	Buenos Aires, ARG	193-160-89-200.fibertel.com.ar	Cablevision SA
7	200.89.165.222	Buenos Aires, ARG	222-165-89-200.fibertel.com.ar	Cablevision SA
8	159.63.53.213	EEUU	xe-7-1-2.ar3.eze1.gblx.net	Global Crossing
9	67.17.106.162	Broomfield, CO, EEUU	po2-30G.ar2.MIA2.gblx.net	Global Crossing
10	64.212.107.98	GreenBelt , Maryland, EEUU	185.PRSN - upto 20	-
11	129.250.3.172	Englewood, CO, EEUU	ae-4.r21.miamf02.us.bb.gin.ntt.net	Verio Inc.
12	129.250.2.219	Englewood, CO, EEUU	ae-10.r20.dllstx09.us.bb.gin.ntt.net	Verio Inc.
13	129.250.7.69	Englewood, CO, EEUU	ae-3.r20.lsanca03.us.bb.gin.ntt.net	Verio Inc.
14	129.250.2.230	Englewood, CO, EEUU	ae-1.r05.lsanca03.us.bb.gin.ntt.net	Verio Inc.
15	204.1.253.166	LA, California, EEUU	xe-0-0-0-16.r05.lsanca03.us.ce.gin.ntt.net	Levinson and Hill DSL Dallas
16	202.158.194.172	Sidney, New South Wales, AUS	xe-0-0-3.pe1.tkpa.akl.aarnet.net.au	Australian Academic and Research Network
17	182.255.119.139	Sidney, New South Wales, AUS	et-1-0-0-201.and12-nsh.reannz.co.nz	Australian Academic and Research Network
18	210.7.39.251	Wellington, NZ	-	Research and Educationa Advanced Network New Zealand (REANNZ)
19	210.7.39.178	Wellington, NZ	-	Research and Educationa Advanced Network New Zealand (REANNZ)
20	130.216.95.106	Auckland, NZ	br-cpf1-north.net.auckland.ac.nz	imported inetnum object for AUCKLA
21	130.216.95.122	Auckland, NZ	cxj-alfa-430.net.auckland.ac.nz	imported inetnum object for AUCKLA
22	Desconocido	-	-	-
23	130.216.159.127	Auckland, NZ	www.auckland.ac.nz	imported inetnum object for AUCKLA

De la tabla sabemos que la IP 67.17.106.162 se encuentra en Broomfield, Colorado, Estados Unidos, y se encuentra visualizada en el mapa con conexión directa a Buenos Aires (dado que no se encontró la localización geográfica exacta de la IP anterior). Como solo sabemos que el paquete le llegó de algún lugar de Estados Unidos desde el nodo con IP 159.63.53.213, no podemos saber a priori si la distancia entre ese nodo y el ubicado en Broomfield, Colorado es significativa o no. Sin embargo, el ZRTT para la IP 159.63.53.213, desde donde se llega a Estados Unidos desde Argentina, es -0.79072. Esto indica que el enlace entre ambos países está por debajo del RTT promedio. Esto anula la hipótesis que obtuvimos a partir del mapa: la conexión entre Argentina y Estados Unidos no indica un valor

alto de ZRTT debido a la larga distancia entre nodos. La IP 159.63.53.213 no tiene siquiera un ZRTT positivo y es el nodo de acceso a Estados Unidos desde Argentina.

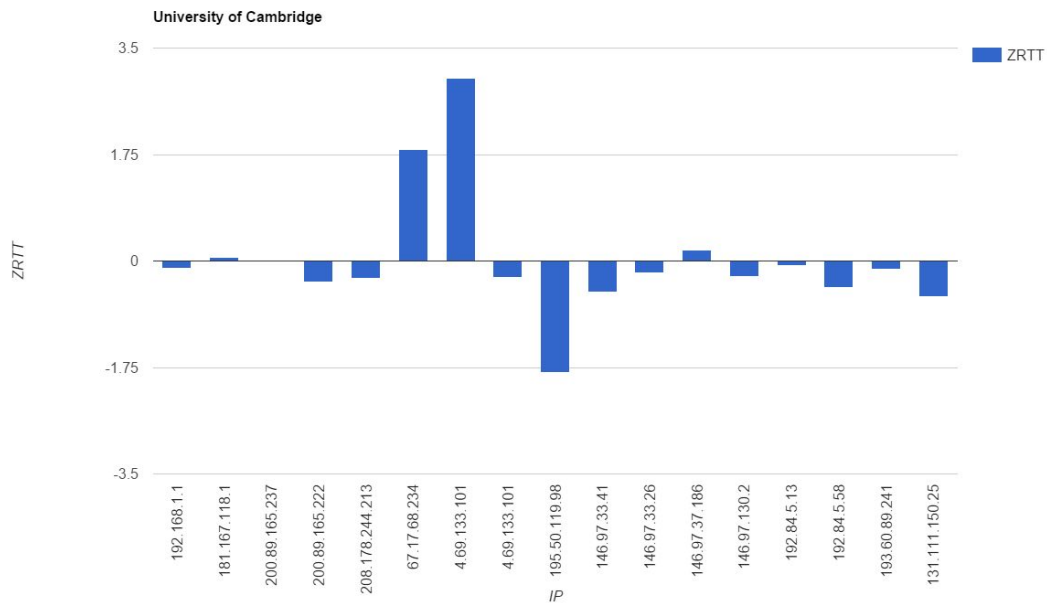
Podemos ver que la IP 67.17.106.162 tiene un ZRTT muy alto, pero no se corresponde con ningún salto interoceánico, con lo que asumimos que el retraso se debe al encolamiento del paquete ICMP. Posteriormente se verá un análisis un poco más profundo sobre la situación particular de la ciudad de Broomfield, Colorado para la empresa Global Crossing.

Por otro lado, la IP 202.158.194.172 se corresponde en la tabla con Sidney, New South Wales, Australia. Se llegó a la misma enviando un ping con TTL 16. Como podemos observar en la tabla, el antecesor inmediato corresponde con la IP 204.1.253.166 que proviene de Los Ángeles, California, Estados Unidos. Efectivamente, este enlace se puede visualizar en el mapa como la conexión transoceánica entre América y Oceanía. En este caso, la hipótesis acerca de un mayor ZRTT debido a una larga distancia entre nodos se ve validada.

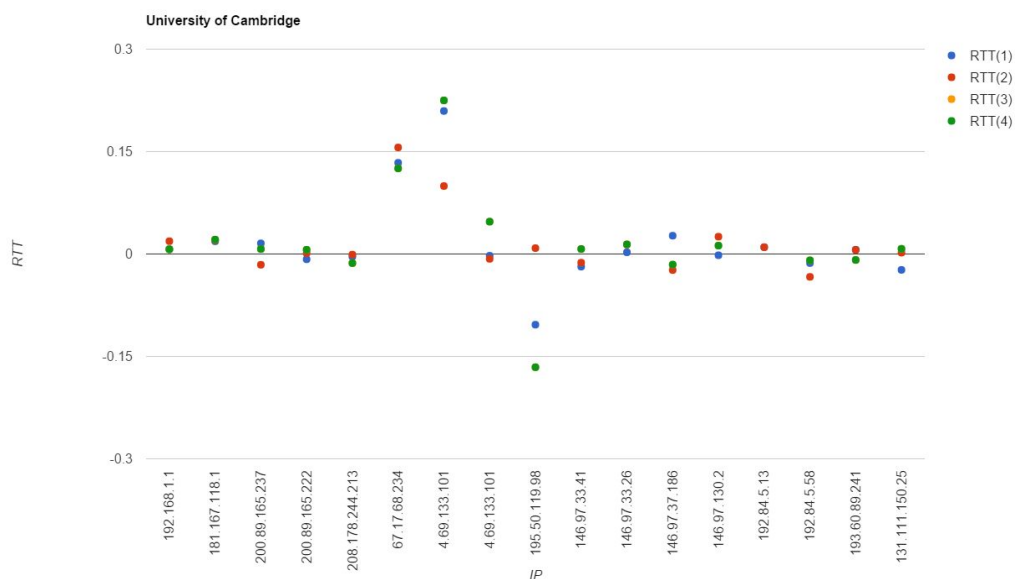
Por último, debido a que suponemos que existe un enlace subacuático entre Australia y Nueva Zelanda, también nos encontramos con un ZRTT negativo que indica que, a pesar de estar bajo agua y cubrir grandes distancias, el RTT de esta, está por debajo del RTT promedio.

## Universidad de Cambridge

A continuación, se realizará el mismo análisis para la Universidad de Cambridge.



Podemos observar que inmediatamente se distinguen dos IP en cuanto a su valor de ZRTT. Las IP 67.17.68.234 y 4.69.133.101, parecen indicarnos potenciales saltos de larga longitud, o tiempos de encolamiento muy altos.



Luego de efectuar cuatro corridas a la ruta, podemos ver que las tendencias se mantienen.

Podemos destacar los RTT obtenidos para las IP 4.69.133.101 y 195.50.119.98, que tuvieron una amplitud visiblemente mayor a la del resto de las IP. Con el análisis hecho hasta este punto, vamos a suponer a la primera IP mencionada como un salto intercontinental. Veremos con los siguientes gráficos si efectivamente el salto se hace en este *router*. La segunda IP fluctúa en tiempo de respuesta. A priori, parece difícil prever su comportamiento, lo que nos lleva a teorizar que quizás mucha información atraviesa esta punto.



A partir del mapa, podemos ver que la conexión entre Estados Unidos y Gran Bretaña hay un cable submarino de gran longitud. Pareciera que entre América del sur y América del norte también hay un gran salto. Al analizar el mapa con todos los *backbones*<sup>2</sup> existentes, se ve que no existe un cable que una directamente Buenos Aires con Estados Unidos. Por otro lado, el bajo RTT de este salto nos hace pensar que no puede ser satelital. La explicación de este RTT bajo y que no aparezcan saltos en el medio, es que si existen nodos intermedios, no son de nivel 3. Para IP es completamente transparente lo que sucede en el medio, donde puede haber repetidoras, switches de nivel dos, o el hardware necesario para que se realice el enlace entre ambos routers de nivel tres.

TTL	IP	Locación	Router	Empresa
1	192.168.1.1	Buenos Aires, Argentina	-	-
2	181.167.118.1	Buenos Aires, Argentina	1-118-167-181.fibertel.com.ar	Cablevision SA
3	Desconocido	-	-	-

<sup>2</sup> <http://www.submarinecablemap.com/>

4	Desconocido	-	-	-
5	Desconocido	-	-	-
6	200.89.165.237	Buenos Aires, Argentina	237-165-89-200.fibertel.com.ar	Cablevision SA
7	200.89.165.222	Buenos Aires, Argentina	222-165-89-200.fibertel.com.ar	Cablevision SA
8	208.178.244.213	Ventura, California, EEUU	xe-1-2-2.ar3.eze1.gblx.net	Global Crossing
9	67.17.68.234	Broomfield, CO, EEUU	po2.ar3.MIA2.gblx.net	Global Crossing
10	Desconocido	-	-	-
11	4.69.133.101	EEUU	ae-4-4.car1.Manchester.uk1.Level3.net	Level 3 Communications Inc.
12	4.69.133.101	EEUU	ae-4-4.car1.Manchester.uk1.Level3.net	Level 3 Communications Inc.
13	195.50.119.98	Manchester, England	-	Level 3 Communications
14	146.97.33.41	London, England	ae29.erdiss-sbr1.ja.net	UK Academic Joint Network Team (NET-JANET-IP)
15	146.97.33.26	London, England	ae30.lowdss-sbr1.ja.net	UK Academic Joint Network Team (NET-JANET-IP)
16	146.97.37.186	London, England	ae0.camb-rbr2.ja.net	UK Academic Joint Network Team (NET-JANET-IP)
17	146.97.130.2	Cambridge CambridgeShire England	University-of-Cambridge.Camb-rbr1.eastern.ja.net	UK Academic Joint Network Team (NET-JANET-IP)
18	192.84.5.13	Cambridge CambridgeShire England	route-enetc.route-cent.net.cam.ac.uk	Medical Research Council
19	192.84.5.58	Cambridge CambridgeShire England	route-cent.route-nwest.net.cam.ac.uk	Medical Research Council
20	193.60.89.241	Cambridge CambridgeShire England	mint.admin.cam.ac.uk	Cambridge University UK
21	131.111.150.25	Cambridge CambridgeShire England	primary.admin.cam.ac.uk	Cambridge University local area network

Si analizamos las IP 67.17.68.234 y 4.69.133.101, podemos observar que ambas se encuentran en Estados Unidos. La primera en Broomfield, Colorado perteneciente a Global Crossing mientras que la segunda a algún lugar incierto del país. Sabemos que la empresa dueña del segundo host es Level 3 Communications Inc<sup>3</sup>, que tiene su casa central en

<sup>3</sup> [https://en.wikipedia.org/wiki/Level\\_3\\_Communications](https://en.wikipedia.org/wiki/Level_3_Communications)

Broomfield, Colorado, por lo que notamos un buen solapamiento en las direcciones (a pesar que haya una dirección con locación no encontrada en el medio de ambas, posiblemente de algún router interno en el traspaso de ambas compañías). Además, Global Crossing fue adquirida por Level 3 Communications Inc en el 2011<sup>4</sup>, por lo que es viable que exista una conexión entre los cables de ambas empresas en esa ciudad. Podemos notar además, que no existe un salto interoceánico entre ambas direcciones, y las distancias entre ambos no deben ser tan extensas ya que se encuentran en el mismo país. De esta forma, podemos deducir que el alto valor de ZRTT se corresponde con grandes tiempos de encolamiento, posiblemente por atravesar un punto neurálgico en Level 3 Communications Inc. Como se mencionó previamente con la Universidad de Auckland, aquí se justifica el alto valor de ZRTT que se obtuvo para esta locación en el análisis de ambas universidades, y, en particular, para la misma red.

Por otro lado, notamos que el enlace transoceánico se corresponde con la IP 195.50.119.98. Ésta fue mencionada como una de las direcciones que tuvieron una amplitud visiblemente mayor a la del resto de las IP en la experimentación, por lo que habíamos deducido que mucha información atraviesa este punto. Como podemos ver, en el gráfico de los ZRTT, esta IP es la que menor valor obtuvo. Esto implica que el bajo valor del ZRTT se corresponde con el bajo tiempo de encolamiento ya que si el factor decisivo fuese el tiempo de transmisión, el valor del RTT debería ser de los más altos. Este bajo tiempo de encolamiento se lo atribuimos al gran ancho de banda que posiblemente posee un enlace que une estos dos continentes (grandes países con mucho tráfico de red), necesario para poder tener comunicaciones fluidas.

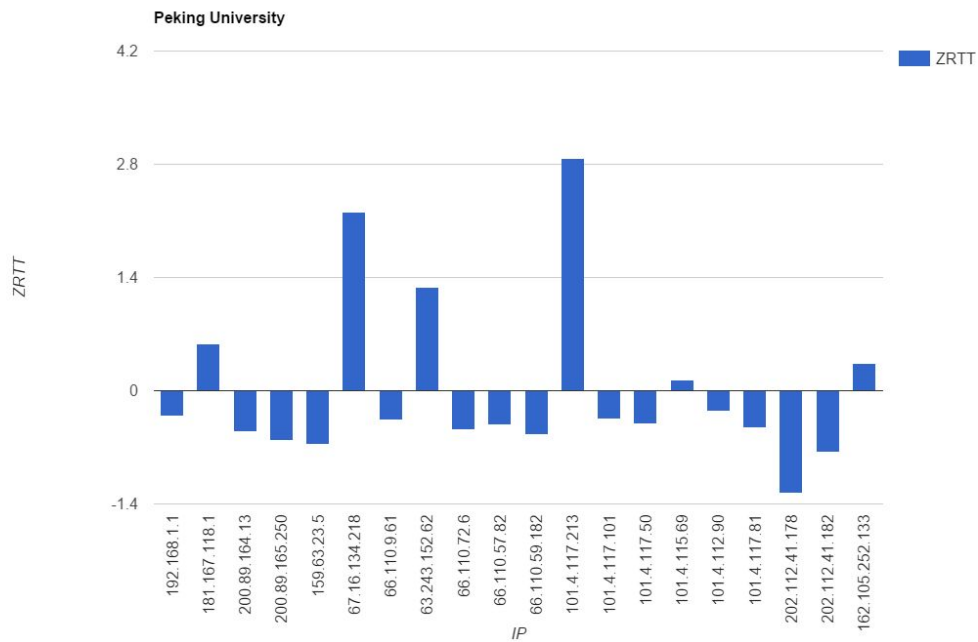
---

<sup>4</sup> [http://es.wikipedia.org/wiki/Global\\_Crossing](http://es.wikipedia.org/wiki/Global_Crossing)

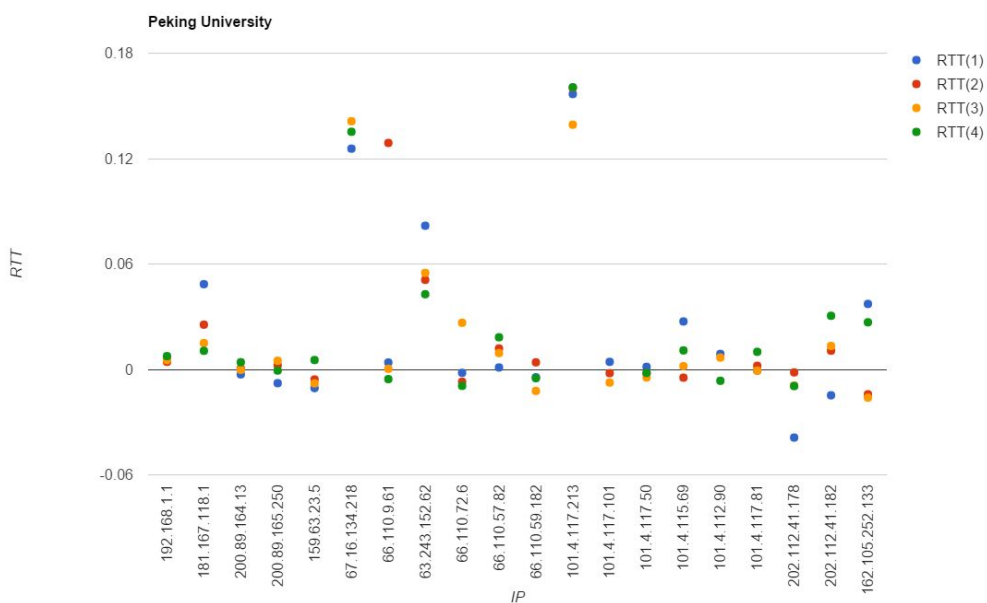


## Universidad de Peking

En este caso, analizaremos el traceroute a la Universidad de Peking, en Beijing, China.



En este caso las direcciones 67.16.134.218 y 101.4.117.101 sobresalen sobre los demás ZRTT. En menor medida, la IP 63.243.152.62 también posee un ZRTT que puede llegar a indicarnos algún comportamiento que valga la pena destacar.



Luego de analizar cuatro rastreos diferentes, podemos ver que los datos del ZRTT previamente calculados parecieran ser bastante representativos, no habiendo grandes fluctuaciones, con la excepción la IP 66.110.9.61 que posee un *outlier* significativo. El resto de las IP se corresponden directamente con el gráfico anterior. También podemos observar que no todas las corridas encontraron todas las IP, es decir, se observa que hay direcciones IP que no tienen un RTT de cada corrida.

Teniendo en cuenta esto, veamos como es el mapa del camino realizado por los paquetes hasta la universidad china.



Como se puede notar, existe una conexión transoceánica que se establece entre Estados Unidos y China. Como pudimos notar en la experimentación previa, la conexión entre Argentina y Estados Unidos no suele acarrear un ZRTT alto.

Además, podemos ver que el camino se mueve desde el oeste de Estados Unidos hacia el sureste de Canadá, para luego volver y cruzar el océano. Sin embargo, encontramos dos nodos en Canadá. Uno corresponde a la ciudad de Montreal y otro a Stoney Creek. La información obtenida indica que el paquete va hasta Montreal, pasa por Stoney Creek y vuelve a la ciudad de Montreal. La diferencia entre ambas ciudades es de aproximadamente 612km<sup>5</sup>. Dado que tratamos con herramientas de geolocalización a las que no tenemos acceso a su implementación, no podemos asegurar que los resultados obtenidos por las mismas sean libres de error. De esta manera, no podemos afirmar que el paquete efectivamente pase por Stoney Creek y vuelva a Montreal, o que simplemente pase por otro router en Montreal y que sea simplemente un error obtenido por la herramienta utilizada. Todas las direcciones fueron validadas con las cuatro herramientas utilizadas y se decidió utilizar la localización que parecía ser la acertada dada las respuestas de las mismas.

---

5

<https://www.google.com.ar/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=Distancia+entre+stoney+creek+y+montreal>

A su vez, sucede una situación similar con las direcciones en China. El paquete llega primeramente a Beijing, donde circula por varios routers hasta moverse a Shanghai. Luego, vuelve a Beijing donde finaliza en la Universidad de Peking.

Esto se visualizará en la siguiente tabla:

TTL	IP	Locación	Router	Empresa
1	192.168.1.1	Buenos Aires, ARG	-	-
2	181.167.118.1	Buenos Aires, ARG	1-118-167-181.fibertel.com.ar	Cablevision.SA
3	Desconocido	-	-	-
4	Desconocido	-	-	-
5	Desconocido	-	-	-
6	200.89.164.13	Buenos Aires, ARG	13-164-89-200.fibertel.com.ar	Cablevision.SA
7	200.89.165.250	Buenos Aires, ARG	250-165-89-200.fibertel.com.ar	Cablevision.SA
8	159.63.23.5	San Diego, California, EEUU	ge-0-1-2.ar3.eze1.gblx.net	Global Crossing
9	67.16.134.218	Manhattan, Illinois, EEUU	po4-20G.ar1.MIA2.gblx.	Global Crossing
10	66.110.9.61	Montreal, Quebec, CA	ix-2-3-1-0.tcore1.MLN-Miami.as6453.net	CGI Group
11	63.243.152.62	Stoney Creek, Ontario, CA	if-1-2.tcore2.MLN-Miami.as6453.net	Velcom
12	66.110.72.6	Montreal, Quebec, CA	if-3-2.tcore2.DT8-Dallas.as6453.net	Netnexus Inc
13	66.110.57.82	Montreal, Quebec, CA	if-8-2.tcore1.LVW-Los-Angeles.as6453.net	Wavex Fortis Network for Malaysia
14	66.110.59.182	LA, California, EEUU	-	Subic Telecommunications Co. Inc.
15	101.4.117.213	Beijing, China	-	Cernet Corporation NOC
16	101.4.117.101	Beijing, China	-	Cernet Corporation NOC
17	101.4.117.50	Beijing, China	-	Cernet Corporation NOC
18	101.4.115.69	Beijing, China	-	Cernet Corporation NOC
19	101.4.112.90	Beijing, China	-	Cernet Corporation NOC
20	101.4.117.81	Beijing, China	-	Cernet Corporation NOC
21	202.112.41.178	Shanghai, China	-	CERNET super computer center
22	202.112.41.182	Shanghai, China	-	CERNET super computer center
23	162.105.252.133	Beijing, China	-	China Education and Research Network Center

24	Desconocido		-	-
25	Desconocido		-	-
26	Desconocido		-	-

El ZRTT más alto corresponde con la IP 101.4.117.101, la cual es la primera dirección en China luego de saltar desde Los Ángeles, California. En este caso, el valor de ZRTT nos aporta información sobre el salto interoceánico.

Por otro lado, el segundo valor más alto de ZRTT corresponde a la dirección IP 67.16.134.218. Esta se ubica en Manhattan, Illinois. Sin embargo, esta no es la llegada desde Buenos Aires a Estados Unidos, sino el primer salto que se hace en el país norteamericano. De esta forma, y dado a la poca fluctuación del RTT en las varias pasadas del experimento, podemos inferir que el gran valor de ZRTT se corresponde con un mayor tiempo de encolamiento y no de transmisión.

Finalmente, vimos que la dirección 63.243.152.62 también tenía un valor alto, aunque en menor medida, de ZRTT. Analizando la tabla, podemos observar que esta dirección corresponde a Stoney Creek, Ontario, Canadá, la misma locación que no pudimos asegurar si era correcta o si se trataba de un error de las herramientas de geolocalización. La empresa dueña de esa dirección es *Velcom*. La misma es una empresa de *Web Hosting* cuya sede se encuentra en Brampton, Canadá, a 70kms de Stoney Creek.<sup>6 7</sup> Esto nos muestra que los datos son consistentes, y que es posible que la herramienta de geolocalización haya estado acertada y el paquete efectivamente pase por esta ciudad para luego volver a Montreal. Lo que observamos con esto es que hay un cambio de red (desde la empresa CGI Group a Velcom) donde hay posibilidad de encolamiento, lo que implicaría un aumento en el valor del ZRTT.

Es muy importante notar que la IP de destino nunca es alcanzada por nuestra herramienta. Sabemos que entramos en la red que la contiene (*China Education and Research Network Center*), pero la máquina destino no nos responde, posiblemente, por que está configurada para descartar los paquetes ICMP.

---

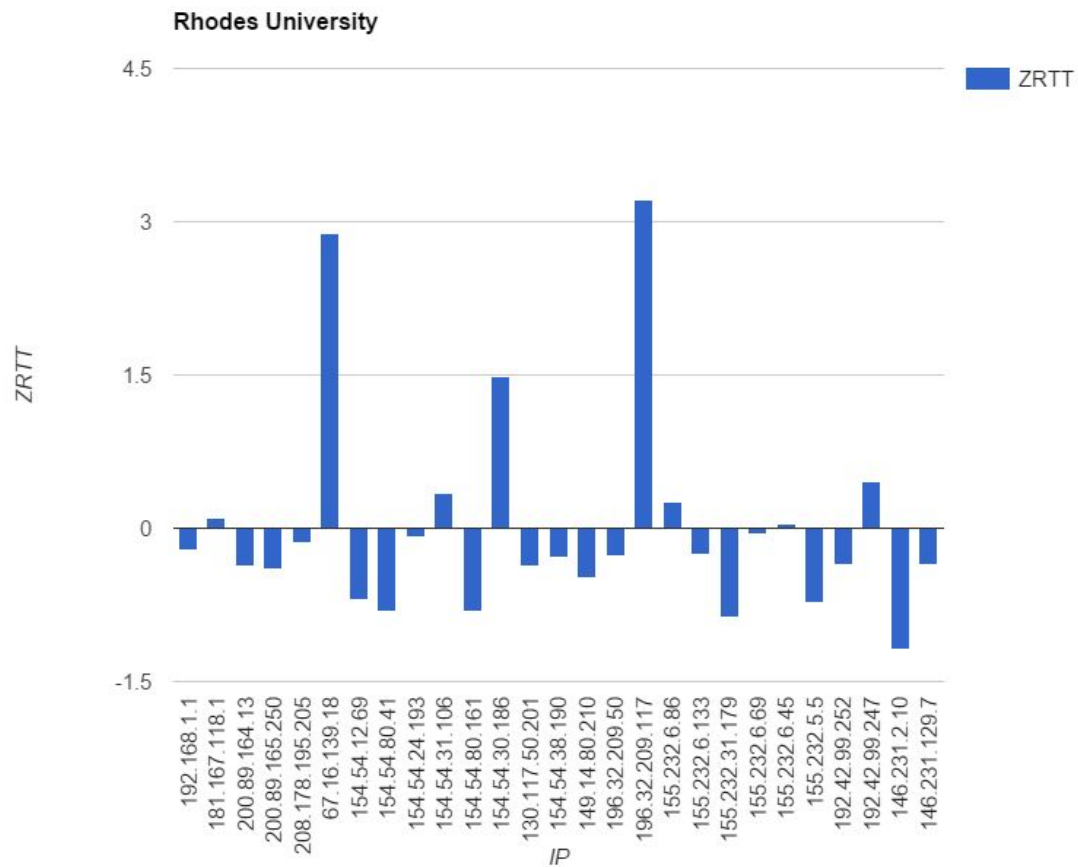
<sup>6</sup> <http://www.velcom.com/>

<sup>7</sup>

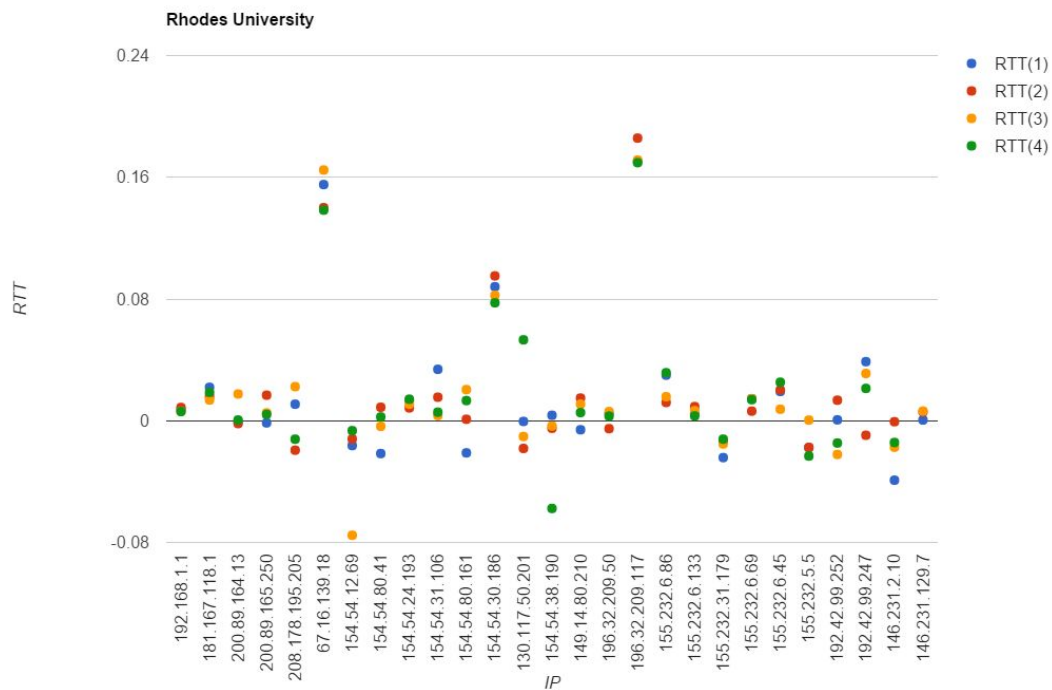
<https://www.google.com.ar/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=distancia%20brampton%20stoney%20creek>

## Universidad de Rhodes

A continuación se realizará el mismo análisis para la Universidad de Rhodes



El grafico que se presenta muestra dos claros valores de ZRTT que desprenden de la media, que son las IP 67.16.139.18 y 196.32.209.117, y un tercero en menor medida, cuyo IP es 154.54.30.186.



Como se apreció en los análisis previos, las tendencias se mantienen. En particular, en el caso de las direcciones que mayor ZRTT obtuvieron, podemos notar como los valores de RTT de las distintas corridas no fluctúan demasiado. Sin embargo, podemos encontrar valores cuya variación es mayor a lo que se encontró en los gráficos anteriores.



Como en los casos previos, el salto entre Buenos Aires y Estados Unidos no acarrea un gran costo en tiempo. Luego de algunas retransmisiones dentro de Estados Unidos, el paquete se envía a Ciudad del Cabo, Sudáfrica, desde donde se dirige a su IP destino. Al ver que solo hay un salto interoceánico que brindaría un alto valor de ZRTT, el enlace entre Estados Unidos y Sudáfrica, se refuerza la idea de que el tiempo de encolamiento aumenta los valores de ZRTT mientras que, en muchos casos, el tiempo de transmisión está sujeto al tráfico al que está expuesto el nodo y la tecnología del enlace.

TTL	IP	Locación	Router	Empresa
1	192.168.1.1	Buenos Aires, Argentina	-	-
2	181.167.118.1	Buenos Aires, Argentina	1-118-167-181.fibertel.com.ar	CableVision SA
3	Desconocido	-	-	-
4	Desconocido	-	-	-
5	Desconocido	-	-	-
6	200.89.164.13	Buenos Aires, Argentina	13-164-89-200.fibertel.com.ar	CableVision SA
7	200.89.165.250	Buenos Aires, Argentina	250-165-89-200.fibertel.com.ar	CableVision SA
8	208.178.195.205	Alexandria, Virginia, EEUU	ge-1-2-0.ar3.eze1.gblx.net	Global Crossing
9	67.16.139.18	Manhattan, Illinois, EEUU	po3-20G.ar2.MIA2.gblx.net	Global Crossing
10	154.54.12.69	Washington, Columbia, EEUU	te0-0-0-34.ccr21.mia03.atlas.cogentco.com	Performance Systems International
11	154.54.80.41	Washington, Columbia, EEUU	be2054.ccr21.mia01.atlas.cogentco.com	Performance Systems International
12	154.54.24.193	Washington, Columbia, EEUU	be2122.ccr41.atl01.atlas.cogentco.com	Performance Systems International
13	154.54.31.106	Washington, Columbia, EEUU	be2170.mpd21.dca01.atlas.cogentco.com	Performance Systems International
14	154.54.80.161	Washington, Columbia, EEUU	be2518.ccr41.jfk02.atlas.cogentco.com	Performance Systems International
15	154.54.30.186	Washington, Columbia, EEUU	be2317.ccr41.lon13.atlas.cogentco.com	Performance Systems International
16	130.117.50.201	Washington, Columbia, EEUU	be2163.ccr22.lon01.atlas.cogentco.com	Performance Systems International
17	154.54.38.190	Washington, Columbia, EEUU	be2426.rcr11.b015533-1.lon01.atlas.cogentco.com	Performance Systems International

18	149.14.80.210	Washington, Columbia, EEUU	-	Performance Systems International
19	196.32.209.50	Cape Town, Western Cape, South Africa	xe-0-0-0.ams1.nl.ubuntunet.net	Ubuntunet Alliance For Research And Education Networking
20	196.32.209.117	Cape Town, Western Cape, South Africa	te-1-4-2018-mtz1-pe1.ubuntunet.net	Ubuntunet Alliance For Research And Education Networking
21	155.232.6.86	Wynberg (Cape Town), Western Cape, South Africa	xe0-0-2-700-dur1-pe2-n.tenet.ac.za	Uninet
22	155.232.6.133	Wynberg (Cape Town), Western Cape, South Africa	te3-0-1-dur1-pe1-n.tenet.ac.za	Uninet
23	155.232.31.179	Wynberg (Cape Town), Western Cape, South Africa	xe0-0-0-dur1-pe3-n.tenet.ac.za	Uninet
24	155.232.6.69	Wynberg (Cape Town), Western Cape, South Africa	te-0-1-0-0-els1-pe2-r.tenet.ac.za	Uninet
25	155.232.6.45	Wynberg (Cape Town), Western Cape, South Africa	te2-0-0-plz1-pe1-n.tenet.ac.za	Uninet
26	155.232.5.5	Wynberg (Cape Town), Western Cape, South Africa	te0-0-0-0-grh1-pe1-n.tenet.ac.za	Uninet
27	192.42.99.252	Grahamstown, Eastern Cape, South Africa	strubenedge-tenet.net.ru.ac.za	Rhodes University Computing Centre
28	192.42.99.247	Grahamstown, Eastern Cape, South Africa	strubencore-strubenedge.net.ru.ac.za	Rhodes University Computing Centre
29	146.231.2.10	Grahamstown, Eastern Cape, South Africa	datacentres-1-strubencore.net.ru.ac.za	Rhodes University
30	146.231.129.7	Grahamstown, Eastern Cape, South Africa	www-real.ru.ac.za	Rhodes University

Nuevamente el paquete comienza su viaje en los servidores de Fibertel, y sale por el mismo IP que la ruta de Cambridge: 200.89.165.250.

La dirección 67.16.139.18 se corresponde con la ciudad de Manhattan, Illinois, bajo la empresa *Global Crossing*. Esto también se pudo visualizar en la Universidad de Peking y el valor de ZRTT fue atribuido a tiempo de encolamiento. Por la misma razón, podemos suponer lo mismo en este caso.

La IP 196.32.209.117 se encuentra en Ciudad del Cabo, Sudáfrica. La misma es el segundo nodo por el que pasa el paquete en África. En ésta se encuentra un ZRTT alto, posiblemente por congestión de datos o por una amplia diferencia en la velocidad del hardware utilizado entre el nexo intercontinental y la red dentro de África, dado que no hay una amplia distancia entre estos nodos (ambos en Ciudad del Cabo).

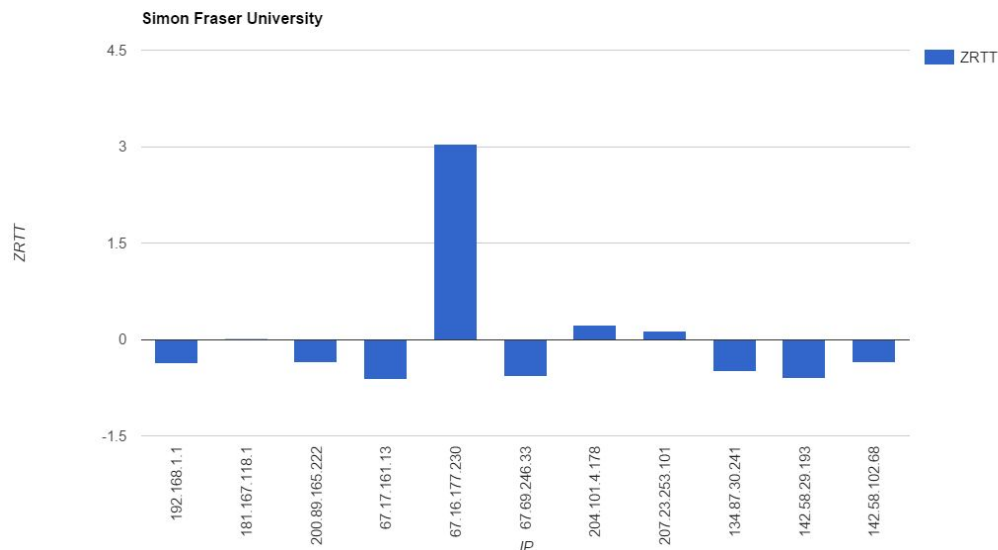


También se había mencionado como un nodo cuyo ZRTT se desprende de la media, al que posee dirección 154.54.30.186. En este caso, si contemplamos la tabla, es el último nodo antes de cambiar de red (pasa de la 154.53.30.186 a la 130.117.50.201). Esto podría implicar un encolamiento ya que ambas redes se encuentran en la misma ciudad.

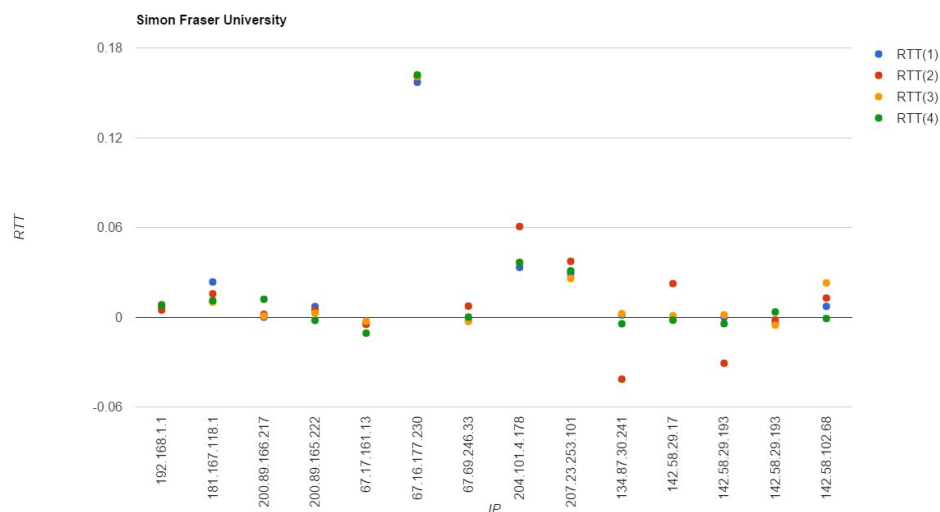
Finalmente, hicimos mención sobre la fluctuación que se puede encontrar en algunos nodos del camino. En particular, los correspondientes a las IPs 154.54.12.69, 130.117.50.201 y 154.54.38.190. Si las analizamos, podemos ver que en todas hay un cambio de red, con lo que podría haber un cambio en la tecnología del hardware o congestión en la entrada y salida de la respectiva red. No disponemos de los medios para asegurar que esto fuese lo que sucedió y no *outliers* de la experimentación.

## Universidad de Simon Fraser

La universidad de Simon Fraser tiene la particularidad de que el servidor que aloja su sitio web se encuentra dentro del mismo continente que la IP de origen de los paquetes que se enviaron, con lo que no deberíamos ver saltos interoceánicos en ninguno de los graficos, y los tiempos de transmisión no deberían ser importantes en el cálculo de cada RTT y ZRTT.



Encontramos que de todos los ZRTT, el de la IP 67.16.177.230 se distingue por ser el máximo, con un valor significativamente mayor al del resto, haciendo que la media esté por encima de todos.



Al realizar el análisis de rastrear varias veces una ruta, encontramos que nuevamente las tendencias se mantienen respecto al gráfico anterior. Nuevamente encontramos picos de RTT, y que los tiempos y amplitudes de los RTT son muy similares a los encontrados en otros graficos, aún no habiendo saltos intercontinentales



Como ya vimos, el enlace entre Argentina y Estados Unidos no aporta un gran ZRTT. Por otro lado, el segundo enlace de mayor longitud debiera ser el que cruza de este a oeste Canadá. Sin embargo, no es un enlace subacuático ni de gran distancia en comparación a los analizados previamente, por lo que los valores de ZRTT y RTT no deberían ser importantes.

TTL	IP	Locacion	Router	Empresa
1	192.168.1.1	Buenos Aires Argentina	-	-
2	181.167.118.1	Buenos Aires Argentina	1-118-167-181.fibertel.com.ar	Cablevision SA
3	Desconocido	-	-	-
4	Desconocido	-	-	-
5	Desconocido	-	-	-
6	Desconocido	-	-	-
7	200.89.165.222	Buenos Aires Argentina	222-165-89-200.fibertel.com.ar	Cablevision SA
8	67.17.161.13	EEUU	xe-1-1-3.ar3.eze1.gblx.net	Global Crossing
9	67.16.177.230	Manhattan Illinois EEUU	ae1-0-70G.ar6.CHI1.gblx.net	Global Crossing

10	67.69.246.33	Montreal Quebec Canada	bx4-chicagodt_10GE0-4-0- 0_peer.net.bell.ca	Bell Sympatico
11	Desconocido	-	-	-
12	Desconocido	-	-	-
13	Desconocido	-	-	-
14	Desconocido	-	-	-
15	Desconocido	-	-	-
16	204.101.4.178	Ottawa Ontario Canada	-	Ontario Investment Services
17	207.23.253.101	Vancouver British Columbia Canada	cr2-tx3928.vncv1.BC.net	BCNet
18	134.87.30.241	Vancouver British Columbia Canada	-	BCNet
19	Desconocido	-	-	-
20	Desconocido	-	-	-
21	142.58.29.193	Burnaby(Vancouver) British Columbia Canada	bby-sh1125-EX4500-1-bby- sh1125-x-1.net.sfu.ca	Simon Fraser University
22	142.58.102.68	Burnaby(Vancouver) British Columbia Canada	buntzenf.sfu.ca	Simon Fraser University

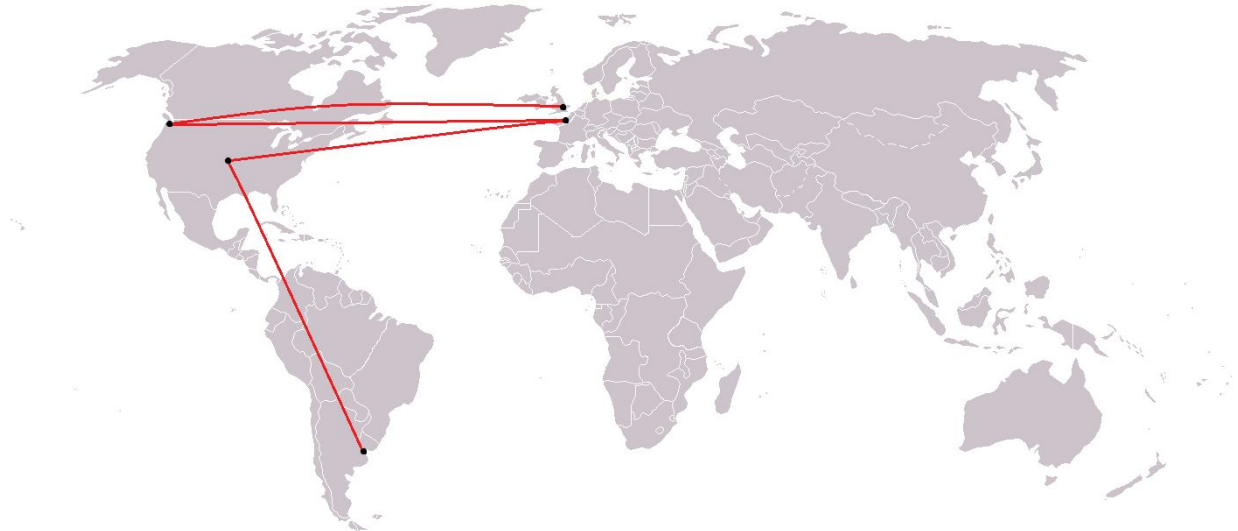
La IP 67.16.177.230 corresponde a Manhattan, Illinois, Estados Unidos. Si recordamos la experimentación realizada para la Universidad de Peking y la Universidad de Rhodes, uno de sus valores altos de ZRTT ocurría también en la misma ciudad bajo la misma empresa, Global Crossing. En el caso de Peking, la dirección IP que atraviesa era la 67.16.134.218, mientras que para Rhodes es 67.16.139.18. Esto hace pensar que las tres direcciones pertenecen a una misma red (67.16.0.0/16) y que en ese lugar se encuentra un centro neurálgico de Global Crossing. De esta manera, el ZRTT alto se corresponde con un mayor tiempo de encolamiento debido a la cantidad de información que procesa dicho lugar.

Por otro lado, y como se mencionó antes, una de las distancias más largas a realizarse es la que cruza de lado a lado Canadá. Cabe mencionar que esto se corresponde con la IP 207.23.253.101, la cual, si miramos en el gráfico de ZRTT, notamos que es positivo. Si analizamos esa dirección en el gráfico comparativo de RTT, vemos que es estable, por lo que podemos atribuir el ZRTT por encima del promedio al tiempo de transmisión que demora cruzar todo el país.

A pesar de esto, debido a no tener enlaces interoceánicos, podemos ver como el mayor desvío del promedio no es generado por los tiempos de transmisión sino por tiempos de encolamiento.

## Curiosidad: Universidad de Pretoria

Con el fin de hacer un análisis más abarcativo se optó por elegir una universidad por cada continente. En un primer momento, se eligió la Universidad de Pretoria, en Pretoria, Gauteng, Sudáfrica, como la representante de África ([www.up.ac.za/](http://www.up.ac.za/)). Sin embargo, al realizar la geolocalización nos encontramos con el siguiente mapa:



Como podemos ver, las herramientas utilizadas nos dieron que se realizan tres saltos interoceánicos. Sin embargo, no era específicas en cuanto al destino de varios de ellos. Algunas herramientas decían que se realizaba un salto entre algún lugar de Estados Unidos a París, Francia, mientras que otras nos lo daban a algún lugar de Gran Bretaña. E inmediatamente después, sale del viejo continente y se dirige al oeste de los Estados Unidos, en particular, a Seattle, Washington. Esto nos resultó anómalo y se lo atribuimos a una respuesta errónea de las herramientas de geolocalización.

Otro comportamiento curioso fue que, luego de pasar por dos routers en Seattle, la siguiente dirección IP corresponde a Londres, Inglaterra, lugar donde llega al host de la página. Esto significa que la página de la Universidad de Pretoria se encuentra en Inglaterra y no en Sudáfrica como se había supuesto en un primer momento.

Por estas dos cosas, se decidió utilizar a la Universidad de Rhodes para representar a África. Sin embargo, creímos interesante mostrar ambos comportamientos en esta sección. De esta forma podemos sustentar los posibles errores que brindan las herramientas de geolocalización en nuestra experimentación (o tal vez, simplemente una muy mala utilización de los routers para direccionar a la página de una universidad), y también brindar un dato interesante como es que una página no necesariamente está hosteada por el lugar de procedencia de aquello que representa.

## Contrastando con la realidad

En esta sección del trabajo, se simuló una conexión mediante el envío de sucesivos paquetes ICMP de tipo *echo-request*.

El fin de esta simulación fue obtener paquetes ICMP *echo-response* para poder hacer análisis de estimación de RTT, pérdida de paquete y throughput.

Se enviaron 149 paquetes, y se los analizó tomando de la misma muestra, la siguiente cantidad de paquetes en orden de ocurrencia: 9, 29, 49, 69, 89, 109, 129 y 149. Por cada grupo se varió el  $\alpha$  entre 0.1 y 0.9 con intervalos de 0.1.

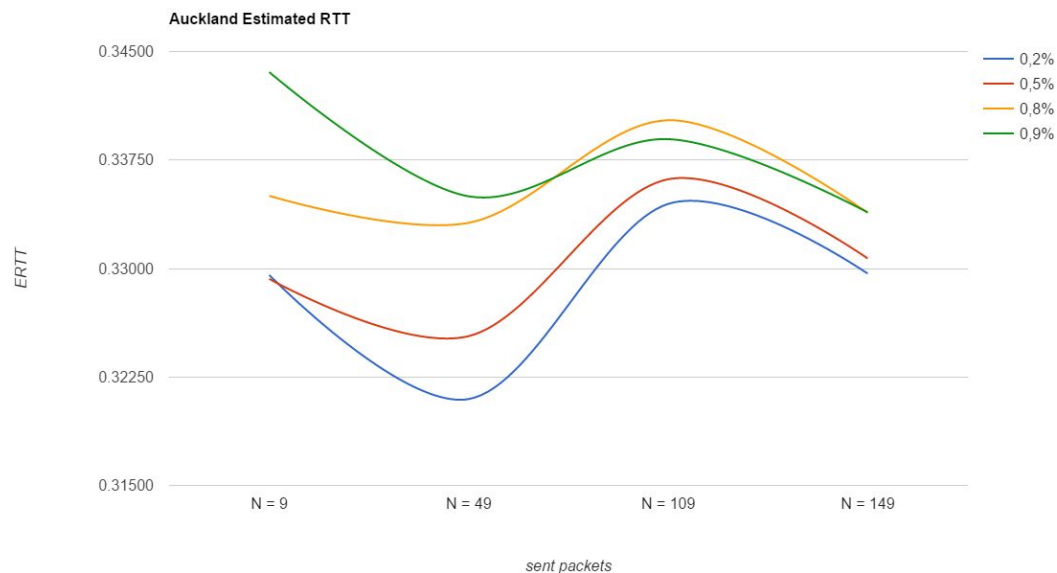
Para cada combinación de  $n$  paquetes y  $\alpha$ , se analizó la cantidad de paquetes perdidos, los tiempos de RTT promedio, el RTT estimado y throughput (ambos últimos explicados en la sección de contexto teórico)

Primero se graficaron los RTT estimados de cada una de las rutas escogidas en el principio del trabajo, acotado a los grupos de 9, 49, 109 y 149 paquetes y variando el  $\alpha$  entre 0.2, 0.5, 0.8 y 0.9, luego se compararon el RTT promedio del grupo de 149 paquetes (por considerarla la muestra más representativa) con el promedio de los RTT calculados con *el traceroute* de la primera parte. Para esto se sumaron todos los RTT intermedios, definiendo para los nodos desconocidos, el RTT promedio obtenido en su ruta.

Por último, se analizará el throughput en función de los RTT estimados previamente, y se analizará cuál es la mejor estrategia de estimación en cada caso.

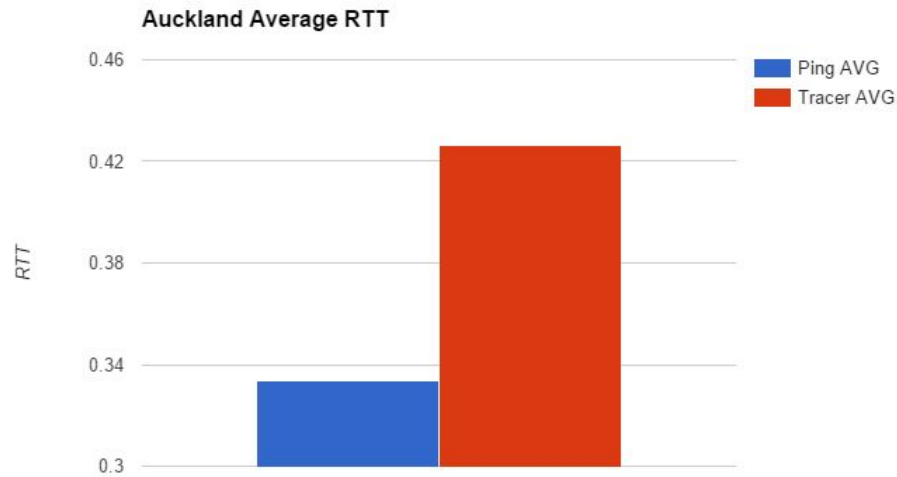
## Universidad de Auckland

Analicemos el gráfico de estimaciones de RTT.



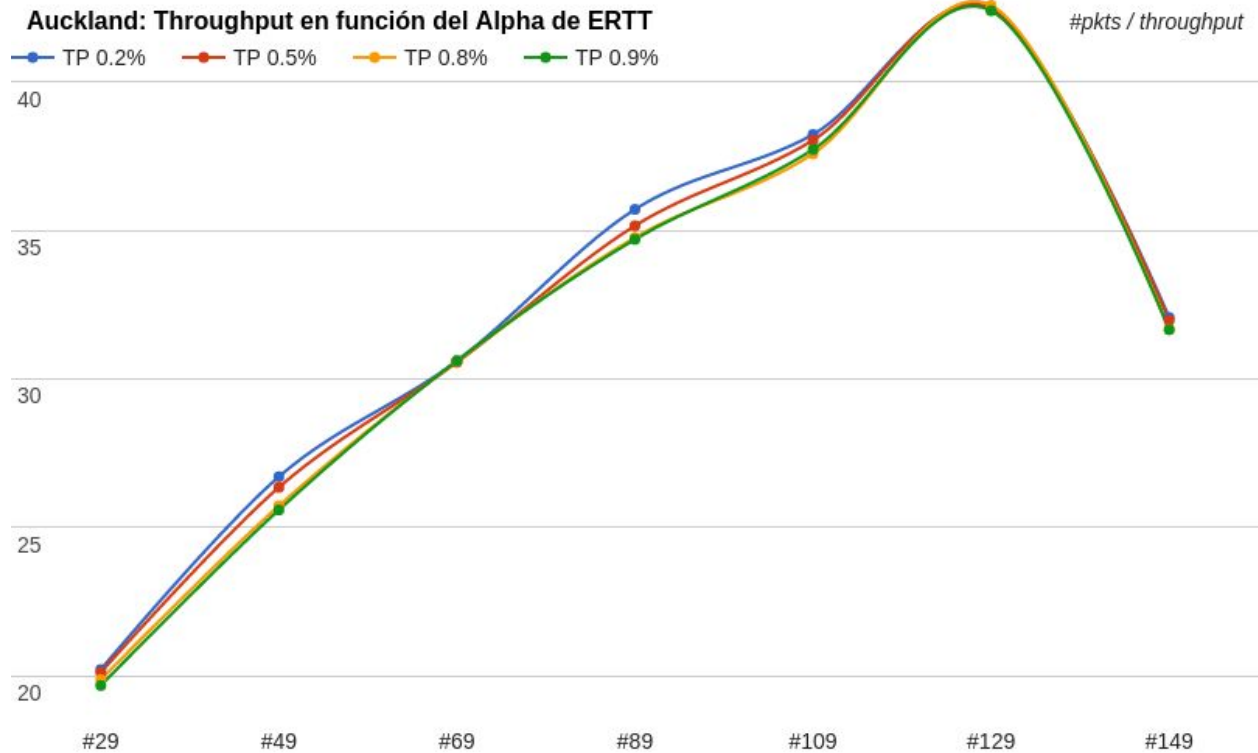
El  $\alpha$  nos indica cuánto se protege la estimación del RTT frente a un nuevo RTT muestreado. Un  $\alpha$  grande es muy conservador del resultado obtenido, mientras que un  $\alpha$  pequeño actualiza la estimación más velozmente.

Veamos en el gráfico que para un  $\alpha$  grande (porcentajes establecidos por cada función de color), el RTT estimado varía más lento que para los  $\alpha$  más chicos. Mientras más chico sea  $\alpha$ , más fluctuantes son los resultados, y esto también nos habla de la homogeneidad de la muestra. Podemos decir que la muestra, además de ser fluctuante, tuvo respuestas muy lentas al principio, que rápidamente mejoraron mucho, luego disminuyeron y al final más rápidas nuevamente. Se puede observar como el RTT estimado para 0.9 no pudo recuperarse rápidamente de unos primeros mensajes lentos (ya que la información inicial pesa más que la que apareció posteriormente), mientras que el resto sí. Como contrapartida, no se vio tan afectado por las fluctuaciones de la muestra.



Si ahora comparamos el promedio de los RTT de los mensajes *ping* que enviamos a la Universidad de Auckland, con la suma de los RTT de los mensajes ICMP enviados individualmente a cada nodo de la ruta, podemos ver que hay mucha diferencia en sus valores. Esto confirma lo dicho anteriormente sobre los tiempos de encolamiento de los paquetes ICMP, ya que el ping sólo contempla el posible encolamiento en servidor de destino, en cambio la suma de los RTT internos contempla todos los encolamientos de cada nodo intermedio, siendo más de un 20% el retardo por encolamiento para esta ruta.





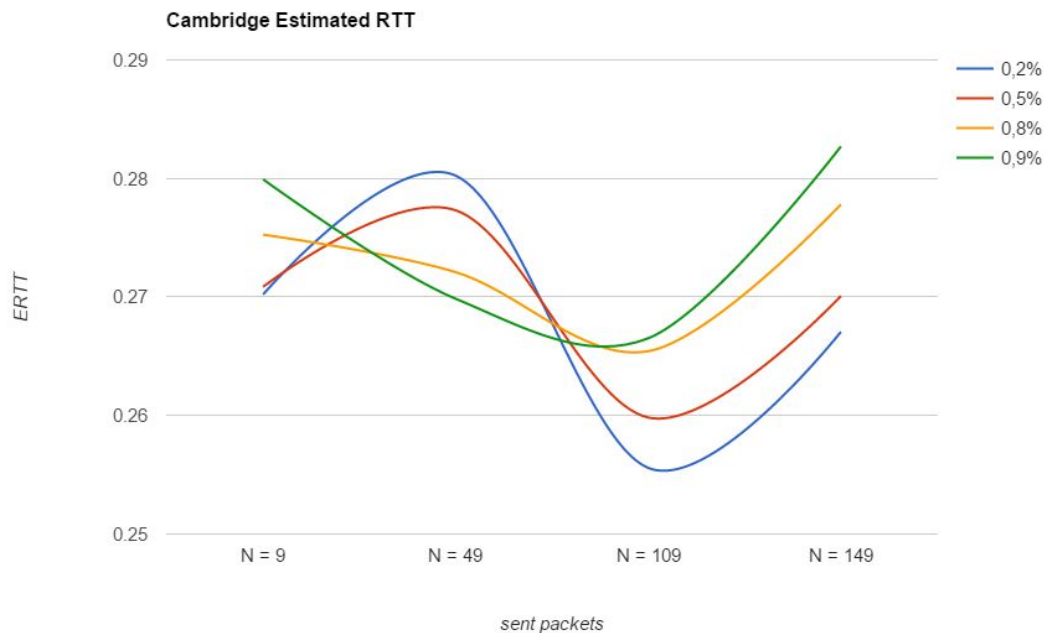
Con respecto al *throughput* en esta muestra, podemos ver que todos poseen un comportamiento similar. Todos llegan a un pico máximo aproximado de 43 paquetes cuando se pierden mensajes, teniendo que ajustar la ventana a un valor menor.

Mientras menor es el porcentaje de *alpha*, más abruptas son las tangentes en cada punto de la muestra. Este resultado implica que el ERTT, es más reactivo a la información nueva. Si existen redes donde el comportamiento es estocástico, consideramos interesante evaluar la posibilidad de usar un valor pequeño para poder ajustarse más rápido al cambio. Si en cambio, el comportamiento está bien definido, darle más importancia a la historia daría mejores resultados, al suavizar los pocos *outliers* generados (suponiendo este, un caso posible en la dinámica de Internet actual).

Si el tráfico de red tuviera épocas, sería interesante analizar un *alpha* adaptativo que al darse cuenta que la época cambió, destruya la historia (disminuyendo su valor) y vuelva a converger elevando su valor suavemente.

## Universidad de Cambridge

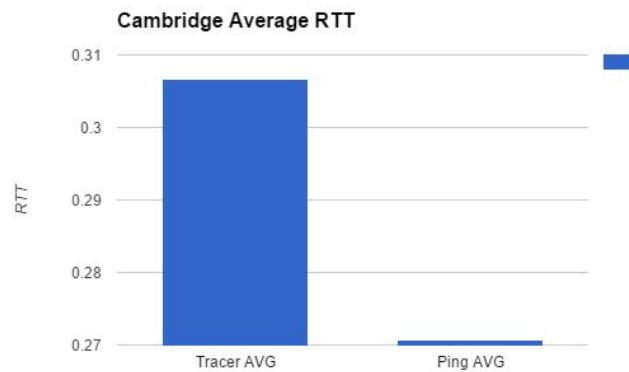
Veamos los resultados obtenidos para las estimaciones de la Universidad de Cambridge



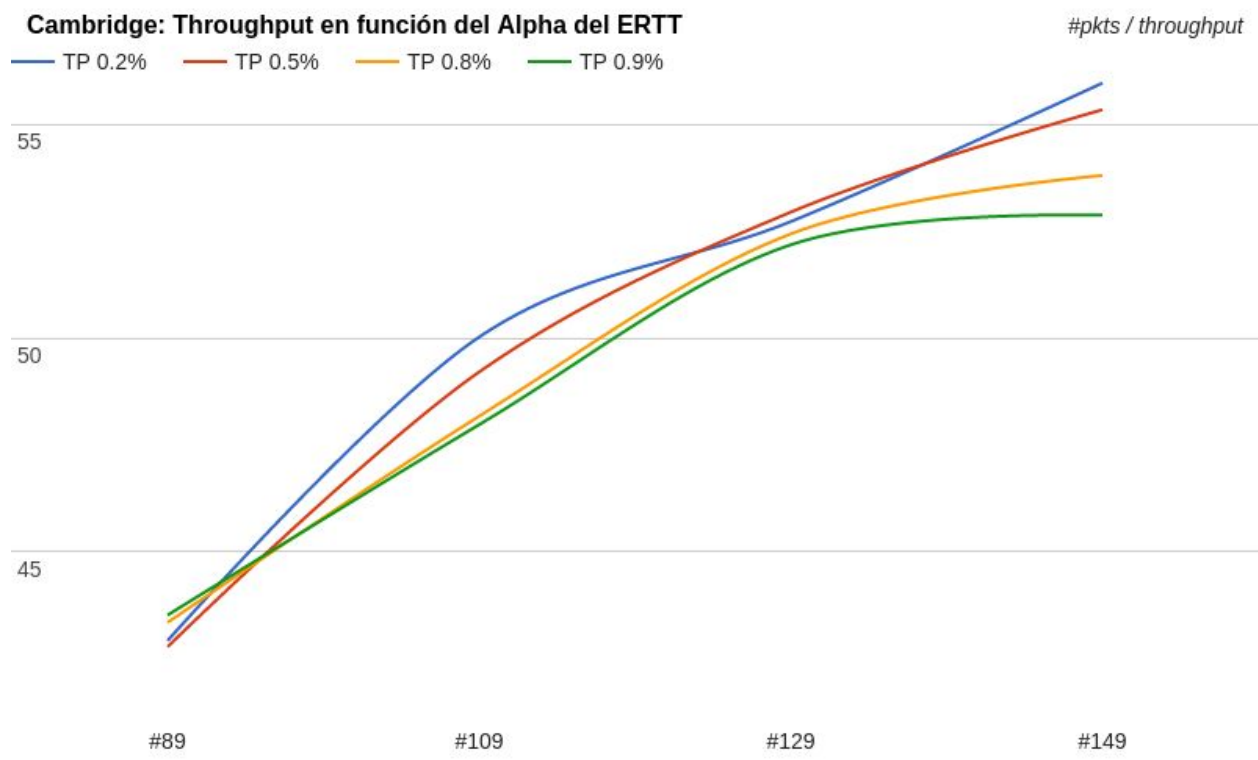
En este caso, podemos ver cómo la política de actualización de la estimación puede cambiar la tendencia en la progresión de estimaciones. Se ve claramente como con un  $\alpha$  pequeño, los cambios son muy bruscos, comenzando por un mensaje de velocidad media, corrigiendo velozmente hacia mensajes muy lentos, luego cayendo en picada hacia mensajes más rápidos, y terminado en mensajes de velocidad media.

El  $\alpha$  más grande, en cambio, mantuvo su actualización constante hacia los mensajes más rápidos, cambiando una única vez hacia los paquetes más lentos del final.

Cabe aclarar que la distribución de los mensajes no es homogénea dentro de cada número de paquetes. Se puede observar como dentro de los primeros 9 paquetes hubo una diferencia significativa entre los primeros y los últimos, ya que la estrategia más conservadora parte de mucho más arriba que las menos conservadoras y más bruscas.

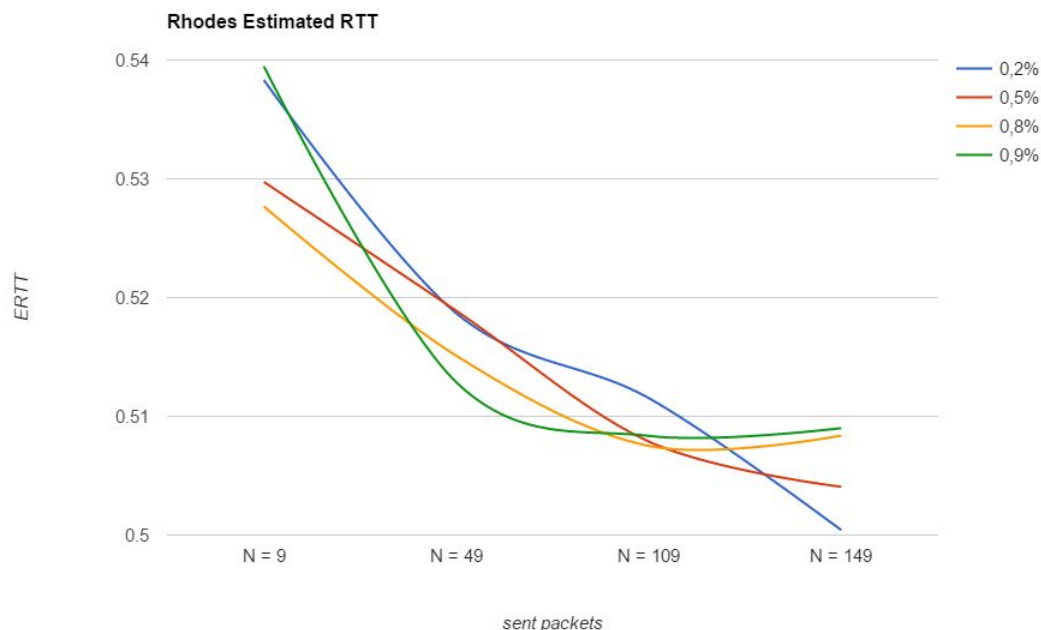


Cuando comparamos el promedio de RTT de los *pings* directos a la IP destino con la suma de los RTT en los nodos intermedios, vemos que la diferencia es menor a la observada en la ruta anterior, siendo ésta de alrededor de un 12%.

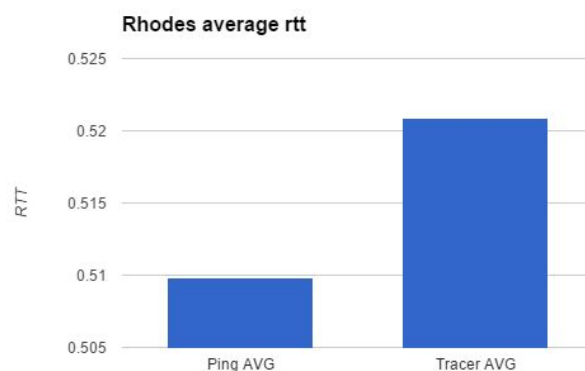


Hemos visto que esta red tuvo muchas fluctuaciones en su tasa de respuesta. Por esta razón, un  $\alpha$  más pequeño obtiene mejores resultados. La razón es que puede corregir más rápidamente las fluctuaciones de la red, aunque por momentos corrige demasiado rápido y se ubica por debajo del  $\alpha$  0.5.

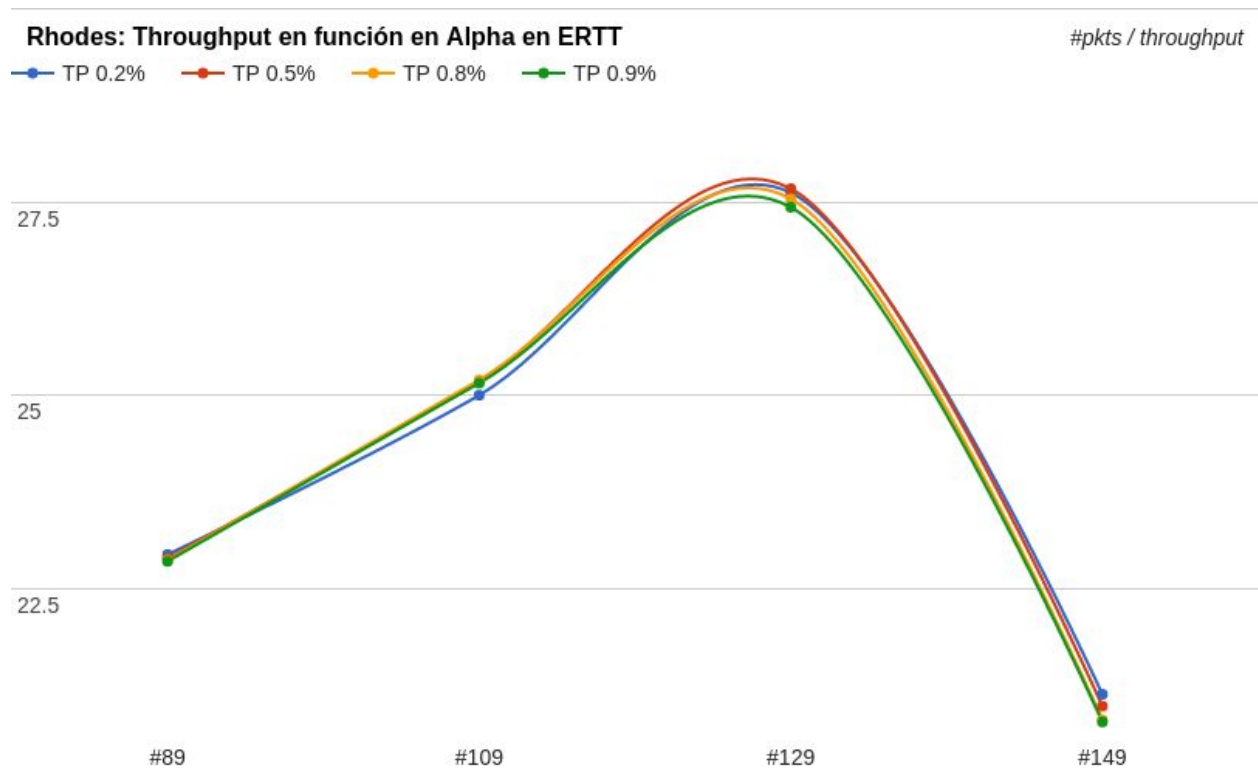
## Universidad de Rhodes



Esta ruta tuvo un comportamiento particular respecto a las muestras de las rutas anteriores. Inicialmente registramos un momento de mucha congestión, donde el encolamiento de paquetes hizo que el RTT crezca aún más que la acumulación de paquetes enviados a los nodos intermedios. Se ve que rápidamente se comienza a descongestionar, mejorando a su RTT continuamente hasta el final. Sin embargo, el comportamiento no es tan lineal como parece, ya que el  $\alpha$  0.9 en un momento deja de aumentar la velocidad de respuesta, pero el  $\alpha$  0.2 sigue bajando. Vemos que el  $\alpha$  0.5 se mantiene constante, sin sucumbir drásticamente al cambio, ni atándose con resultados tan anteriores.

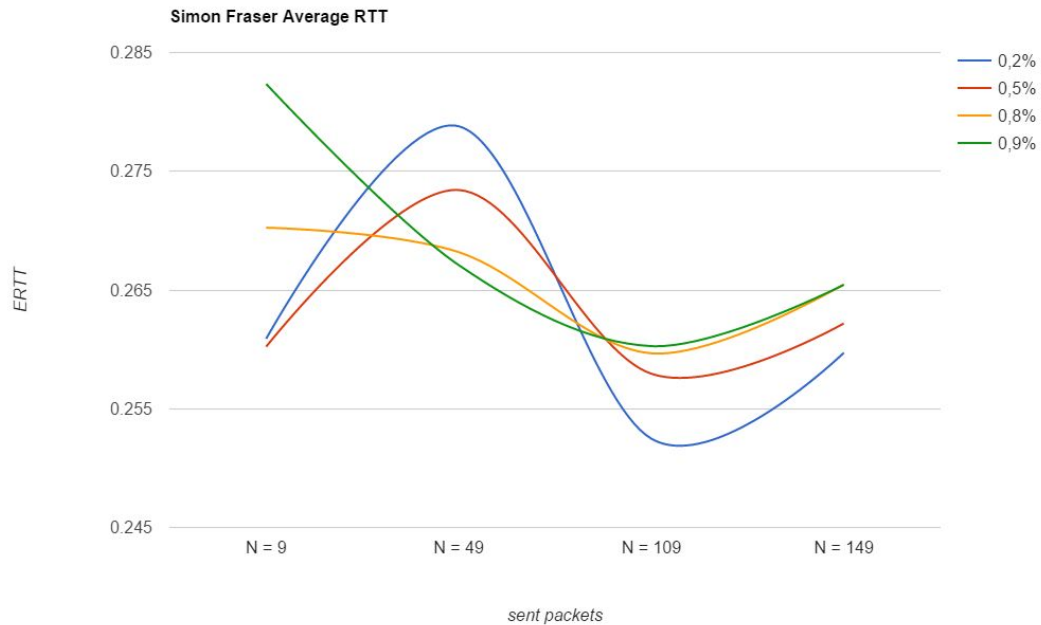


No resulta tan raro, luego de ver que hubo valores de RTT muy altos, que no haya mucha diferencia entre los promedios obtenidos para el ping y el promedio de nuestra ejecución del *traceroute*. Debido al lento comienzo que acarreó el ping, su RTT promedio aumenta haciéndolos significativos. De esta manera, la diferencia entre ambos es casi tan chica como 0,1 segundos. De esta forma podemos ver como una gran espera en ciertos nodos de la red en un determinado viaje del paquete puede ser determinante a la hora de una buena performance del ping.



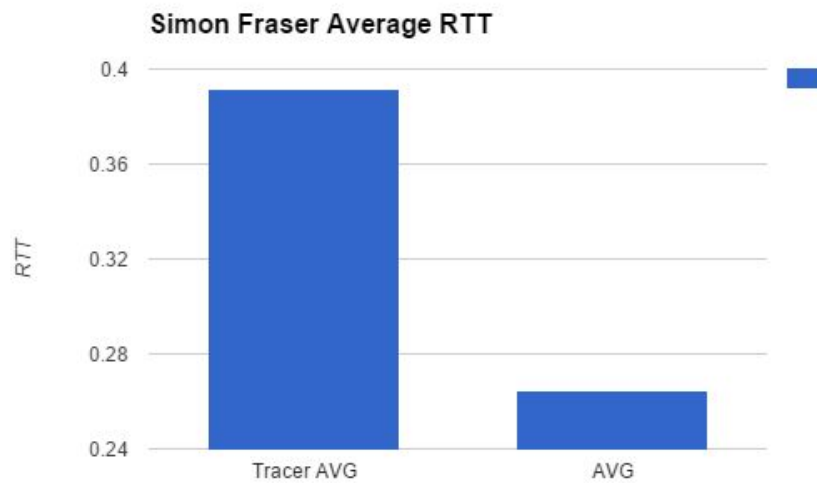
El *throughput* se maximiza con *alpha* 0.5. Tener una actitud equilibrada ayudó mantener la estabilidad de la estimación, en una red que, a priori, parecía tener una tendencia muy marcada y donde no habia necesidad alguna de ser conservador en cuanto a la actualización de la estimación. Teniendo este gráfico, podemos ver que los RTT no cambian a la velocidad que *alpha* 0.2 nos decía inicialmente.

## Universidad de Simon Fraser



Este análisis resulta muy similar al de la universidad de Cambridge, siendo las tendencias de cada  $\alpha$  muy similares a esa ruta.

La diferencia entre estos dos análisis radica en que la ruta a Cambridge tiene un salto interoceánico entre Estados Unidos e Inglaterra, y la ruta a Simon Fraser no. Vemos una vez más como las largas distancias no son siempre significativas, o cuando menos determinantes, respecto al RTT de paquetes ICMP.



Nuevamente obtenemos iguales resultados. El tiempo de encolamiento en cada *router* agrega mucho tiempo y corre el promedio significativamente.

No podemos hacer cálculo de *throughput* para esta universidad dado que en la muestra no se perdió ningún paquete. Si la probabilidad de pérdida es 0, según la fórmula, el *throughput* sería infinito.

Para la Universidad de Peking, tampoco pudimos hacer las pruebas, ya que el *end-point* filtra los *pings*. Al no tener los pings, no se puede estimar el RTT, y por consiguiente, tampoco calcular su *throughput*.

## Conclusiones

Al tratar de encontrar los enlaces submarinos encontramos que la forma más efectiva de hacerlo es a través de buscar la geolocalización de cada IP en la ruta. Si bien hay direcciones IP que no son precisamente localizables, siempre se puede seguir el camino realizado por el paquete y saber a través desde qué routers (o cercano a qué routers) se realiza el salto interoceánico. Sin embargo, al tratar de deducir cuáles son los enlaces submarinos a partir del RTT y ZRTT de cada router en la ruta, no siempre fue posible predecirlo. Concluimos que este último método no es siempre confiable debido a que hay ciertos nodos cuyo RTT fluctúa mucho debido a la enorme carga que tienen, como por ejemplo los *backbones* que fueron analizados en secciones anteriores.

Debido a que el tiempo de encolamiento es muy notorio en varios routers, un gran valor de ZRTT o RTT no siempre va a indicar que exista un gran tiempo de transmisión. Sin el análisis de la fluctuación del RTT promedio, no hay suficiente información para asegurar si el ZRTT se corresponde a tiempo de transmisión o de encolamiento. Analizando los RTT promedio y sus fluctuaciones, se podría inferir una relación entre las colas de ICMP y el tiempo de encolamiento.

Encontramos casos donde el salto interoceánico no superó ampliamente el RTT promedio (como es el caso de la Universidad de Cambridge). No se puede asegurar que haya un gran salto sin realizar, además, un análisis geográfico de las direcciones para corroborar si el RTT se debe en mayor parte a la distancia atravesada o al tiempo que el paquete estuvo esperando a ser atendido.

Debemos ser cautelosos al intentar comprender el funcionamiento de Internet utilizando paquetes ICMP. Hemos visto que gran cantidad de *routers* los bloquean, o tratan con menor prioridad, y por lo tanto los resultados pueden llegar a ser muy poco precisos. Esperamos ansiosos al nuevo algoritmo de *traceroute* especificado en el RFC 1393. Consideramos que la información devuelta por los ICMP deben tomarse como orientativa.



## Referencias

- <https://geoiptool.com/es>
- <http://www.submarinecablemap.com/>
- [http://es.wikipedia.org/wiki/Global\\_Crossing](http://es.wikipedia.org/wiki/Global_Crossing)
- <http://www.plotip.com/ip/>
- <https://db-ip.com/>
- <https://www.findip-address.com/>
- <https://www.google.com.ar/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=Distancia+entre+stoney+creek+y+montreal>
- [https://en.wikipedia.org/wiki/Level\\_3\\_Communications](https://en.wikipedia.org/wiki/Level_3_Communications)
- <http://www.velcom.com/>
- <https://www.google.com.ar/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=distancia%20brampton%20stoney%20creek>