Traceroute

22 de octubre de 2014

Universidad de Buenos Aires - Departamento de Computación - FCEN

Integrantes:

- Gallardo, Guillermo L.U.: 32/10 gagdiez.c@gmail.com
- Fixman, Martin L.U.: 391/11 martinfixman@gmail.com
- Matayoshi, Leandro L.U.: 79/11 leandro.matayoshi@gmail.com
- Szyrej, Alexander L.U.: 642/11 alexander.szyrej@gmail.com

Índice

1. Introducción

1.1. Objetivos generales

ICMP es el módulo del protocolo TCP/IP que se encarga de proveer mensajes de error y de control cuando se produce alguna anormalidad en el envío de un datagrama IP. Existen distintas herramientas que se apoyan sobre este módulo para obtener información acerca del estado de las rutas que debe atravesar un paquete para llegar al destino, como por ejemplo, el valor del RTT (round-trip-time) entre 2 hosts. Entre estas herramientas se destacan los comandos *ping* y *traceroute*.

El objetivo de este trabájo práctico es realizar nuestra propia implementación de *traceroute* y utilizar la misma para comprender el funcionamiento de las comunicaciones a larga distancia sobre internet. Para esto último realizaremos un análisis de la distribución geográfica del conjunto de enlaces y routers atravesados por los paquetes ICMP. A su vez intentaremos detectar cuando dichos paquetes atraviesan enlaces intercontinentals utilizando solamente los valores de los RTT.

Por todos estos motivos, los hosts destino de los paquetes son cuatro universidades ubicadas en otros continentes, las mismas son:

- **Oxford** University of Oxford, Londres, Reino Unido
- **MSU** Московский государственный университет (Universidad Estatal de Moscú), Moscú, Federación Rusa
- **Queensland** University of Queensland, Queensland, Australia
- **Tsinghua** 清华大学 (Universidad de Tsinghua), Beijing, República Popular China

1.2. Tipos de mensajes ICMP

Los mensajes de ICMP se transmiten en forma de datagramas. El emisor puede ser tanto un host como router, y el destino es siempre la dirección source del datagrama IP que motivó el mensaje.

Entre los tipos de mensajes de error más comunes se destacan:

- Echo reply: Respuesta a echo request. Los datos recibidos por el request deben ser incluídos en el mensaje. type: 0
- Destination host unreachable: El router no encuentra en su tabla una dirección a la cual forwardear el paquete. type: 3
- Redirect: El router que recibe el paquete detecta que otro router ofrece un camino más efectivo para forwardear el paquete. type: 5
- Echo request: Se espera que los datos enviados sean recibidos nuevamente en un mensaje echo reply. type: 8
- Time exceeded: Mensaje generado por un router para indicarle al host emisor de un datagrama que su TTL ("Time to live") ha alcanzado el valor 0.

1.3. Ping

El comando ping es una tool que permite testear la actividad de un host dentro del protocolo IP y medir el RTT entre el dispositivo que ha ejecutado el comando y el host de interés. El mismo se basa en la emisión de mensajes *echo request*, y sus respectivas respuestas *echo reply*. El RTT queda determinado entonces por el tiempo que tarda el host emisor en recibir la respuesta. Los requests para los cuales no se recibe ninguna respuesta son registrados como paquetes perdidos.

1.4. Traceroute

A diferencia de ping, *traceroute* provee información acerca de la ruta que siguen los datagramas para arribar al destino. Esta herramienta arma un registro ordenado con los routers que ha atravesado el paquete, junto con el valor de los RTT para cada uno de ellos. En la siguiente sección explicaremos el mecanismo de esta herramienta con mayor detalle.

2. Desarrollo

2.1. Implementando traceroute

Como dijimos anteriormente, *traceroute* es una herramienta de dignóstico que se utiliza para hacer un análisis del estado de la conexión entre 2 hosts comunicados a través del protocolo TCP/IP. Este comando pone especial énfasis en los distintos tramos (determinados por los hops entre routers) que va debe atravesar el paquete para llegar a destino. Mediante este tipo de análisis es posible obtener información de gran interés, como por ejemplo identificar los enlaces con mayor RTT (determinantes en el cálculo del RTT "global", entre el host origen y el destino). De esta manera es posible caracterizar los distintos enlaces: RTT's altos pueden corresponderse a enlaces submarinos o terrestres de largas distancias, o enlaces con poca velocidad de transmisión.

La idea básica del algoritmo consiste en enviar paquetes con TTL's incrementales hacia el nodo destino y obtener información en función de los datagramas ICMP obtenidos, tal como muestra el siguiente diagrama:

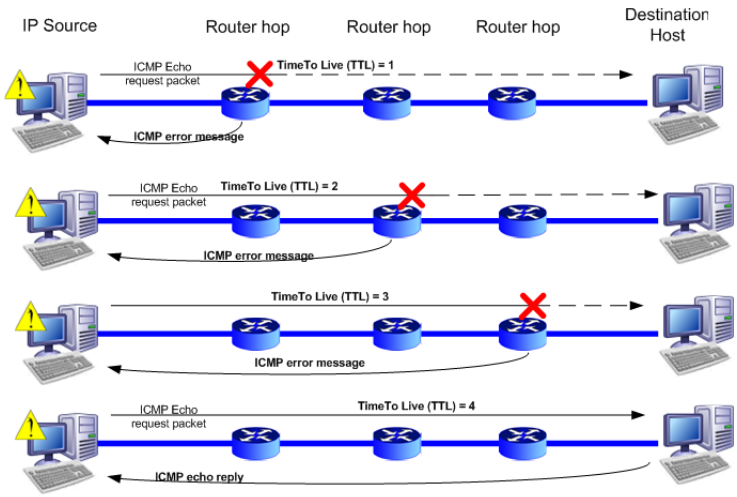

Figura 1: Mecanismo de acción de traceroute

Cada vez que un paquete es forwardeado hacia un router, el valor de su TTL se decrementa en una unidad. Cuando un routers advierte que el TTL de un paquete ha alcanzado el valor 0, envía un mensaje ICMP hacia el host fuente del mensaje, de tipo "time exceeded". Conociendo la hora exacta de emisión del paquete original y hora en la cual arriba el mensaje de error es posible determinar el RTT entre el host en el cual se corre el algoritmo y el router generador del paquete ICMP. El algoritmo se extiende a cada uno de los nodos intermedios: En la primera iteración se envía un paquete con valor de TTL 1. Por lo tanto el router a 1 hop de distancia envía un mensaje de error, y el algoritmo puede calcular el RTT entre el origen y dicho router. Generalizando, en la iteración i se envía un paquete con valor de TTL i, y utilizando la información recibida, el algoritmo puede calcular el RTT entre el origen y el router ubicado a i hops. El algoritmo finaliza o bien cuando se recibe una respuesta afirmativa por parte del destino; o bien cuando se alcanza el límite de TTL permitido.

2.1.1. Algunas consideraciones y detalles implementativos

Para implementar el comando utilizamos la librería *Scapy* de Python.

Traceroute por default envía una secuencia de paquetes UDP hacia el nodo destino. Paquetes del estilo TCP SYN también pueden ser usados. En nuestra implementación la alternativa utilizada son los paquetes ICMP de tipo "echo request" . Los mensajes recibidos serán por lo tanto del tipo "time exceeded" para los nodos intermedios y "echo reply" cuando el paquete llega a destino.

La función debe recibir como argumentos el valor de TTL inicial con el que envía el primer paquete y el máximo de saltos permitidos hasta alcanzar el destino. En nuestro caso utilizamos los valores por defecto: 1 y 30 respectivamente.

Otro de los parámetros que debe especificarse es el número de reintentos que debe realizarse por cada valor de TTL. ICMP, al igual que IP, es una capa "sin garantías" en el envío de mensajes. Los routers hacen el "mejor esfuerzo" para lograr el envío de los paquetes, pero no hay garantías de que los mismos alcancen el destino. Teniendo esto en cuenta, es posible que los mensajes ICMP enviados por los routers no lleguen al emisor. En dicho caso, es deseable que se realice más de un intento para un determinado valor de TTL. Usualmente la mayoría de las implmentaciones utilizan 2 o 3 como valor. En nuestro caso decidimos realizar 10 intentos por cada TTL. Este valor nos protege contra otro aspecto sensible del algoritmo, descripto a continuación.

Un paquete no llega al mismo destino atravesando siempre las mismas rutas. Los nodos intermedios pueden caerse o levantarse. Determinados enlaces pueden congestionarse o liberarse en distintos momentos. Supongamos que el algoritmo envía hacia el destino un paquete con TTL 10. ¿Qué garantías tenemos de que, en caso de ser necesario un segundo intento porque no ha llegado ningún mensaje de error, el router alcanzado luego del décimo hop sea el mismo? Ninguna. En otras palabras, dependiendo la ruta que siga el datagrama, el router alcanzado luego del décimo hop será uno u otro. Para tener cierto control respecto a esta situación, por cada valor de TTL se envían 10 paquetes y se guardan todas las direcciones de IP que han respondido los mensajes de error. Luego, el algoritmo selecciona aquella dirección que ha respondido más veces.

Finalmente, el valor de RTT entre el host que corre el *traceroute* y el router a i hops de distancia es calculado como el promedio de los valores obtenidos por cada intento.

2.2. Estimando Enlaces Intercontinentals

Recordando algunas fórmulas pertenecientes a la capa de enlace, sabemos que el delay está determinado por la siguiente ecuación:

$delay[seg] = T_{tx} + T_{prop}$, donde T_{tx} es el tiempo de transmisión determinado principalmente por la capacidad del canal y la relación señal ruido dentro del mismo, y el tiempo de propagación está determinado por:

$T_{prop} = \frac{D}{V}$, con D la distancia del enlace y V la velocidad de propagación de la forma de onda en el medio físico.

El RTT equivale a $2 * delay$.

Si analizamos exclusivamente la capa de enlace punto a punto del modelo de capas de Internet, podemos llegar a la conclusión de que el factor de mayor peso en el cálculo del RTT es la distancia del enlace. Dado que se envía un único datagrama con una cantidad despreciable de datos de test (caracteres ASCII pertenecientes al "echo request"), el tiempo de transmisión del mismo dentro del enlace es ínfimo (independientemente de la velocidad de transmisión de dicho enlace). Por lo tanto, desde este punto de vista es lógico pensar que los resultados con mayor valor de RTT corresponderán a enlaces submarinos. Suponemos que el tiempo que le toma a un paquete ir de un nodo a otro por tierra es significativamente menor al que le toma atravesar un enlace intercontinental, ya que estos últimos cubren distancias mucho mayores.

Sin embargo, la capa de nivel 1 no es la única que debemos tener en cuenta a la hora de realizar el análisis. Podría suceder que por algún motivo (congestión, por ejemplo), el paquete sea almacenado temporalmente en un buffer antes de ser forwardeado hacia el próximo router. O que algún conflicto de índole similar suceda a nivel Ethernet. Por lo tanto, estos factores pueden influir en un resultado con RTT alto sin que el router involucrado provenga necesariamente de un enlace submarino.

El *zscore* es una medida que nos permite medir el peso de un hop respecto a los demás. (En particular, respecto a la media de todos los hops de la ruta, y considerando también el desvío standard de los datos). La fórmula utilizada para calcularlo es:

$ZRTT_i = \frac{RTT_i - RTT_{mean}}{SRTT}$

$ZRTT_i$ representa el RTT para el i-ésimo hop. Para calcularlo, obtenemos la distancia en tiempo que hay entre los pares de nodos vecinos y asumimos que los mismos siguen una distribución normal. Finalmente fijamos un umbral de Zscore para determinar los tramos son submarinos.

3. Resultados y análisis

Luego de correr todos los experimentos notamos que la dirección IP de los nodos no necesariamente refleja su posición geográfica real.

Intentamos hacer uso de la herramienta www.geoiptool.com para orientarnos en el curso de las rutas y algunas veces encontrábamos que no tenían sentido las ubicaciones que nos proponía esta herramienta.

Un ejemplo de esto mismo seria:

Host name	***IP***	***RTT(media) ms***
ET6-0-0-0-GRTBUECU1.red.telefonica-wholesale.net	94.142.103.153	30.104

Dicha IP figura en geoiptool como localizada en España. Es decir que de Buenos Aires, la ruta pasará por España antes de llegar a Estados Unidos, todo con un RTT medio de 30ms. Esto no parece para nada razonable, pero el nombre del host nos presenta información que puede contrastar aquella proveída por geoiptool. GRT**BUE**CU1 indicaría que la IP realmente pertenece a Buenos Aires, algo mucho más lógico.

Afortunadamente capturamos los nombres de los hosts en cada salto y la mayoria tiene indicios de ubicación en sus nombres. Claro que no siempre encontramos hosts 'bien nombrados'.

Otro ejemplo podría ser *be2384.ccr21.**lpl**01.atlas.cogentco.com* con el código IATA de Liverpool.

3.1. Moscow State University (Rusia)

3.1.1. Ruta

Ubicación	***IP***	***RTT(media) ms***	***ZScore***	***Tipo***
Buenos Aires	200.51.240.181	31.018	0.220	Continental
Buenos Aires (telefónica)	94.142.103.153	30.104	-0.265	Continental
Miami (telefónica)	94.142.123.22	164.933	1.795	Intercontinental
Dallas (telefónica)	94.142.127.105	199.813	0.278	Continental
Dallas/Ft Worth (cogentco)	154.54.13.225	221.383	0.077	Continental
Dallas/Ft Worth (cogentco)	154.54.7.45	212.266	-0.389	Continental
Kansas (cogentco)	154.54.2.113	214.954	-0.210	Continental
Chicago (cogentco)	154.54.6.86	215.663	-0.240	Continental
Toronto (cogentco)	154.54.27.182	228.466	-0.056	Continental
Montreal (cogentco)	154.54.30.206	226.107	-0.286	Continental
Liverpool (cogentco)	154.54.44.138	294.383	0.785	Continental
Amsterdam (cogentco)	154.54.77.245	307.648	-0.049	Continental
Hamburgo (cogentco)	154.54.74.122	264.320	-0.908	Continental
Estocolmo (cogentco)	154.54.63.2	327.827	0.713	Continental
Helsinki (cogentco)	154.54.62.250	332.424	-0.181	Continental
Moscú	149.6.58.42	333.589	-0.233	Continental
Moscú (runnet)	194.85.40.229	525.315	2.658	Intercontinental
Moscú (runnet)	194.190.254.118	357.420	-2.798	Continental
Moscú (runnet)	93.180.0.172	344.003	-0.454	Continental
Moscú	188.44.33.1	346.421	-0.214	Continental
Moscú	188.44.50.103	347.007	-0.242	Continental

Las ciudades fueron atravesadas en el siguiente orden:

Buenos Aires - Miami - Dallas - Kansas - Chicago - Toronto - Montreal - Liverpool - Amsterdam - Hamburg - Stockolm - Helsinki - Moscow

Podemos ver que la ruta pasa de América del Sur (BUE) a América del Norte (MIA), luego de Canada en America del Norte (Montreal) a Europa (Liverpool) y por último llega a Moskú en Asia. En el primero

de los saltos descriptos el ZScore es bastante alto, y por eso figura como intercontinental en la tabla. Luego el segundo salto no es significativo para un umbral de 1.5, si lo será con uno de 0.5. Dentro de los saltos en Moscu obtenemos un ZScore de 2.66 aun no siendo un enlace submarino. Esto puede deberse al entrar en la Russian University Network. ESTO AHORA HAY QUE VERLO BIEN, DEPENDE MUCHO DEL ANALISIS QUE HAGAMOS PARA EL UMBRAL, YA QUE EL TIPO SE CORRESPONDE CON ESO.

Figura 2: Mapa de la ruta atravesada para llegar a la universidad de Rusia

mas analisis y grafico de barra IP zscore + umbral

3.2. Tsinghua

Para el caso de China, la ruta comienza por Estados Unidos como el caso anterior, pero en lugar de cruzar a Europa por el Este, los paquetes viajan por el pacífico. Veamos la siguiente tabla.

Ubicación	***IP***	***RTT(media) ms***	***ZScore***	***Tipo***
Buenos Aires	200.51.240.156	31.907	0.259	Continental
Buenos Aires (telefónica)	84.16.9.233	30.095	-0.437	Continental
Miami (telefónica)	94.142.121.222	165.469	2.396	Intercontinental
Miami (telefónica)	94.142.122.249	165.140	-0.407	Continental
Miami (telefónica)	84.16.12.238	167.934	-0.342	Continental
Miami	63.243.152.45	164.176	-0.478	Continental
Ashburn	66.198.154.177	265.945	1.702	Intercontinental
Dallas	66.198.154.118	254.661	-0.633	Continental
Dallas	66.110.56.6	267.287	-0.139	Continental
Los-Angeles	66.110.57.82	256.103	-0.631	Continental
Los-Angeles	66.110.59.182	257.170	-0.378	Continental
Chongming	101.4.117.213	428.694	3.143	Intercontinental
Chongming	101.4.117.97	428.055	-0.413	Continental
Beijing	101.4.116.146	424.990	-0.463	Continental
Beijing	101.4.118.78	427.001	-0.358	Continental
Beijing	202.112.38.10	425.663	-0.428	Continental
Beijing	118.229.4.66	425.672	-0.400	Continental
Beijing	118.229.4.34	438.217	-0.141	Continental
Beijing	118.229.2.74	430.018	-0.569	Continental
Beijing	118.229.2.69	425.922	-0.485	Continental
Beijing	118.229.8.6	427.147	-0.375	Continental
Beijing (Tsinghua)	166.111.4.100	426.084	-0.422	Continental

Las ciudades fueron atravesadas en el siguiente orden:
Buenos Aires - Miami - Ashburn - Dallas - Los Ángeles - Chongming - Beijing

Podemos destacar tres enlaces que superan el umbral de 1.5. Buenos Aires → Miami; Miami → Ashburn y Los-Angeles → Beijing. De estos tres, el más preocupante es el segundo, puesto que es un enlace continental, dentro de Estados Unidos.

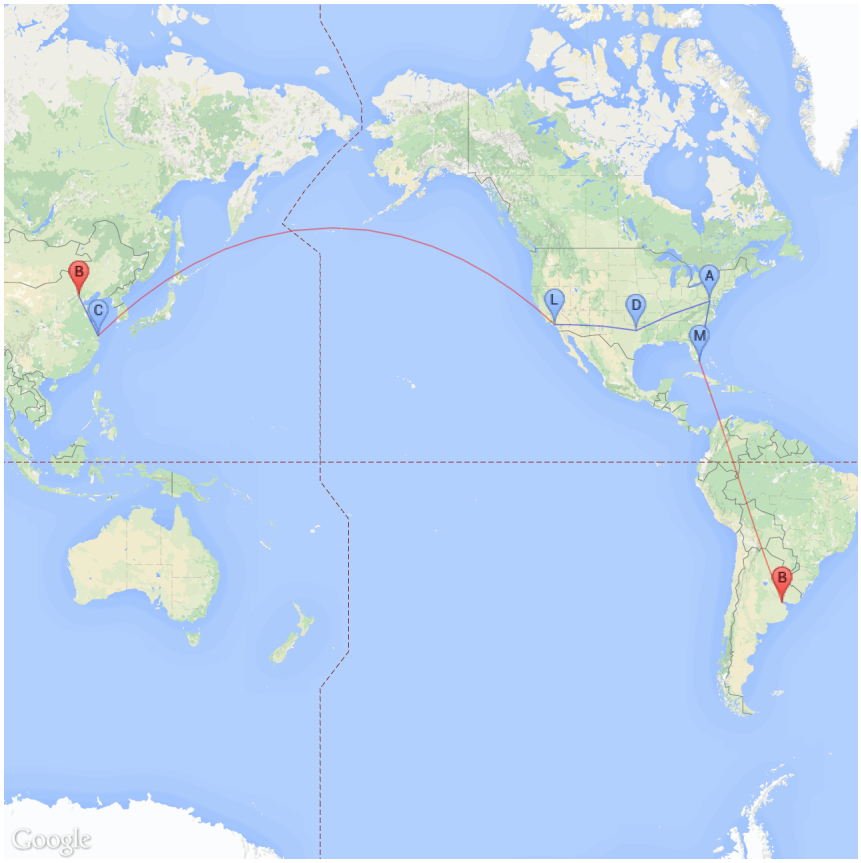

Figura 3: Mapa de la ruta atravesada para llegar a la universidad de China

mas analisis y grafico de barra IP zscore + umbral

3.3. Oxford

Ubicación	*IP*	*RTT(media) ms*	*ZScore*	*Tipo*
Buenos Aires	200.51.240.181	37.154	0.426	Continental
Buenos Aires (telefónica)	84.16.9.233	51.008	-0.009	Continental
Miami (telefónica)	5.53.5.138	210.915	2.722	Intercontinental
Miami (telefónica)	94.142.123.5	174.734	-0.945	Continental
Miami (as6453)	63.243.152.45	175.240	-0.259	Continental
Ashburn (as6453)	66.198.154.177	293.857	1.950	Intercontinental
Ashburn (as6453)	216.6.87.1	286.600	-0.404	Continental
Newark (as6453)	216.6.87.138	277.667	-0.435	Continental
Newark (as6453)	66.198.70.1	307.315	0.286	Continental
Londres (as6453)	66.198.70.26	403.133	1.523	Intercontinental
Londres (as6453)	80.231.130.42	298.757	-2.220	Continental
195.219.100.82	195.219.100.82	285.687	-0.513	Continental
Londres	146.97.33.2	289.063	-0.205	Continental
Londres	146.97.37.206	291.484	-0.223	Continental
Londres	193.63.108.129	281.783	-0.450	Continental
Londres	193.63.108.134	294.226	-0.036	Continental
Londres	193.63.109.114	289.814	-0.351	Continental
Londres	192.76.21.21	280.879	-0.435	Continental
Londres	192.76.22.201	282.251	-0.243	Continental
Londres	192.76.32.66	286.466	-0.190	Continental
Londres	129.67.242.155	301.388	0.011	Continental

Las ciudades fueron atravesadas en el siguiente orden:
Buenos Aires - Miami - Ashburn - Newark - London - Oxford

En este caso destacamos nuevamente tres enlaces que superan el umbral de 1.5. Buenos Aires → Miami; Miami → Ashburn y Newark → Londres. Los dos primeros son identicos al caso anterior, nuevamente preocupa el segundo por las mismas razones.

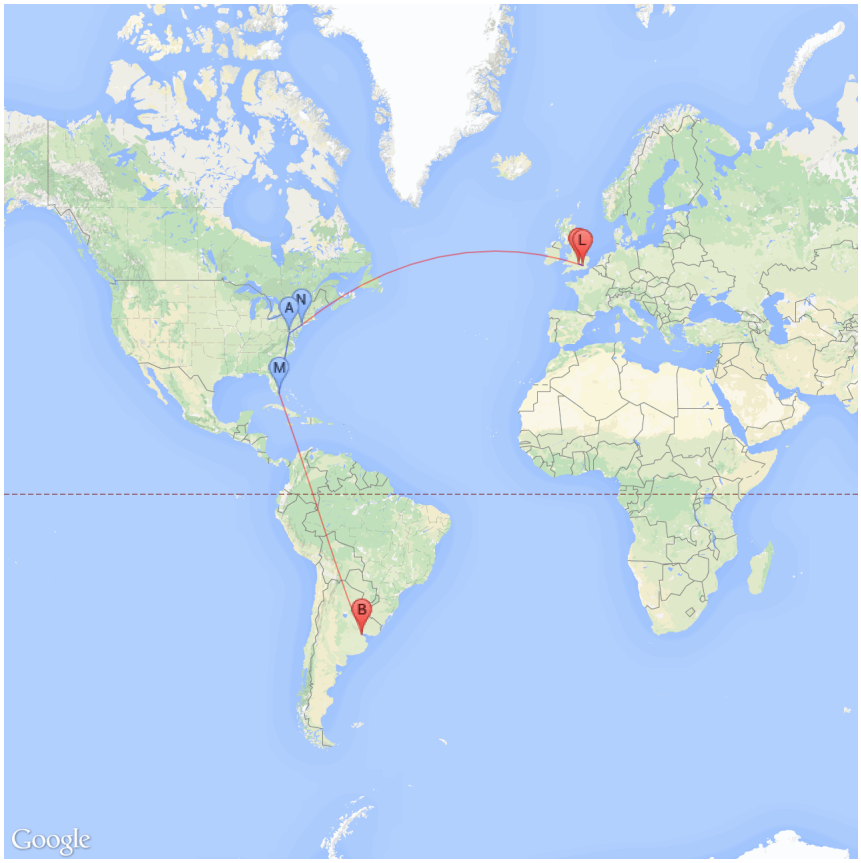

Figura 4: Mapa de la ruta atravesada para llegar a la universidad de Inglaterra

mas analisis y grafico de barra IP zscore + umbral

3.4. Queensland

Ubicación	*IP*	*RTT(media) ms*	*ZScore*	*Tipo*
Buenos Aires	200.51.240.156	31.896	0.110	Continental
Buenos Aires (telefónica)	84.16.9.233	30.748	-0.399	Continental
Miami (telefónica)	94.142.123.14	165.811	1.700	Intercontinental
213.140.49.13	213.140.49.13	230.069	0.609	Continental
xe-3-1-1.mpr1.pao1.us.above.net	64.125.13.113	229.511	-0.390	Continental
208.185.52.74	208.185.52.74	392.486	2.131	Intercontinental
xe-1-2-1.pe2.brwy.nsw.aarnet.net.au	202.158.194.176	391.129	-0.403	Continental
Sydney (aarnet)	113.197.15.57	514.913	1.527	Intercontinental
Brisbane (aarnet)	202.158.194.54	407.555	-2.037	Continental
Brisbane (aarnet)	202.158.194.213	394.376	-0.585	Continental
Queensland (aarnet)	202.158.209.3	394.951	-0.373	Continental
Queensland (aarnet)	113.197.8.34	391.479	-0.435	Continental
Queensland	130.102.159.1	392.041	-0.373	Continental
Queensland	130.102.0.242	401.994	-0.228	Continental
Queensland	130.102.82.28	403.280	-0.362	Continental
Queensland	130.102.131.70	396.128	-0.492	Continental

Las ciudades fueron atravesadas en el siguiente orden:
Buenos Aires - Miami - Hermosa Beach - Sydney - Brisbane - Queensland

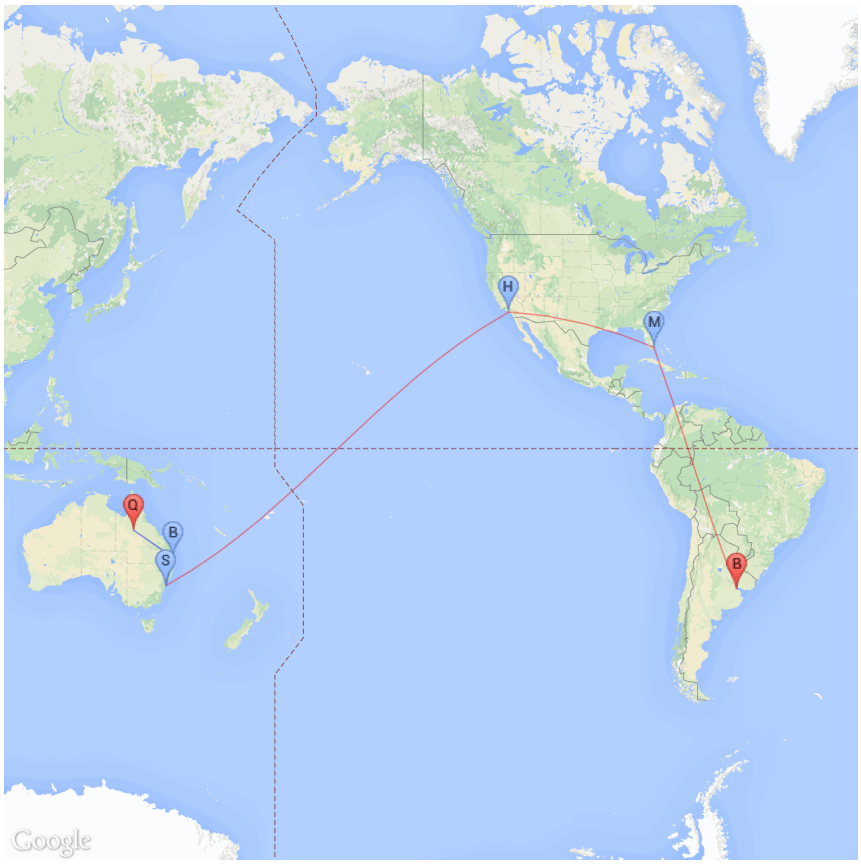

Figura 5: Mapa de la ruta atravesada para llegar a la universidad de Australia

mas analisis y grafico de barra IP zscore + umbral

4. Conclusiones

5. Referencias

- **Computer Networks: A Systems Approach**, *Larry L. Peterson and Bruce S. Davie.*
- **Computer Networks**, *Andrew S. Tanenbaum*
- **http://submarinecablemap.com/**