



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	3
2.1.2. RTT acumulado	3
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	11
3.3. Universidad de Málaga	12
3.3.1. Datos	12
3.3.2. RTT y Δ RTT	13
3.3.3. Test de Grubbs	13
3.3.4. Geolocalización	14
3.4. Universidad MIT	15
3.4.1. Datos	15
3.4.2. RTT y Δ RTT	17
3.4.3. Test de Grubbs	17
3.4.4. Geolocalización	18
4. Conclusiones	20
4.1. Universidad de Tokyo	20
4.2. Universidad de Pretoria	20
4.3. Universidad de Málaga	20

4.4. Universidad MIT	21
--------------------------------	----

1. Introducción

En el presente trabajo nos propondremos analizar las diferentes rutas que siguen los paquetes IP en internet desde un host origen hasta alcanzar su host destino.

Para ello implementaremos una serie de herramientas basadas en el protocolo “ICMP” que nos permitan emular un “traceroute” al host destino.

Como objetivo adicional trataremos con esta herramienta poder detectar cuando un paquete pasa por un enlace submarino para lo cuál implementaremos un test de hipótesis que nos permita detectar estos enlaces y posteriormente compararemos los resultados obtenidos con la realidad.

Para cumplir con estos objetivos correremos una serie de test sobre hosts de distintas universidades, concretamente analizaremos los siguientes casos de estudio:

- **Tokyo:** University of Tokyo. Tokyo, Japon.
- **Pretoria:** University of Pretoria. Pretoria, Sudáfrica.
- **Málaga:** Universidad de Málaga. Málaga, España.
- **MIT:** Massachusetts Institute of Technology. Cambridge, Estados Unidos

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 “outliners” 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 plantea 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 desvío 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 países 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.

Aclaremos 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

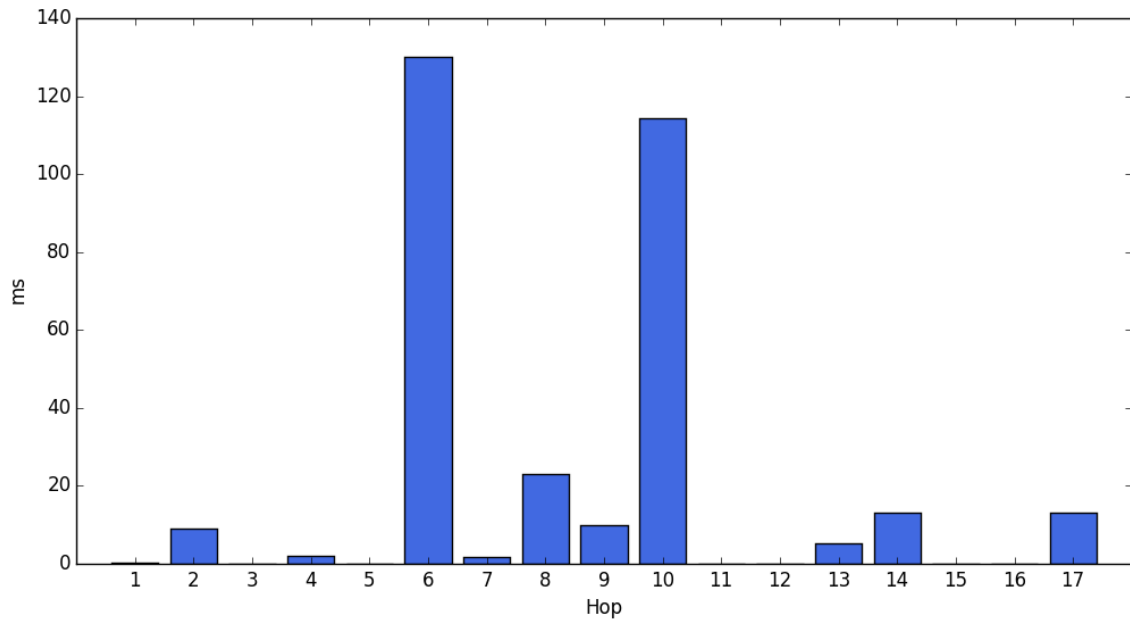


Figura 1: www.u-tokyo.ac.jp - Δ RTT

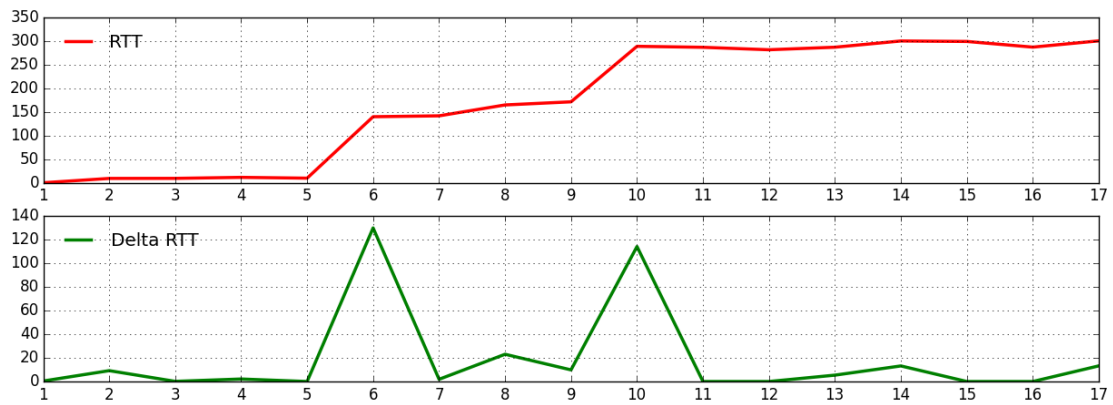


Figura 2: www.u-tokyo.ac.jp - RTT y Δ RTT

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 tiene una distribución 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:

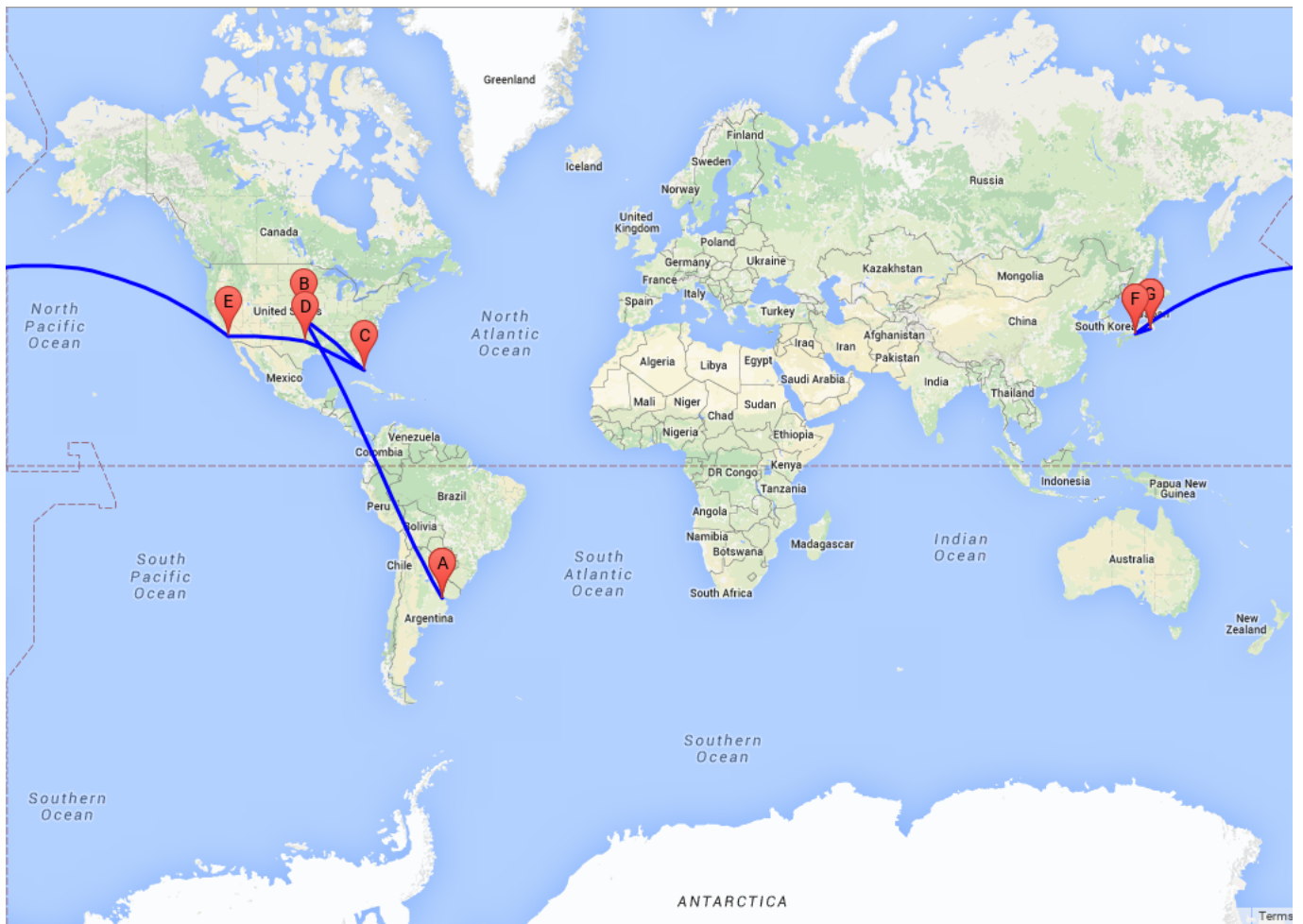
- 64.212.107.98
- 129.250.2.177

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 Londres, Inglaterra a pesar de corresponder a la universidad de la ciudad de Pretoria, Sudafrica. 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	212.73.206.174	292.420	28.952	15.094
10	50.97.19.101	281.778	31.841	0.000
11	50.97.19.41	289.224	33.909	7.446
12	5.10.118.135	278.807	23.145	0.000
13	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 3.2.4 podemos notar que los saltos 6 y 8 sobresalen por sobre el resto en cuanto a sus tiempos de Δ RTT.

3.2.2. RTT y Δ RTT

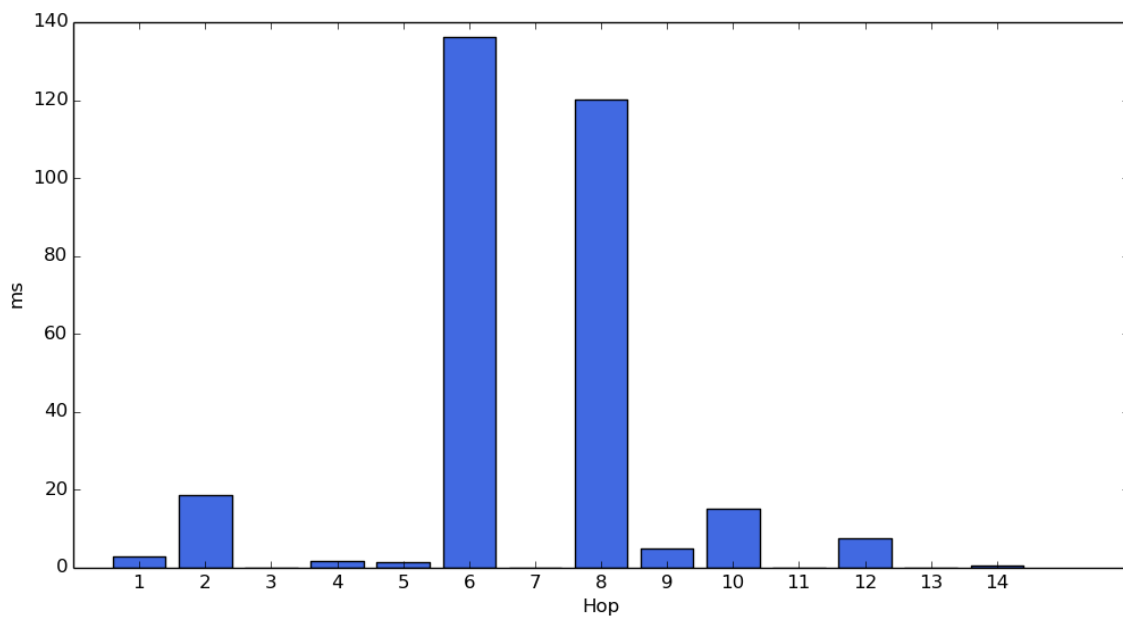
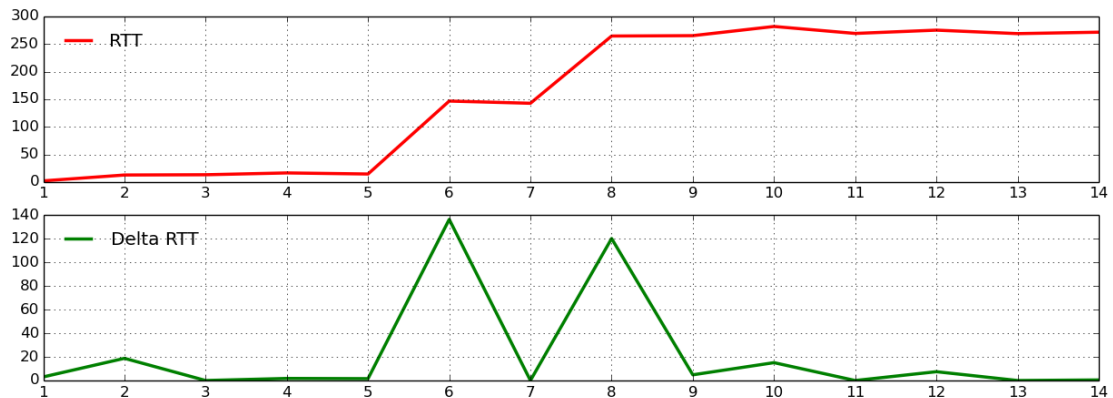


Figura 4: www.up.ac.za - Δ RTT

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 3.2.4. Esto es que tanto los saltos 6y 8 se destacan por sobre el resto. En caso de existir algún enlace submarino seguramente este se correspondería con alguno de estos dos últimos saltos nombrados.

3.2.3. Test de Grubbs

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

- **z-score: 16.044**
- **p-value: 0.033**

De los resultados obtenidos deducimos entonces que la distribución de los Δ RTT 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:

- 67.17.75.66
- 4.69.168.11
- 10.19.0.1
- 212.73.206.174

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	Buenos Aires, Argentina
5	208.178.195.213	xe-0-3-1.ar3.eze1.gblx.net	Buenos Aires, Argentina
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	212.73.206.174	unknown.Level3.net	Londres, Inglaterra
10	50.97.19.101	ae1.bbr02.tg01.lon01.networklayer.com	Londres, Inglaterra
11	50.97.19.41	ae6.dar01.lon02.networklayer.com	Londres, Inglaterra
12	5.10.118.135	po1.fcr01b.lon02.networklayer.com	Londres, Inglaterra
13	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

Se presenta a continuación el mapa 6 en los cuales se puede ver reflejada la información indicada en la tabla

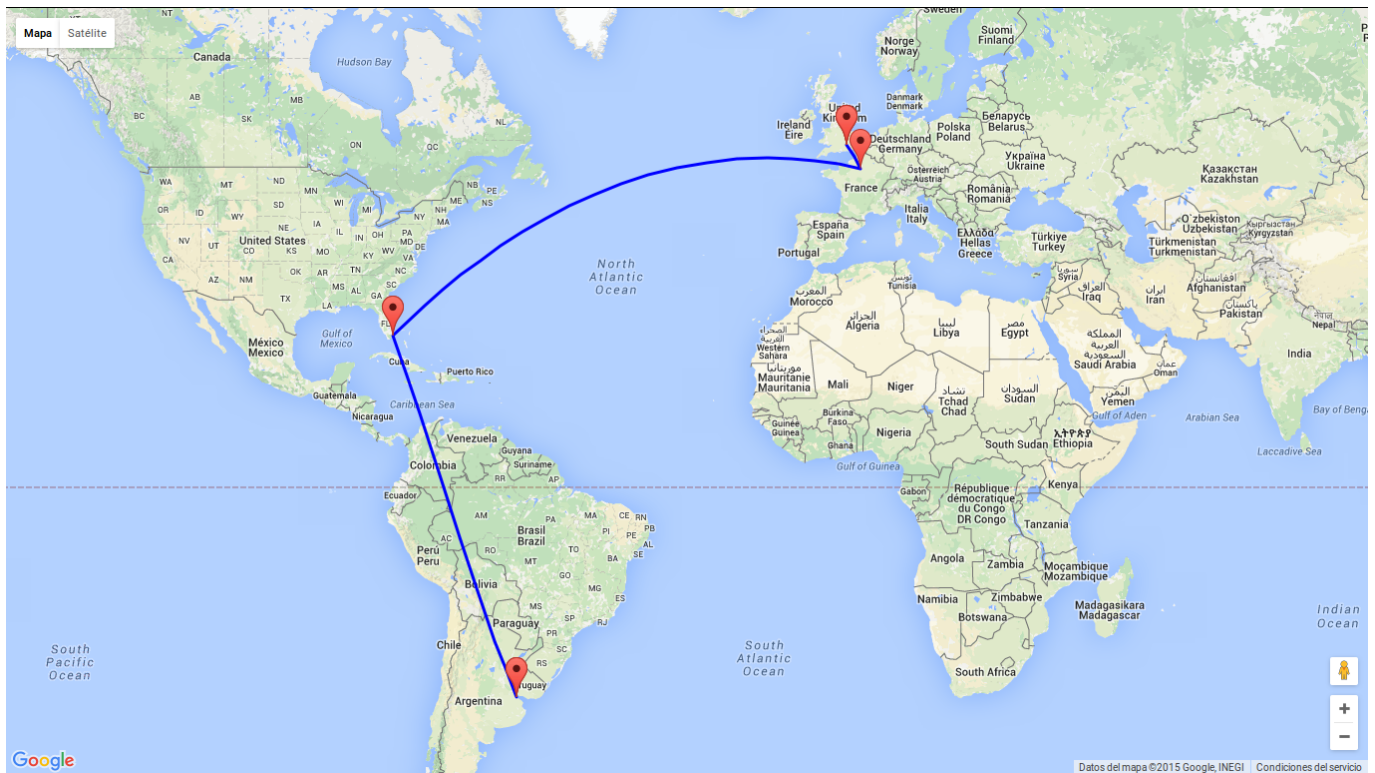


Figura 6: www.up.ac.za - Traceroute

3.3. Universidad de Málaga

El host de destino de la universidad de Málaga sera el dominio “www.uma.es” cuya IP es “150.214.40.97”. El host de la universidad de Málaga se encuentra ubicado en la ciudad de Málaga, España. El origen sera un host ubicado en Nueva York, Usa utilizando como ISP a Digital Ocean Inc.

3.3.1. Datos

Los datos obtenidos para este caso fueron los siguientes:

TTL	IP	E(RTT) (ms)	S(RTT) (ms)	Δ RTT (ms)
1	45.55.128.253	13.816	16.728	13.816
2	162.243.188.221	0.722	2.366	0.000
3	62.115.45.9	1.729	3.298	1.007
4	154.54.11.109	1.967	0.282	0.237
5	154.54.47.29	1.895	0.254	0.000
6	154.54.31.190	74.812	0.185	72.917
7	130.117.50.78	100.630	0.541	25.818
8	130.117.50.26	110.259	0.347	9.629
9	130.117.0.118	95.341	0.390	0.000
10	149.11.68.50	100.158	16.421	4.817
11	130.206.245.38	124.906	5.886	24.748
12	130.206.194.2	109.992	8.925	0.000
13	150.214.231.2	112.184	7.347	2.192
14	150.214.231.170	115.863	0.639	3.679
15	150.214.40.97	110.658	0.106	0.000

Cuadro 5: \overline{RTT} , σ RTT y Δ RTT para la ruta utilizada para llegar www.uma.es

Analizando la información aportada por la tabla 6 podemos notar que el salto 6 sobresale por sobre el resto en cuanto a sus tiempos de Δ RTT.

3.3.2. RTT y Δ RTT

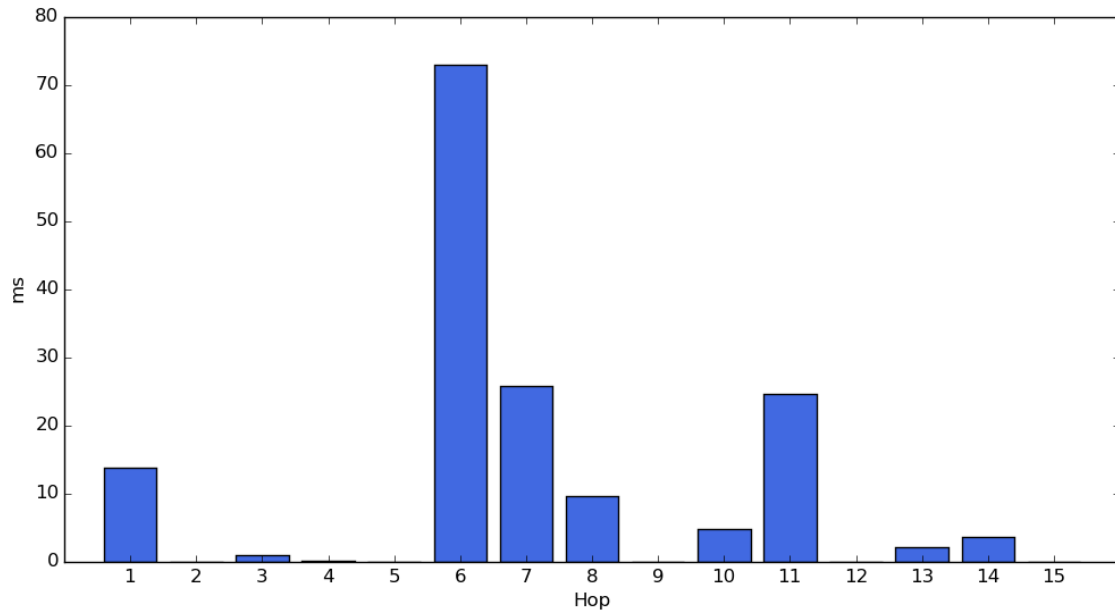


Figura 7: www.uma.es - Δ RTT

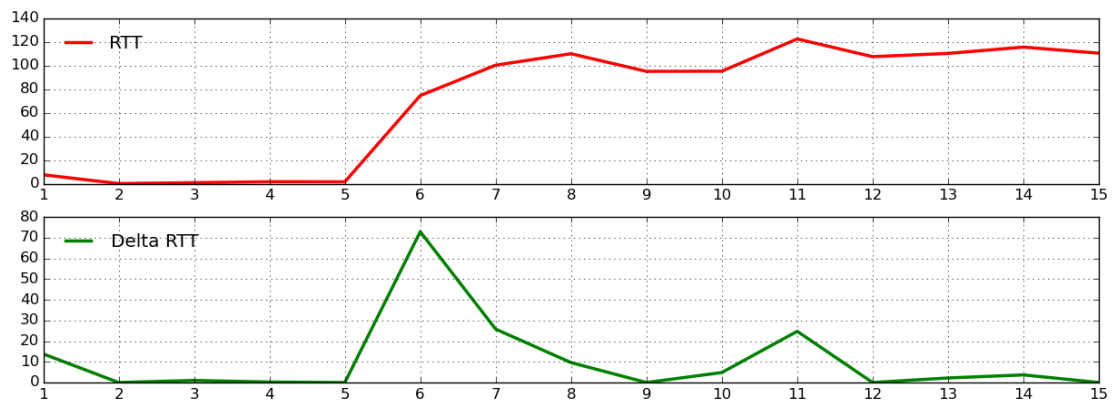


Figura 8: www.uma.es - RTT y Δ RTT

Tanto en la figura 7 como en la figura 8 podemos comprobar los que habíamos notado en la tabla 6. El salto 6 se destaca sobre el resto. Es probable que exista un enlace submarino utilizado para ir de América a Europa en ese salto. Esto lo analizaremos en las siguientes secciones.

3.3.3. Test de Grubbs

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

- **z-score: 26.158**
- **p-value: 0.000**

De los resultados obtenidos deducimos entonces que la distribución de los ΔRTT no tiene una distribución 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:

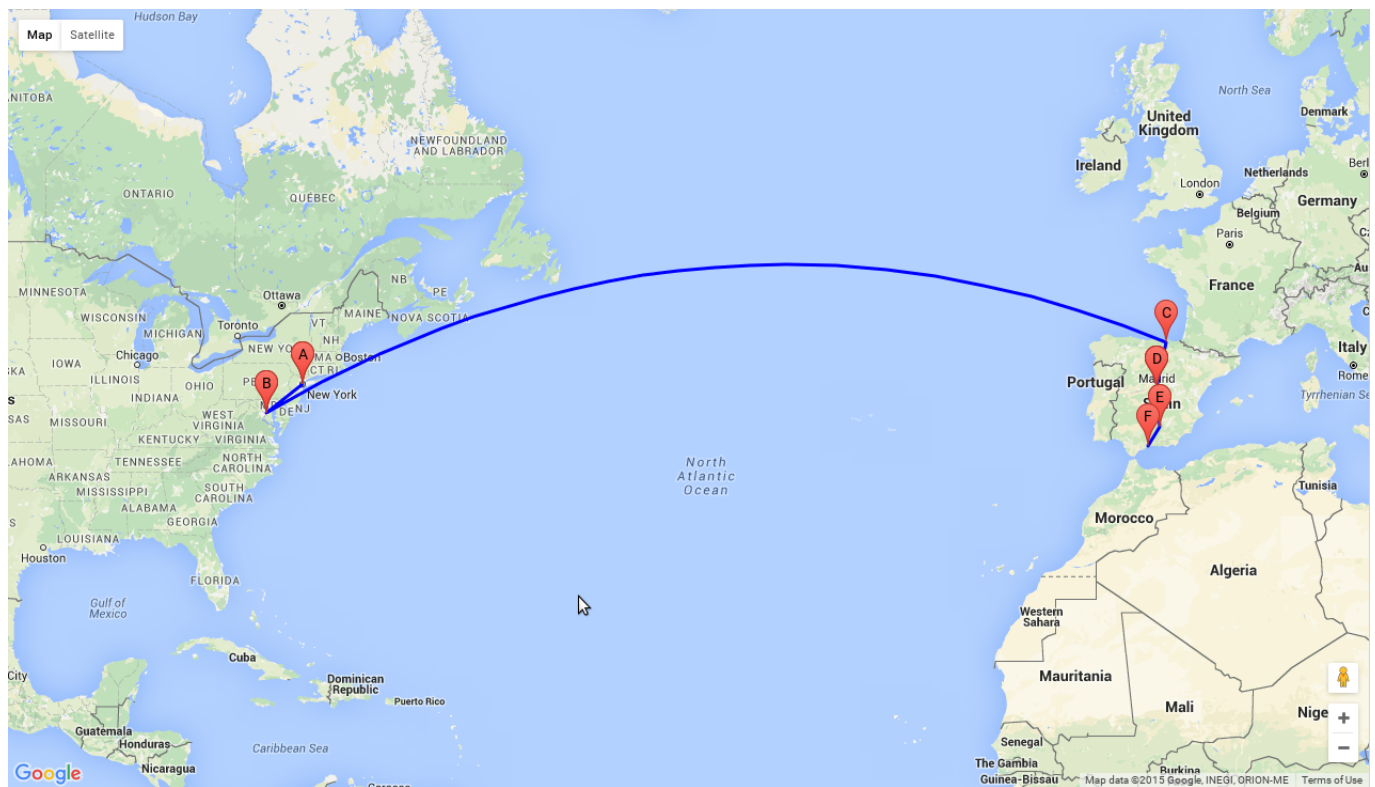
- 154.54.31.190

3.3.4. Geolocalización

TTL	IP	DNS	Ubicación
1	45.55.128.253	no disponible	United States, New York
2	162.243.188.221	no disponible	United States, New York
3	62.115.45.9	nyk-b3-link.telia.net	United States, New York
4	154.54.11.109	be1299.ccr21.jfk04.atlas.cogentco.com	United States, Washington
5	154.54.47.29	be2325.ccr42.jfk02.atlas.cogentco.com	United States, Washington
6	154.54.31.190	be2747.ccr42.par01.atlas.cogentco.com	United States, Washington
7	130.117.50.78	be2423.ccr22.bio02.atlas.cogentco.com	Spain, Bilbao
8	130.117.50.26	be2293.ccr22.mad05.atlas.cogentco.com	Spain, Madrid
9	130.117.0.118	te0-0-2-0.rcr11.b015537-1.mad05.atlas.cogentco.com	Spain, Madrid
10	149.11.68.50	no disponible	Spain, Madrid
11	130.206.245.38	ciemat.ae1.cica.rt1.and.red.rediris.es	Spain, Madrid
12	130.206.194.2	cica-router.red.rediris.es	Spain, Madrid
13	150.214.231.2	xe-0-0-0.malaga01.red.cica.es	Spain, Andalucía, Baeza
14	150.214.231.170	uma-router.red.cica.es	Spain, Andalucía, Baeza
15	150.214.40.97	www.uma.es	Spain, Andalucía, Málaga

Cuadro 6: Ruta utilizada para llegar www.uma.es con la ubicación de los diferentes saltos por los que se pasa. Se encuentra resaltado el salto distinguido calculado en la sección 3.3.3

En la tabla 6 notamos que el salto 6 figura ubicado en Washington, Estados Unidos siendo correctamente el distinguido ya que el siguiente salto figura situado en Europa. En el mapa 9 se puede apreciar el enlace intercontinental. Los saltos 6 y 7 aparecen en el mapa con el nombre de “B” y “C” respectivamente.

Figura 9: www.uma.es - Traceroute

3.4. Universidad MIT

El host de destino fue la universidad M.I.T cuyo dominio es “web.mit.edu” con dirección ip “23.3.254.242”. El server que contiene el sitio se encuentra en Boston, EEUU. El traceroute se originó en Buenos Aires.

3.4.1. Datos

Los datos obtenidos para este caso fueron los siguientes:

TTL	IP	E(RTT) (ms)	S(RTT) (ms)	Δ RTT (ms)
1	36.6.64.1	16.857	19.297	16.857
2	190.220.185.65	14.007	8.700	0.000
3	10.2.8.205	16.958	17.230	2.951
4	10.2.11.217	19.137	13.277	2.179
5	10.2.11.217	18.659	15.835	0.000
6	10.2.11.229	17.837	10.482	0.000
7	10.2.11.229	18.594	11.833	0.758
8	208.48.239.69	155.411	63.920	136.817
9	4.69.207.38	143.480	7.582	0.000
10	4.69.132.114	175.854	17.489	32.374
11	4.69.140.133	175.043	15.968	0.000
12	4.69.151.161	173.678	21.824	0.000
13	4.69.145.209	172.987	14.266	0.000
14	4.59.36.26	175.472	15.564	2.485
15	94.142.125.70	208.940	20.446	33.468
16	94.142.124.33	303.767	24.269	94.828
17	5.53.1.26	302.054	23.695	0.000
18	120	0.000	0.000	0.000
19	186.148.62.33	303.300	17.808	303.300
20	186.148.62.34	349.613	63.907	46.313
21	23.3.254.242	303.657	18.741	0.000

Cuadro 7: \overline{RTT} , σ RTT y Δ RTT para la ruta utilizada para llegar a web.mit.edu

3.4.2. RTT y Δ RTT

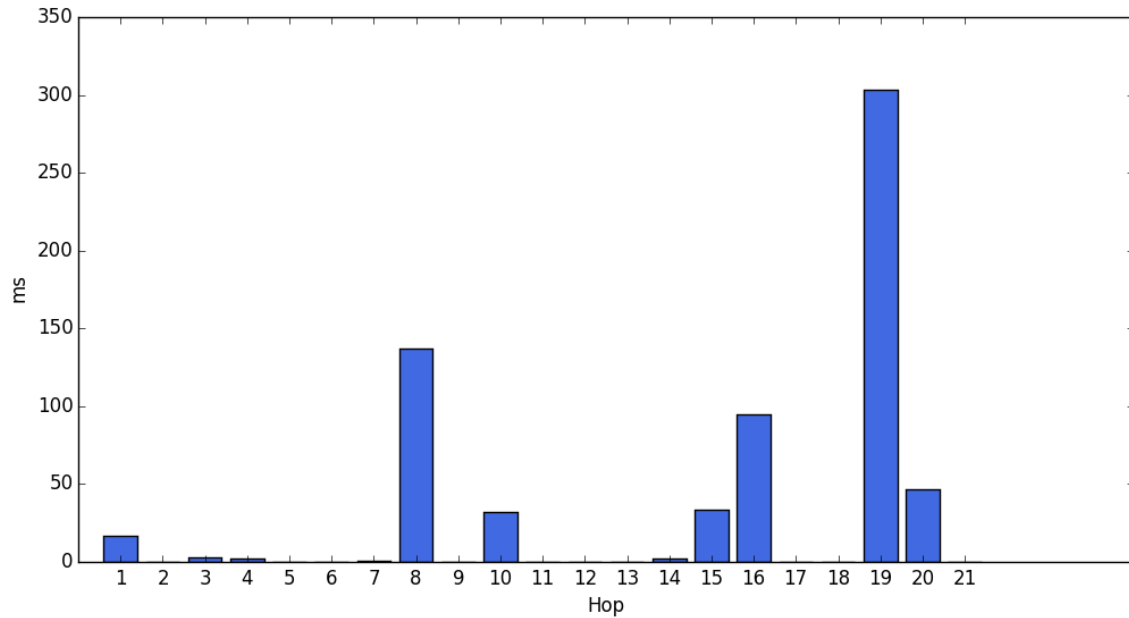


Figura 10: web.mit.edu - Δ RTT

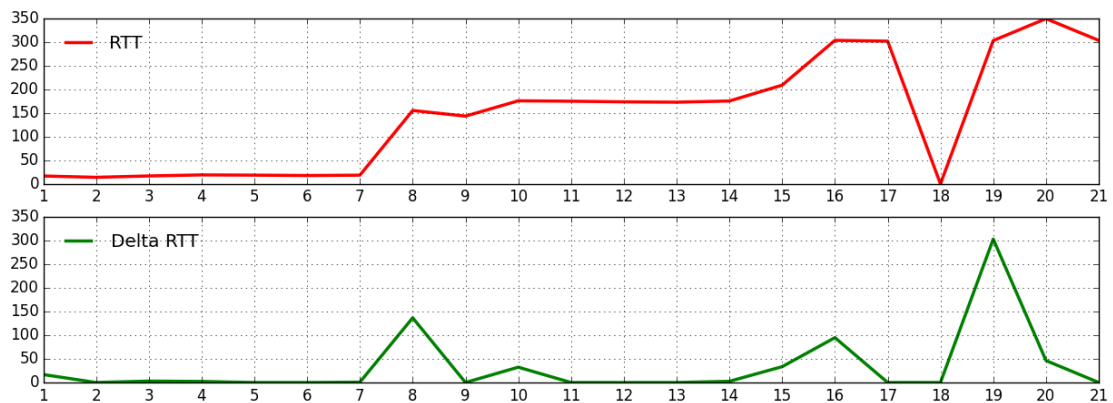


Figura 11: web.mit.edu - RTT y Δ RTT

Podemos ver en las figuras 8, 10 y en el cuadro 11 que el Δ RTT correspondiente a los *TTL* 8, 16, 19 y en menor medida 21, son mas grande que el resto. En las siguientes secciones se analizará si estos corresponden a transmisiones por enlaces submarinos.

3.4.3. Test de Grubbs

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

- **z-score: 35.795**
- **p-value: 0.000**

De los resultados obtenidos deducimos entonces que la distribución de los Δ RTT no tiene una distribución 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:

- 186.148.62.33
- 208.48.239.69
- 94.142.124.33
- 186.148.62.34

3.4.4. Geolocalización

TTL	IP	DNS	Ubicación
1	36.6.64.1	no disponible	China, Hefei
2	190.220.185.65	no disponible	Argentina, Berazategui
3	10.2.8.205	no disponible	no disponible
4	10.2.11.217	no disponible	no disponible
5	10.2.11.217	no disponible	no disponible
6	10.2.11.229	no disponible	no disponible
7	10.2.11.229	no disponible	no disponible
8	208.48.239.69	7-2-34.ear4.Miami2.Level3.net	United States, Lawrenceville
9	4.69.207.38	no disponible	United States, Kansas
10	4.69.132.114	no disponible	United States, Kansas
11	4.69.140.133	ae-2-2.ebr1.Dallas1.Level3.net	United States, Hialeah
12	4.69.151.161	ae-91-91.csw4.Dallas1.Level3.net	United States, Dallas
13	4.69.145.209	ae-4-90.edge5.Dallas3.Level3.net	United States, Dallas
14	4.59.36.26	TELEFONICA.edge5.Dallas3.Level3.net	United States, Kansas
15	94.142.125.70	no disponible	España
16	94.142.124.33	no disponible	España
17	5.53.1.26	no disponible	España
18	*	no disponible	no disponible
19	186.148.62.33	akamai.Vl366.lflo.internacional.pe.nap.movistar.cl	Chile, Santiago
20	186.148.62.34	akamai.Vl366.lflo.internacional.ce.nap.movistar.cl	Chile, Santiago
21	23.3.254.242	242.deploy.static.akamaitechnologies.com	Chile

Cuadro 8: Ruta utilizada para llegar web.mit.edu con la ubicación de los diferentes saltos por los que se pasa. Se encuentran resaltados los saltos correspondientes a outliers encontrados con el test de Grubb

En el cuadro 8 se observa que los saltos distinguidos corresponden a enlaces submarinos. Podemos notar que el primer salto ocurre a un servidor que nuestras herramientas de geolocalización sitúan

en China, pero si notamos el rtt hacia el mismo, es probable que la localización sea errónea. Luego de investigar esa ip, nos dimos cuenta que, realizando traceroutes hacia servidores que se encuentran en Argentina, la ip 36.6.64.1 aparece igualmente, lo que, aunque no es imposible, tiene poco sentido si el servidor realmente se encuentra en China.

Teniendo en cuenta esto, el rtt bajo y el hecho de que rutas hacia servidores en argentina también pasan por dicha ip, creemos que el servidor correspondiente pertenece a alguna red interna del ISP (Claro en este caso), posiblemente con alguna mala configuración. Otro dato raro, en comparación con las demás rutas, es la cantidad de ip privadas que aparecen en las rutas. Estas direcciones ip privadas son conexiones entre routers configuradas como redes privadas, configuradas de esa manera por el ISP. Podemos notar que la ruta pareciera ser muy indirecta, teniendo como destino un servidor localizado en Chile, país limítrofe con Argentina, pero ruteando los paquetes usando conexiones submarinas, pasando por EEUU y España.

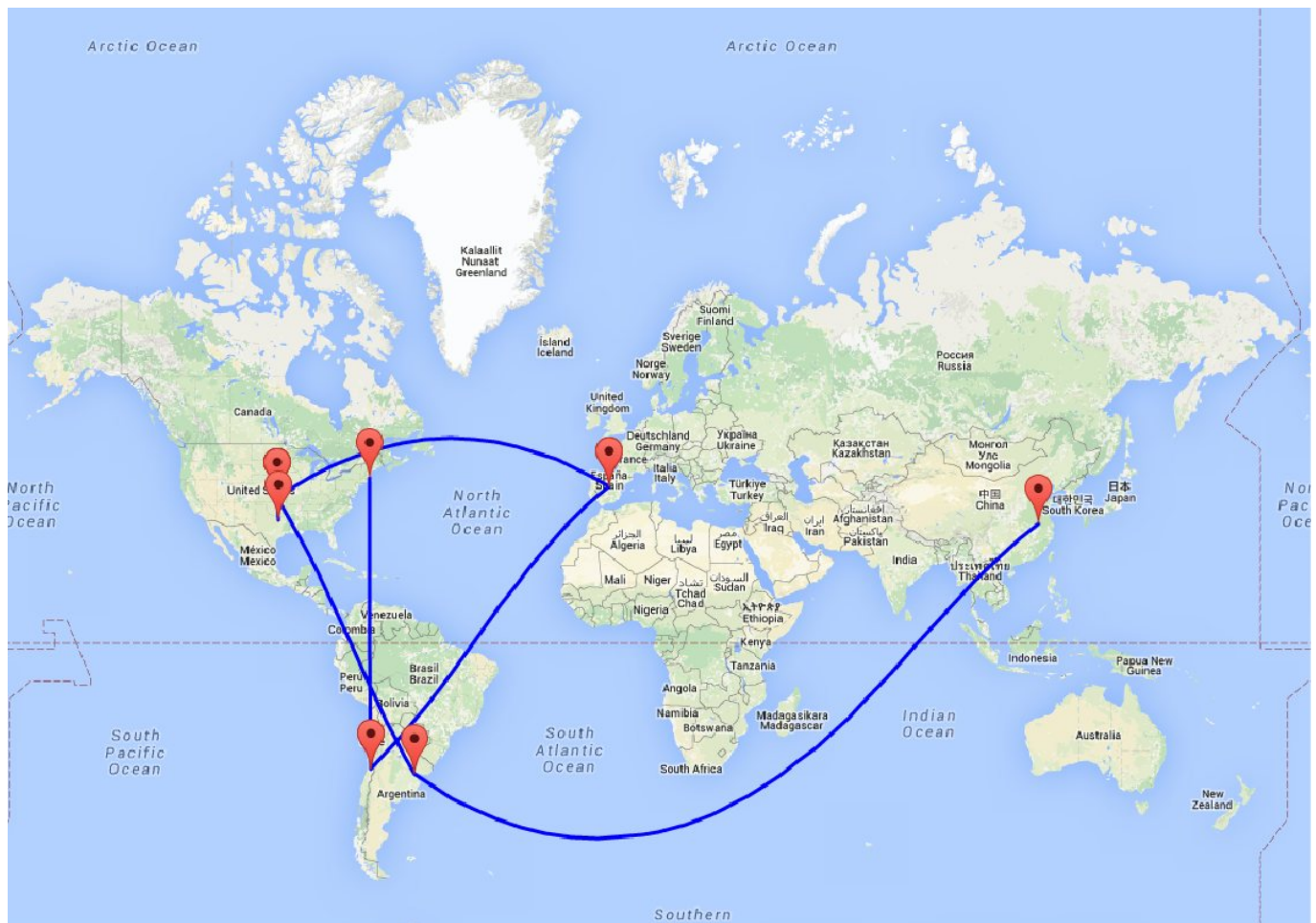


Figura 12: web.mit.edu - Traceroute

Vemos, nuevamente, en la figura 12 que los outliers encontrados corresponden a enlaces submarinos.

4. Conclusiones

Tras haber corrido los distintos test sobre los host bajo estudio notamos que no obtuvimos variaciones en las rutas utilizadas por los paquetes, sino que generalmente se mantuvieron las mismas rutas entre las distintas corridas. Notamos también que la información provista por los servicios de geolocalización en muchos casos no se corresponde con la localización física del router.

En cuanto a la localización de enlaces submarinos mediante el test de hipótesis realizado en algunos casos detecto correctamente los mismos pero otros como ser el caso de la universidad de Pretoria si bien detecto los enlaces submarinos de forma correcta también arrojó otros outliers que no se corresponden con enlaces submarinos. En vista de estos resultados concluimos que el uso de esta herramienta no sería viable para la detección de los enlaces submarinos, si podría utilizarse para acotar los posibles candidatos pero deberíamos utilizar alguna otra herramienta como apoyo para evitar estos falso positivos.

Otra particularidad que notamos es que muchos routers asignan una menor prioridad a los paquetes "ICMP" lo que origina que varios saltos tuviesen ΔRTT negativos.

A continuación expondremos las particularidades de cada caso de estudio:

4.1. Universidad de Tokyo

Para este caso de estudio mas allá del error informado por los servicios de geolocalización para el salto 10 de la tabla de la figura 2, tanto los valores de RTT obtenidos como los outliers detectados por el test de Grubbs parecen tener correspondencia con lo realmente acontecido.

Si bien los ΔRTT obtenidos parecen no seguir una distribución normal los outliers obtenidos mediante el test de Grubbs para detectar los enlaces submarinos parecen ser los correctos y coinciden con lo que se puede apreciar en los gráficos de la figura 1 y la figura 2.

4.2. Universidad de Pretoria

Este caso de estudio se eligió originalmente para obtener la ruta a un continente diferente a los otros casos elegidos, pero al realizar las tareas de geolocalización nos encontramos con que el servidor de esta universidad sudafricana se encuentra en Inglaterra. Aún así se decidió no cambiar el caso dado que el correspondiente a España tiene un origen diferente, lo que nos permite ver la diferencia entre ambas rutas que tienen un destino cercano.

En este caso de estudio se puede ver que con el test de Grubbs se detectaron cuatro outliers, pero siendo dos de ellos falsos positivos como se pueden ver que son el salto 2 y el 9, lo cual se puede ver claramente en los gráficos de la figura 4 y la figura 5. Aún así devolvió correctamente los correspondientes a enlaces submarinos entre Buenos Aires y Miami, y entre Miami y París.

4.3. Universidad de Málaga

Este caso a diferencia de los otros el trace tiene un origen diferente (USA) quizás por eso la ruta parece más directa. Si bien la distribución según el test no es normal, al localizar los outliers con el test de Grubbs se pudo encontrar el único enlace continental en dicho path. Esto quedo claramente evidenciado en la figura 7 y la figura 8. Otro detalle menor es que los RTT son bastante más chicos comparados con los de los otros traces, esto quizás se deba a que es otro ISP en otro país.

4.4. Universidad MIT

La herramienta implementada detectó correctamente outliers en los tiempos de las rutas. y como se comentó anteriorente, estos correspondieron a enlaces submarinos. En cuanto a la ruta tomada por los paquetes enviados hacia el servidor con la página del MIT, podemos notar que la misma no es muy directa, saltando de servidores en EEUU hacia España, luego pasando por Chile para llegar nuevamente hacia EEUU.