



Teoría de las Comunicaciones

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

Trabajo Práctico N°2

Rutas en Internet

Conformación del grupo

Integrante	LU	Correo electrónico
Alvaro Jose Fernando	89/10	fer1578@gmail.com
Barbeito Nicolás	147/10	nicolasbarbeiton@gmail.com
Brum Raúl	199/98	brumraul@gmail.com
Nievas Yésica	340/05	yesica.nievas@gmail.com

Reservado para la cátedra

Instancia	Docente	Nota
Primera entrega		
Segunda entrega		

Índice

1. Introducción	2
2. Desarrollo	2
2.1. Traceroute	2
2.1.1. Rutas alternativas	2
2.1.2. RTT acumulado	2
2.2. Estadísticas	3
2.3. Geolocalización	3
3. Resultados y Análisis	4
3.1. Universidad de Tokyo	4
3.1.1. Datos	4
3.1.2. RTT y Δ RTT	6
3.1.3. Test de Grubbs	7
3.1.4. Geolocalización	7
3.2. Universidad de Pretoria	8
3.2.1. Datos	8
3.2.2. RTT y Δ RTT	9
3.2.3. Test de Grubbs	10
3.2.4. Geolocalización	10
4. Conclusiones	10

1. Introducción

2. Desarrollo

Para realizar las consignas planteadas en el presente trabajo práctico utilizaremos una serie de herramientas cuya descripción y detalles de implementación mostraremos a continuación.

2.1. Traceroute

Para la implementación una herramienta similar a traceroute utilizaremos la librería “scapy” de python a fin de generar paquetes “ICMP” variando el campo “TTL” y posteriormente analizaremos las respuestas recibidas.

El encabezado del paquete IP tiene un campo llamado “TTL” (Time To Live) y un limite superior de la cantidad de tiempo que un paquete IP puede permanecer en la red. El campo TTL es seteado por el remitente del paquete y es reducido por cada router por el que pasa el paquete para llegar a su destino. Si el campo llega a 0 antes de llegar a destino el paquete es descartado y un paquete ICMP “Time Exceeded” es enviado al remitente para notificarlo de lo sucedido. La IP fuente de ese paquete es la IP del router que descarto el paquete. En Teoría el campo TTL bajo IPv4 es medido en segundos y cada host por el que pasa el paquete debe reducirlo en al menos una unidad. En la practica el campo es reducido en una unidad por cada host.

Para determinar la ruta de paquete al host destino enviaremos varios paquetes IP incrementando el campo TTL en una unidad para ir recibiendo los “Time Exceeded” de cada router por el que pasa el paquete. EL “RTT” (Round Trip Time) se compondrá del tiempo que tarda el paquete en viajar hasta cada nodo mas el tiempo de encolamiento en cada nodo. A fin de homogeneizar el resultado obtenido y descartar “outliers” correremos nuestro algoritmo con varias iteraciones y tomaremos valores promedios.

Dada la decisión adoptada de correr el algoritmo en varias iteraciones, la forma de calcular la rutas y la naturaleza de internet se nos pueden plantear los siguientes casos.

2.1.1. Rutas alternativas

Dada la naturaleza de internet y el funcionamiento de los routers por los que pasa nuestro paquete puede suceder que un paquete a un mismo destino tome rutas distintas según el momento en que sea enviado. Esto puede suceder por ejemplo por la congestión de un router que decida forwardear un paquete por un puerto distinto y por lo tanto tomara una ruta distinta o puede suceder que un router se encuentre caído por lo que en router anterior envié el paquete por otra ruta. A los efectos de nuestra herramienta se nos planteara que en un determinado salto un paquete tiene rutas distintas por las que pasa, a fin de subsanar este inconveniente para cada salto tomaremos la ruta con mayor frecuencia de aparición en las diferentes corridas de nuestro algoritmo.

2.1.2. RTT acumulado

Pueden darse casos donde el RTT al salto i sea menor que el RTT al salto anterior. Parecería extraño que RTT_i sea menor que RTT_{i-1} pero esto aparece con frecuencia en la practica. Las razones para este comportamiento pueden ser por la congestión de los routers como así también por la

prioridad en la cola de los mismos. En este ultimo caso por ejemplo el router puede tener menor prioridad para la cola de paquetes ICMP y por lo tanto el tiempo de encolamiento en este router sera mayor cuando descarta el paquete y enviá un paquete ICMP “Time Exceed” que cuando forwardea el paquete al router siguiente. Esto generara que el RTT a ese router sea mayor que el RTT al router siguiente.

En la implementación de nuestra herramienta para obtener el ΔRTT correspondiente al RTT en el salto i usaremos la siguiente formula:

$$\begin{aligned} \Delta RTT_0 &= 0 \\ \Delta RTT_1 &= RTT_1 \\ \Delta RTT_i &= \begin{cases} RTT_i - RTT_{i-1} & \text{Si } RTT_i > RTT_{i-1} \\ 0 & \text{Caso Contrario} \end{cases} \end{aligned}$$

Esto es para evitar computar ΔRTT negativos que pueden generarse por lo comentado anteriormente.

2.2. Estadísticas

Para el cumplimiento de la consigna sobre estadísticas de las rutas utilizamos la librería “numpy” de python para el calculo de la media y el desvió estándar, la librería “scipy” de python para el calculo del test de normalidad sobre los ΔRTT y finalmente implementamos el “Test de Grubbs” sobre los ΔRTT a fin de detectar outliers para relacionarlos con la detección de enlaces submarinos en las rutas.

Para el test de Grubbs si bien es requisito para correr el mismos que la distribución de los ΔRTT sea “Normal”, a sugerencia de la cátedra en caso de no serlo correremos igualmente el test y verificaremos si de todas maneras detecta los enlaces submarinos.

2.3. Geolocalización

En esta parte intentaremos localizar la ubicación geográfica de los distintos routers por los que pasan los paquetes y exponerlos luego en un mapa trazando la probable ruta recorrida. Para esto nos valeremos de servicios de geolocalización que permiten relacionar una dirección IP con una ubicación geográfica. Cabe aclarar que la información brindada por estos servicios no siempre es exacta, ya sea porque la base de datos esta desactualizada, tenga errores o puede suceder que una red este registrada en un país pero la ubicación física del router este en otro por lo que la ubicación aportada por el servicio de geolocalización sera errónea.

En las tablas de traceroute dejaremos reflejada la ubicación aportada por los servicios de geolocalización, si embargo a la hora de realizar el mapa tomaremos algunas medidas a fin de tratar de mitigar estos errores.

- Si la geolocalización informa que hay un cambio de país en el salto con una distancia considerable entre ambos paises pero esto no se condice con el ΔRTT pequeño del salto asumiremos que la geolocalización esta informando el lugar de registro de la red y no la ubicación física del router por lo que utilizaremos como ubicación la de su salto anterior.
- Si la geolocalización informa que el próximo salto esta en el mismo país y ese salto tiene un ΔRTT muy alto, lo que haremos es mirar la ubicación del salto siguiente a ese, si este esta en

otro país pero tiene un ΔRTT pequeño, entonces asumiremos que el salto en cuestión esta en otro país y que se trata del mismo error anterior de registración de la red.

- Ya sea para confirmar la opción tomada en los items anteriores o para decidir en caso de no ser tan clara las diferencias de ΔRTT utilizaremos también la información aportada por “Reverse DNS” para así atraves del nombre de dominio de cada IP tratar de conseguir pistas sobre la ubicación geográfica de los routers.

Aclaramos que estas heurísticas no son del todo eficaces por lo que bien podríamos estar utilizando información errónea al dibujar la ruta en el mapa.

3. Resultados y Análisis

En esta sección presentaremos y analizaremos los resultados obtenidos al correr los distintos test propuestos. Para ello correremos los mismos con una iteración de 100 repeticiones sobre los host de las siguientes universidades.

3.1. Universidad de Tokyo

El host de destino de la universidad de Tokyo sera el dominio “www.u-tokyo.ac.jp” cuya IP es “210.152.135.178”. El host de la universidad de Tokyo se encuentra ubicado la ciudad de Tokyo, Japón. El origen sera un host ubicado en la Ciudad de Buenos Aires, Argentina utilizando como isp a Telecentro.

3.1.1. Datos

Los datos obtenidos para este caso fueron los siguientes:

TTL	IP	E(RTT) (ms)	S(RTT) (ms)	Δ RTT (ms)
1	192.168.10.1	0.414	0.025	0.414
2	10.20.64.1	9.588	2.179	9.174
3	200.115.194.173	9.709	2.050	0.121
4	208.178.195.210	11.823	2.660	2.114
5	208.178.195.209	10.154	3.919	0.000
6	64.212.107.98	140.102	2.736	129.948
7	129.250.3.172	141.972	6.459	1.870
8	129.250.2.219	165.020	5.163	23.048
9	129.250.7.69	174.848	10.839	9.828
10	129.250.2.177	289.040	10.215	114.191
11	129.250.6.144	286.955	9.046	0.000
12	61.200.80.218	281.767	6.327	0.000
13	158.205.192.173	287.145	8.005	5.378
14	158.205.192.86	300.318	5.018	13.173
15	158.205.121.250	299.293	22.325	0.000
16	154.34.240.254	287.327	2.431	0.000
17	210.152.135.178	300.554	3.888	13.227

Cuadro 1: \overline{RTT} , σ RTT y Δ RTT para la ruta utilizada para llegar www.u-tokyo.ac.jp

Analizando la información aportada por la tabla 2 podemos notar que tanto el salto 6 como 10 sobresalen por sobre el resto en cuanto a sus tiempos de Δ RTT.

3.1.2. RTT y Δ RTT

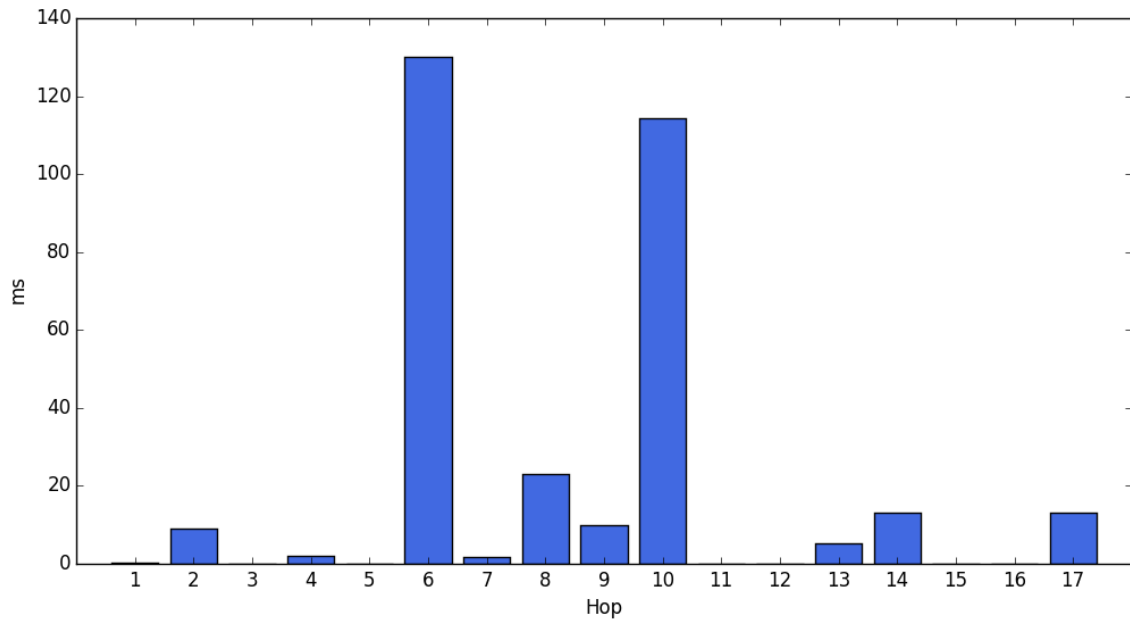


Figura 1: www.u-tokyo.ac.jp - Δ RTT

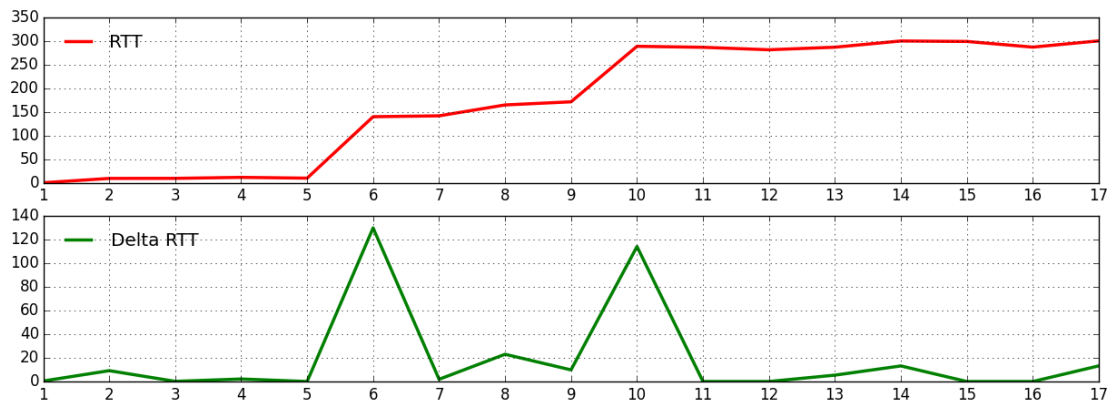


Figura 2: www.u-tokyo.ac.jp - RTT y Δ RTT

Tanto en la figura 1 como en la figura 2 podemos comprobar los que habíamos notado en la tabla 2. Esto es que tanto el salto 6 como 10 se destacan por sobre el resto. En caso de existir algún enlace submarino seguramente este se correspondería con alguno de estos saltos. Esto lo analizaremos en las siguientes secciones.

3.1.3. Test de Grubbs

Previo a correr el test de Grubbs corrimos un test de normalidad sobre la distribución de ΔRTT obteniendo los siguientes resultados:

- **z-score: 21.762**
- **p-value: 0.002**

De los resultados obtenidos deducimos entonces que la distribución de los ΔRTT no es “Normal”, igualmente como mencionamos en la sección 2.2 correremos el test de Grubbs a fin de corroborar luego si encuentra los enlaces submarinos de todas formas. Los resultados obtenidos fueron los siguientes outliers:

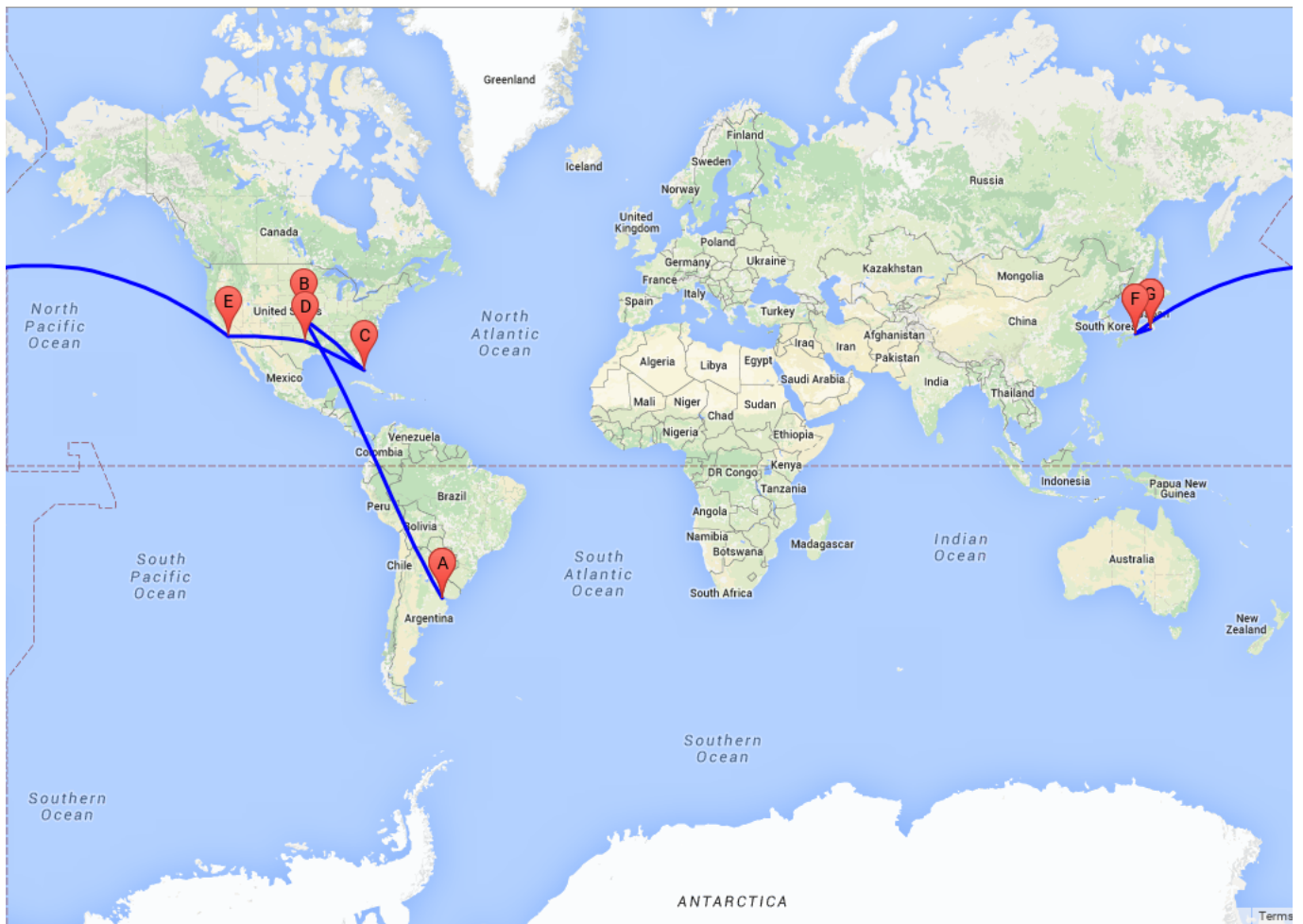
- 64.212.107.98
- 129.250.2.177

3.1.4. Geolocalización

TTL	IP	DNS	Ubicación
1	192.168.10.1	rig0.tuxhome.com.ar(ip privada)	
2	10.20.64.1	no disponible(ip privada)	
3	200.115.194.173	cpe-200-115-194-173.telecentro-reversos.com.ar	Buenos Aires, Argentina
4	208.178.195.210	global-crossing-argentina-s-a.xe-0-1-0.ar3...	Buenos Aires, Argentina
5	208.178.195.209	xe-0-1-0.ar3.eze1.gblx.net	Buenos Aires, Argentina
6	64.212.107.98	no disponible	Los Angeles, Usa
7	129.250.3.172	ae-4.r21.miamf02.us.bb.gin.ntt.net	Miami, Usa
8	129.250.2.219	ae-4.r22.dllstx09.us.bb.gin.ntt.net	Dallas, Usa
9	129.250.7.69	ae-5.r22.lsanca07.us.bb.gin.ntt.net	Los Angeles, Usa
10	129.250.2.177	ae-0.r21.osakjp02.jp.bb.gin.ntt.net	Houston, Usa
11	129.250.6.144	ae-5.r23.osakjp02.jp.bb.gin.ntt.net	Osaka, Japan
12	61.200.80.218	xe-1-1-10.r23.osakjp02.jp.ce.gin.ntt.net	Osaka, Japan
13	158.205.192.173	ae0.ostcr01.idc.jp	Tokyo, Japan
14	158.205.192.86	no disponible	Tokyo, Japan
15	158.205.121.250	po2.l321.fk1.eg.idc.jp	Tokyo, Japan
16	154.34.240.254	no disponible	Tokyo, Japan
17	210.152.135.178	www.u-tokyo.ac.jp	Tokyo, Japan

Cuadro 2: Ruta utilizada para llegar www.u-tokyo.ac.jp con la ubicación de los diferentes saltos por los que se pasa. Se encuentran resaltados los saltos distinguidos calculados en la sección 3.1.3

En la tabla 2 notamos que el salto 10 figura ubicado en Houston, Estados Unidos, sin embargo dado el ΔRTT de este salto que hizo que sea distinguido como outlier en la la sección 3.1.3 y su DNS reverso “ae-0.r21.osakjp02.jp.bb.gin.ntt.net” inferimos que es un error en las bases de datos de geolocalización y que ese salto se encuentra efectivamente ubicado en Osaka, Japon. Por este motivo al trazar el traceroute sobre el mapa de la figura 3 lo ubicamos en esta última localidad.

Figura 3: www.u-tokyo.ac.jp - Traceroute

3.2. Universidad de Pretoria

El host de destino de la universidad de Pretoria sera el dominio “www.up.ac.za” cuya IP es “5.10.110.85”. El host de la universidad de Pretoria se encuentra ubicado la ciudad de Pretoria, en sudáfrica. El origen es un host ubicado en la Ciudad de Buenos Aires, Argentina utilizando como isp a Telecentro.

3.2.1. Datos

Los datos obtenidos para este caso fueron los siguientes:

TTL	IP	E(RTT) (ms)	S(RTT) (ms)	Δ RTT (ms)
1	192.168.0.1	3.037	3.218	3.037
2	10.19.0.1	21.794	23.114	18.757
3	200.115.195.81	19.089	14.663	0.000
4	208.178.195.214	20.840	13.042	1.751
5	208.178.195.213	22.422	18.565	1.582
6	67.17.75.66	158.745	28.768	136.323
7	4.68.111.121	152.379	26.292	0.000
8	4.69.168.11	272.512	19.879	120.133
9	4.69.168.11	277.326	26.226	4.814
10	212.73.206.174	292.420	28.952	15.094
11	50.97.19.101	281.778	31.841	0.000
12	50.97.19.41	289.224	33.909	7.446
13	5.10.118.135	278.807	23.145	0.000
14	5.10.110.85	279.282	18.527	0.476

Cuadro 3: \overline{RTT} , σ RTT y Δ RTT para la ruta utilizada para llegar www.up.ac.za

Analizando la información aportada por la tabla 4 podemos notar que los saltos 2, 6, 8 y 10 sobresalen por sobre el resto en cuanto a sus tiempos de Δ RTT.

3.2.2. RTT y Δ RTT

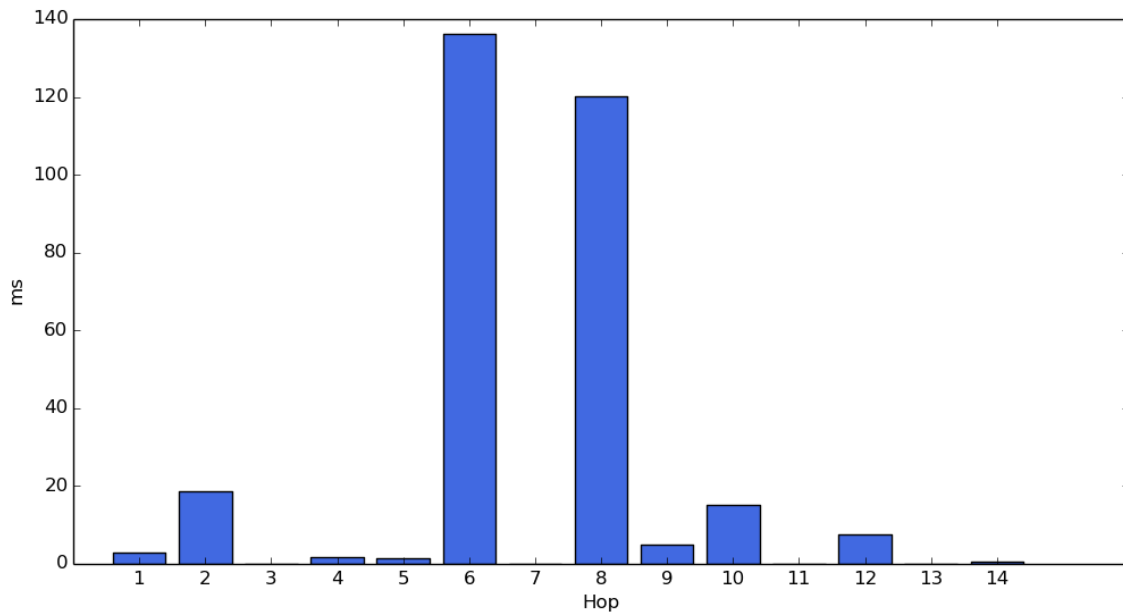
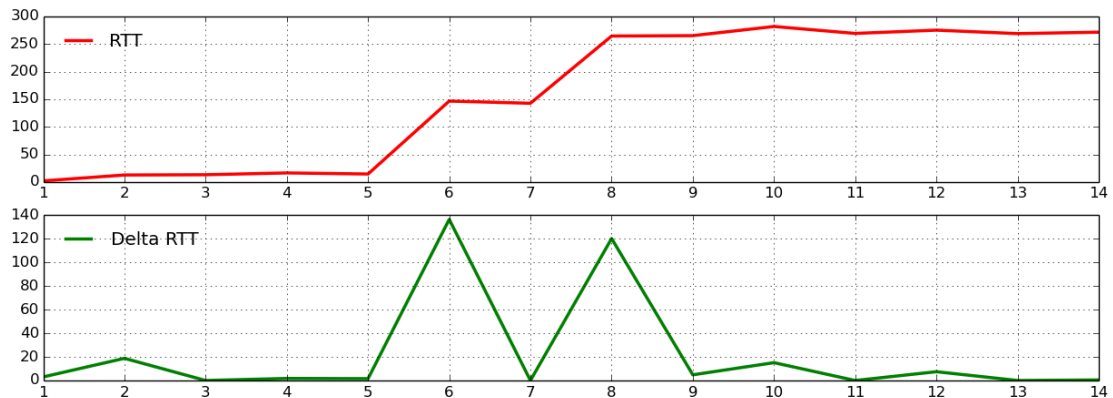


Figura 4: www.up.ac.za - Δ RTT

Figura 5: www.up.ac.za - RTT y Δ RTT

Tanto en la figura 4 como en la figura 5 podemos comprobar los que habíamos notado en la tabla 4. Esto es que tanto los saltos 2, 6, 8 y 10 se destacan por sobre el resto. En caso de existir algún enlace submarino seguramente este se correspondería con alguno de estos saltos. Esto lo analizaremos en las siguientes secciones.

3.2.3. Test de Grubbs

3.2.4. Geolocalización

TTL	IP	DNS	Ubicación
1	192.168.0.1	(ip privada)	
2	10.19.0.1	(ip privada)	
3	200.115.195.81	cpe-200-115-195-81.telecentro-reversos.com.ar	Buenos Aires, Argentina
4	208.178.195.214	global-crossing-argentina-s-a.xe-0-3-1.ar3.eze1.gblx.net	Virginia, USA
5	208.178.195.213	xe-0-3-1.ar3.eze1.gblx.net	Virginia, USA
6	67.17.75.66	po3-20G.ar3.MIA2.gblx.net	Miami, USA
7	4.68.111.121	ae5.edge2.miami2.level3.net	Miami, USA
8	4.69.168.11	ae-1-60.ear1.Paris1.Level3.net	Paris, Francia
9	4.69.168.11	ae-1-60.ear1.Paris1.Level3.net	Paris, Francia
10	212.73.206.174	unknown.Level3.net	Los Angeles, USA
11	50.97.19.101	ae1.bbr02.tg01.lon01.networklayer.com	Londres, Inglaterra
12	50.97.19.41	ae6.dar01.lon02.networklayer.com	Londres, Inglaterra
13	5.10.118.135	po1.fcr01b.lon02.networklayer.com	Londres, Inglaterra
14	5.10.110.85	55.6e.0a05.ip4.static.sl-reverse.com	Londres, Inglaterra

Cuadro 4: Ruta utilizada para llegar www.up.ac.za con la ubicación de los diferentes saltos por los que se pasa. Se encuentran resaltados los saltos distinguidos calculados en la sección 3.2.3

4. Conclusiones