



DEPARTAMENTO  
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA



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

# Trabajo Práctico 2

Teoría de las Comunicaciones

Primer Cuatrimestre de 2014

Apellido y Nombre	LU	E-mail
Delgado, Alejandro N.	601/11	nahueldelgado@gmail.com
Lovisoló, Leandro	645/11	leandro@leandro.me
Petaccio, Lautaro José	443/11	lausuper@gmail.com

# Índice

<b>1. Introducción</b>	<b>3</b>
<b>2. Desarrollo</b>	<b>3</b>
<b>3. Resultados</b>	<b>5</b>
3.1. University of Oxford . . . . .	5
3.2. The University of Sydney . . . . .	9
3.3. Malaysia University of Science and Technology . . . . .	12
<b>4. Discusión</b>	<b>16</b>
4.1. Primer nodo externo . . . . .	16
4.2. Posible error de localización . . . . .	16
4.3. Promedios de RTT . . . . .	16
4.4. Posibles enlaces submarinos . . . . .	16
4.5. Heurística para detección de enlaces submarino . . . . .	17
<b>5. Conclusión</b>	<b>17</b>

## 1. Introducción

En este trabajo estudiamos un método para detectar enlaces submarinos en la traza de rutas entre dos hosts conectados a internet. Basándonos en estadísticas de las rutas utilizadas, delay y geolocalización, caracterizamos nodos en el recorrido que se muestran distinguidos y planteamos un análisis de los mismos.

La herramienta de traceroute existe en todos los SO modernos, y con la ayuda de la librería ScaPy presentamos una herramienta de traceroute que nos permitió generar experimentos significativos para su posterior análisis.

## 2. Desarrollo

Se implementó una herramienta en lenguaje Python para medir los *round-trip times* (RTT) promedio hacia el host destino y cada hop intermedio durante una cantidad de tiempo determinada por el usuario. La herramienta hace fuerte uso del protocolo ICMP [2] tanto para descubrir la cantidad de hops y los gateways en cada hop hacia el host destino, como para medir los RTT hacia el host destino y cada hop intermedio (de manera similar a las herramientas `traceroute` [3] y `ping` [4], respectivamente.)

La herramienta hace uso la biblioteca Scapy [1] para la creación y comunicación de paquetes ICMP.

Una medición consiste en enviar un paquete ICMP de tipo Echo Request al host destino, asignándole al paquete algún *time-to-live* (TTL) entre 1 y 30 inclusive, y tomar el tiempo que transcurre desde que se envía el paquete hasta que se recibe una respuesta. Las respuestas usualmente son de alguno de los siguientes tipos:

- Un paquete ICMP de tipo Echo Reply en caso que el paquete emitido alcanzara el host destino, ó
- Un paquete ICMP de tipo Time Exceeded en caso que el paquete agotara su TTL antes de llegar al host destino.

Es posible recibir respuestas de otros tipos, como por ejemplo paquetes ICMP de tipo Destination Unreachable en el caso que no se haya podido despachar el paquete a su destino por algún motivo, pero la herramienta ignora cualquier respuesta que no sea de los dos tipos anteriores.

Para medir el RTT hacia el host destino, basta con enviarle un paquete a dicho host con un TTL lo suficientemente grande para asegurar que su TTL no se agote durante el envío del paquete, esperar hasta recibir un paquete ICMP de tipo Echo Reply proveniente del host destino.

Para medir el RTT hacia el  $i$ -ésimo hop en la ruta al host destino, se le asigna al paquete un TTL de valor  $i$ . Esto produce que el paquete agote su TTL al llegar al  $i$ -ésimo host, a lo cual éste responde con un paquete ICMP de tipo Time Exceeded.

Tanto cuando se mide el RTT hacia el host destino o hacia un hop intermedio puede ocurrir que no se reciba ninguna respuesta, por ejemplo cuando el host o algún gateway está detrás de un firewall que bloquea el protocolo ICMP. Para evitar esperar indefinidamente una respuesta, la herramienta espera como máximo un segundo la llegada de una respuesta, y si al cabo de ese tiempo no se recibe una, se descarta esa medición.

Las mediciones se hacen por baches: en un determinado momento se envían 30 paquetes al host destino, uno por cada TTL en el rango mencionado y todos con TTL distinto, y se espera o bien hasta recibir las respuestas de todos los paquetes enviados, o bien hasta que transcurra un segundo y se den por perdidas las mediciones para las que no se recibieron respuestas. A continuación se registra el RTT hacia cada hop computando la diferencia entre el tiempo de recepción de una respuesta y el tiempo de envío del paquete de tipo Echo Request que la originó. Luego de esto se procede al siguiente bache de mediciones, o se finaliza en caso de haber excedido el límite de tiempo de medición determinado por el usuario.

Para poder distinguir qué paquete produjo cada respuesta recibida, la herramienta le asigna un identificador único a cada paquete ICMP de tipo Echo Request emitido usando el campo *Identifier* (ver figura 1.)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31								
Type = 8								Code = 0								Header Checksum																							
Identifier																Sequence Number																							
Datos																																							

Figura 1: Paquete ICMP de tipo Echo Request

En el caso que un paquete ICMP de tipo Echo Request haya llegado al host destino, éste contesta enviando un paquete ICMP de tipo Echo Reply (figura 2.) Este paquete también tiene un campo *Identifier*, que conserva el valor del mismo campo en el paquete ICMP de tipo Echo Request que lo originó.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31								
Type = 0								Code = 0								Header Checksum																							
Identifier																Sequence Number																							
Datos																																							

Figura 2: Paquete ICMP de tipo Echo Reply

Cuando un paquete (no necesariamente ICMP) agota su TTL antes de llegar al host destino, el último gateway al que llegó dicho paquete envía al host origen un paquete ICMP de tipo Time Exceeded (figura 3.) Éste paquete incluye el header IP y los primeros 8 bytes de datos del datagrama que agotó su TTL.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type = 11								Code								Header Checksum															
No utilizado																															
Header IP y los primeros 8 bytes de datos del datagrama original																															
⋮																															

Figura 3: Paquete ICMP de tipo Time Exceeded

En particular, cuando el paquete que agotó su TTL es un paquete ICMP de tipo Echo Request, su header ICMP completo se incluye como parte de los 8 bytes de datos del datagrama original, del cual se puede extraer el valor del campo *Identifier* (ver figura 4.)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type = 11								Code								Header Checksum															
No utilizado																															
Header IP del paquete original																															
Type = 8								Code = 0								Header Checksum															
Identifier																Sequence Number															

Header ICMP  
del paquete  
original

Figura 4: Paquete ICMP de tipo Time Exceeded como respuesta a otro paquete ICMP de tipo Echo Request

### 3. Resultados

#### 3.1. University of Oxford

TTL	IP Addresses	Absolute RTT	Relative RTT	Relative ZRTT	Location
1	192.168.1.1	3.915 ms	3.915 ms	-0.088	*
2	190.194.57.1	164.263 ms	160.347 ms	2.231	Avellaneda, Argentina
5	200.89.166.105	44.386 ms	-119.877 ms	-1.554	Argentina
6	200.89.165.197	44.233 ms	-0.153 ms	0.063	Argentina
9	200.89.164.213	43.083 ms	-1.150 ms	0.050	Argentina
10	200.89.165.222	42.798 ms	-0.284 ms	0.062	Argentina
11	208.178.244.125	42.155 ms	-0.644 ms	0.057	United States
12	67.16.134.218	234.253 ms	192.099 ms	2.660	United States
13	4.68.111.121	173.618 ms	-60.636 ms	-0.753	United States
14	4.69.138.123	275.144 ms	101.526 ms	1.437	United States
15	4.69.140.142	189.482 ms	-85.662 ms	-1.091	United States
16	4.69.202.65	271.422 ms	81.940 ms	1.172	United States
17	4.69.148.106	276.174 ms	4.752 ms	0.130	United States
18	4.69.143.214	274.406 ms	-1.769 ms	0.042	United States
19	4.69.201.69	275.762 ms	1.356 ms	0.084	United States
20	4.69.137.65	278.957 ms	3.195 ms	0.109	United States
21	4.69.143.89	278.244 ms	-0.713 ms	0.056	United States
22	4.69.133.101	301.552 ms	23.307 ms	0.380	United States
23	195.50.119.98	262.045 ms	-39.506 ms	-0.468	United Kingdom
24	146.97.33.41	260.679 ms	-1.366 ms	0.047	London, United Kingdom
25	146.97.33.21	263.462 ms	2.783 ms	0.103	London, United Kingdom
26	146.97.37.206	262.942 ms	-0.519 ms	0.059	London, United Kingdom
27	193.63.108.129	263.214 ms	0.272 ms	0.069	United Kingdom
28	193.63.108.134	261.751 ms	-1.464 ms	0.046	United Kingdom
29	193.63.109.110	271.367 ms	9.617 ms	0.195	Wantage, United Kingdom
30	192.76.21.2	271.423 ms	0.056 ms	0.066	Oxford, United Kingdom

Figura 5: Traza hacia University of Oxford

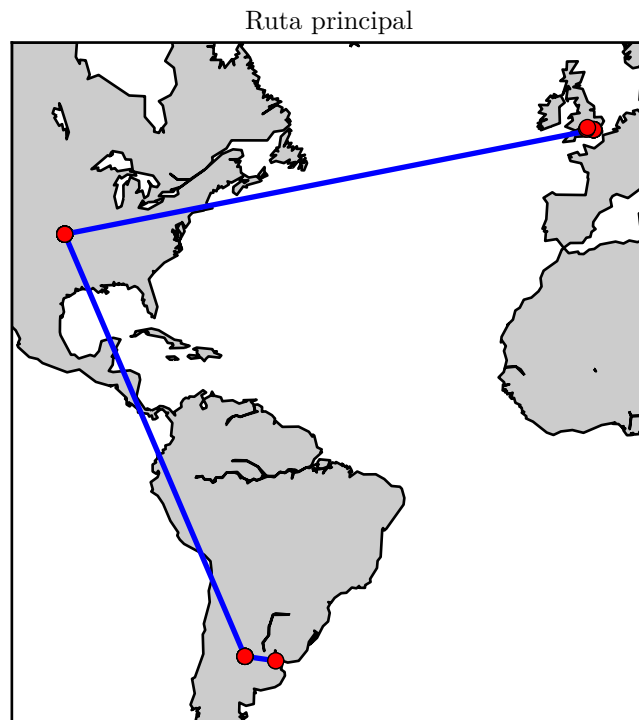


Figura 6: Ruta hacia University of Oxford

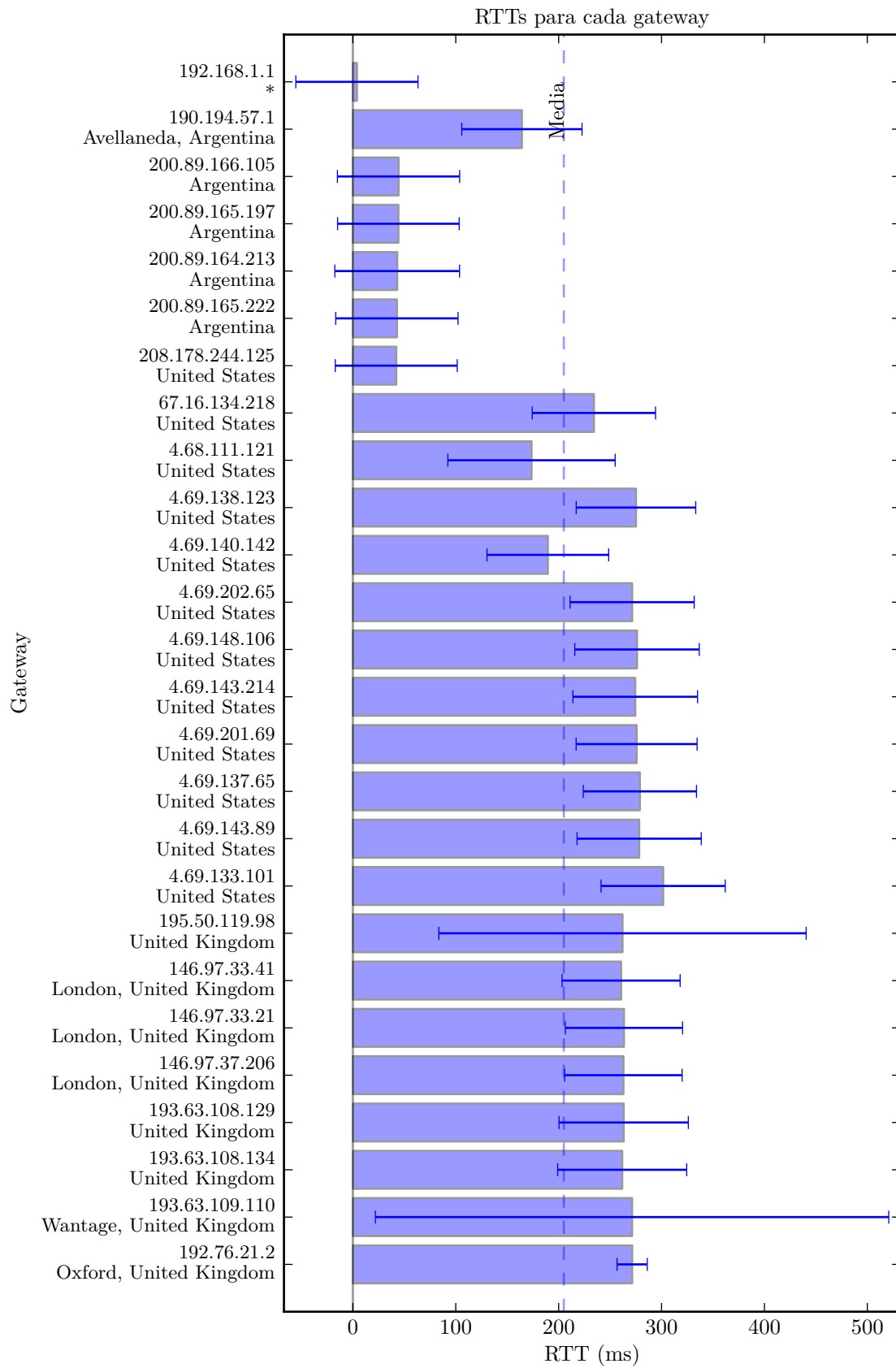


Figura 7: RTT de los gateways de la ruta hacia University of Oxford

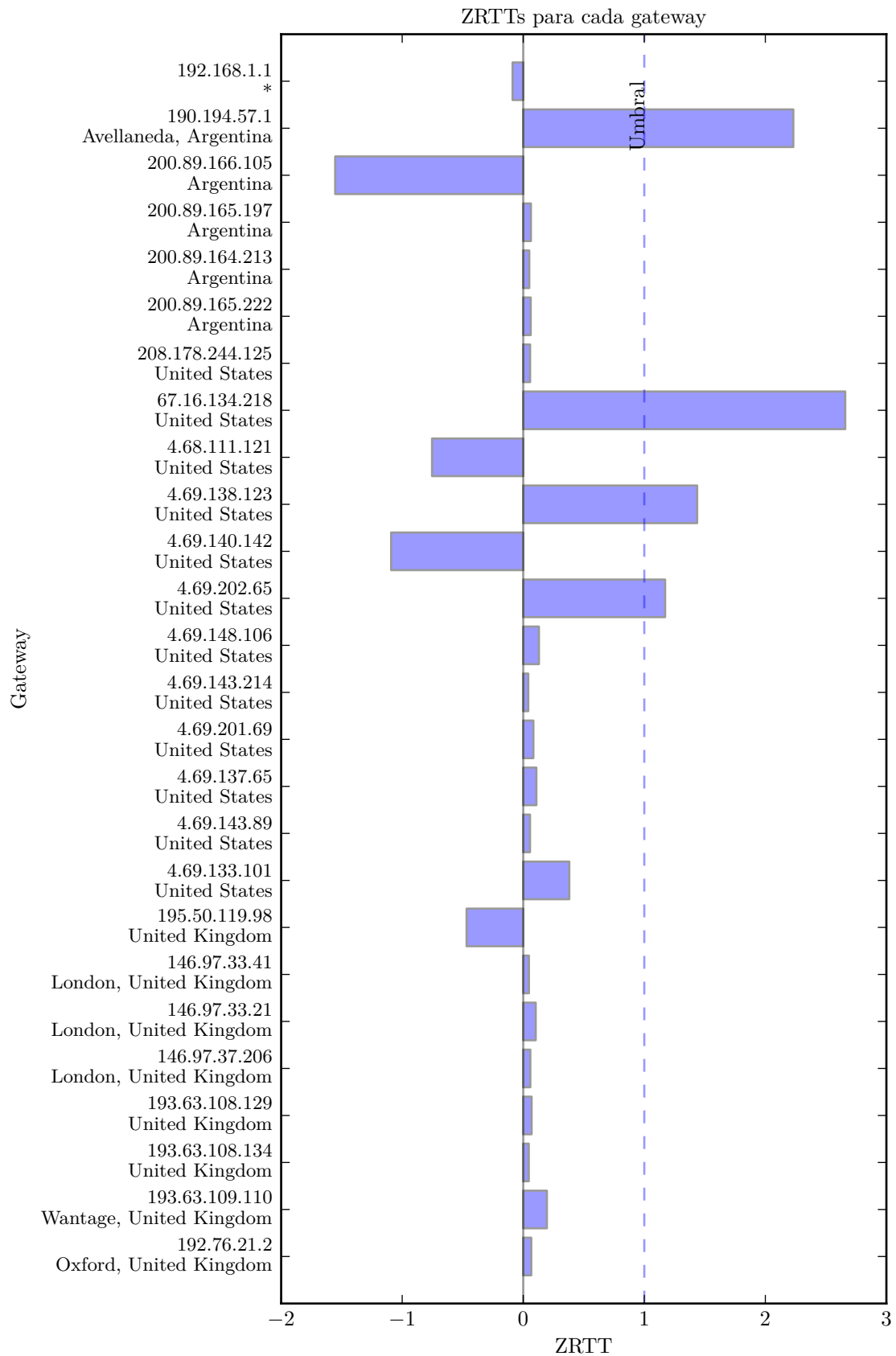


Figura 8: ZRTT de los gateways de la ruta hacia University of Oxford



### 3.2. The University of Sydney

TTL	IP Addresses	Absolute RTT	Relative RTT	Relative ZRTT	Location
1	192.168.1.1	2.495 ms	2.495 ms	-0.213	*
2	190.194.57.1	138.808 ms	136.313 ms	1.956	Avellaneda, Argentina
5	200.89.165.157	30.104 ms	-108.703 ms	-1.586	Argentina
6	200.89.165.130	29.463 ms	-0.641 ms	-0.024	Argentina
9	200.89.164.217	28.635 ms	-0.828 ms	-0.026	Argentina
10	200.89.165.222	28.665 ms	0.031 ms	-0.014	Argentina
11	159.63.53.213	36.210 ms	7.544 ms	0.095	United States
12	67.16.139.18	207.744 ms	171.534 ms	2.465	United States
13	129.250.9.117	192.087 ms	-15.657 ms	-0.241	Englewood, United States
14	129.250.3.172	195.526 ms	3.439 ms	0.035	Englewood, United States
15	129.250.3.174	194.925 ms	-0.601 ms	-0.023	Englewood, United States
16	129.250.2.168	231.937 ms	37.012 ms	0.521	Englewood, United States
17	129.250.2.230	228.437 ms	-3.500 ms	-0.065	Englewood, United States
18	204.1.253.166	228.255 ms	-0.181 ms	-0.017	Englewood, United States
19	202.158.194.172	352.907 ms	124.651 ms	1.788	Australia
20	113.197.15.68	352.569 ms	-0.337 ms	-0.019	Australia
21	113.197.15.66	375.784 ms	23.215 ms	0.321	Australia
22	113.197.15.65	358.409 ms	-17.375 ms	-0.265	Australia
23	202.158.194.197	386.693 ms	28.284 ms	0.395	Australia
24	202.158.205.165	387.616 ms	0.923 ms	-0.001	Australia
25	113.197.9.186	361.201 ms	-26.415 ms	-0.396	Lidcombe, Australia

Figura 9: Traza hacia The University of Sydney

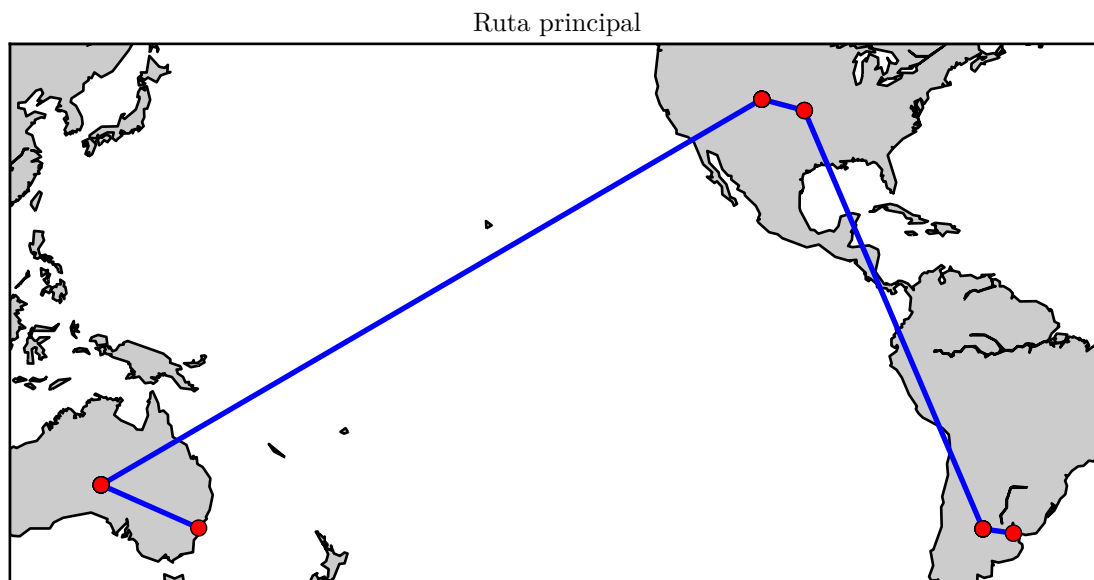


Figura 10: Ruta hacia The University of Sydney

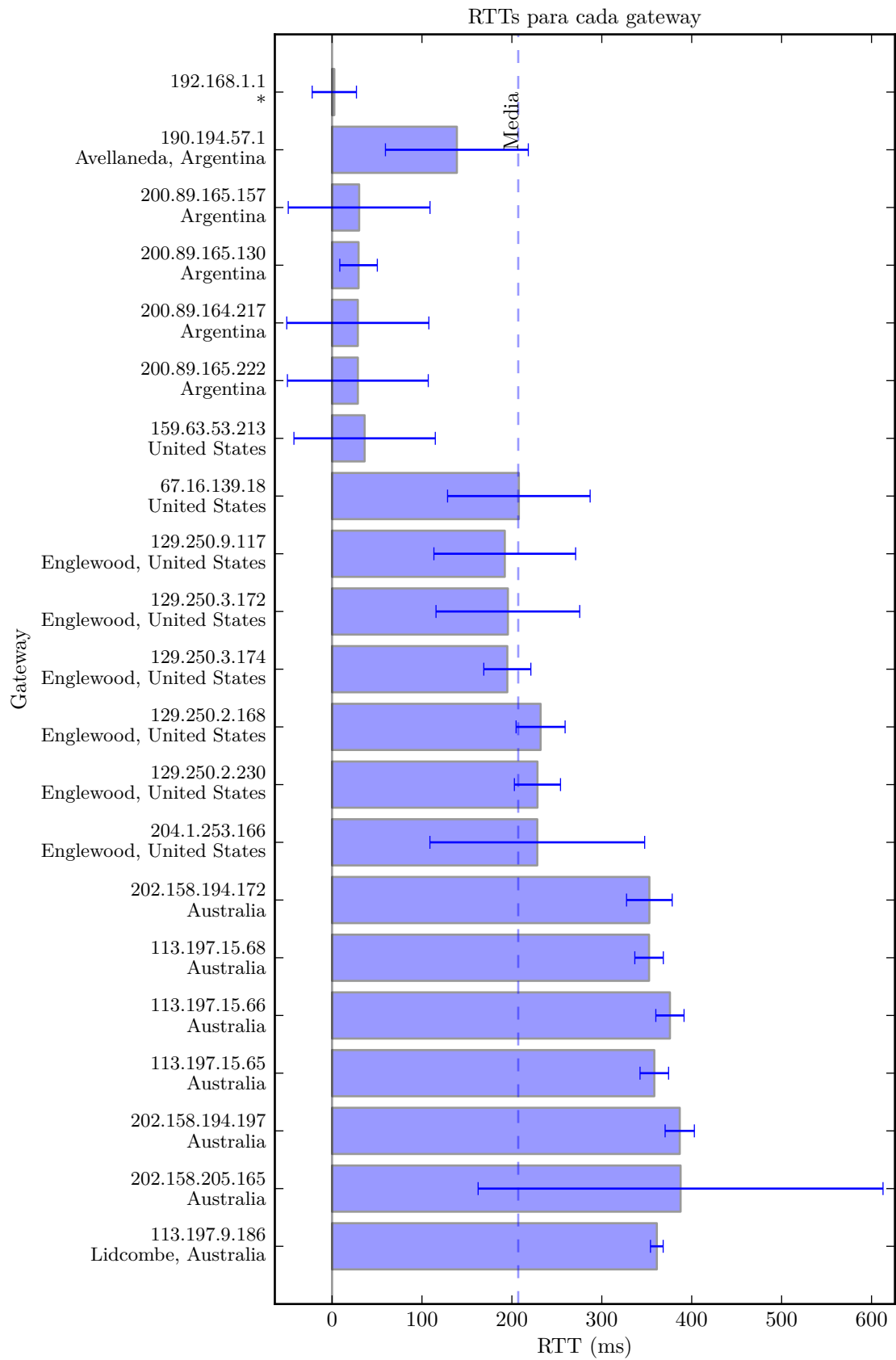


Figura 11: RTT de los gateways de la ruta hacia The University of Sydney

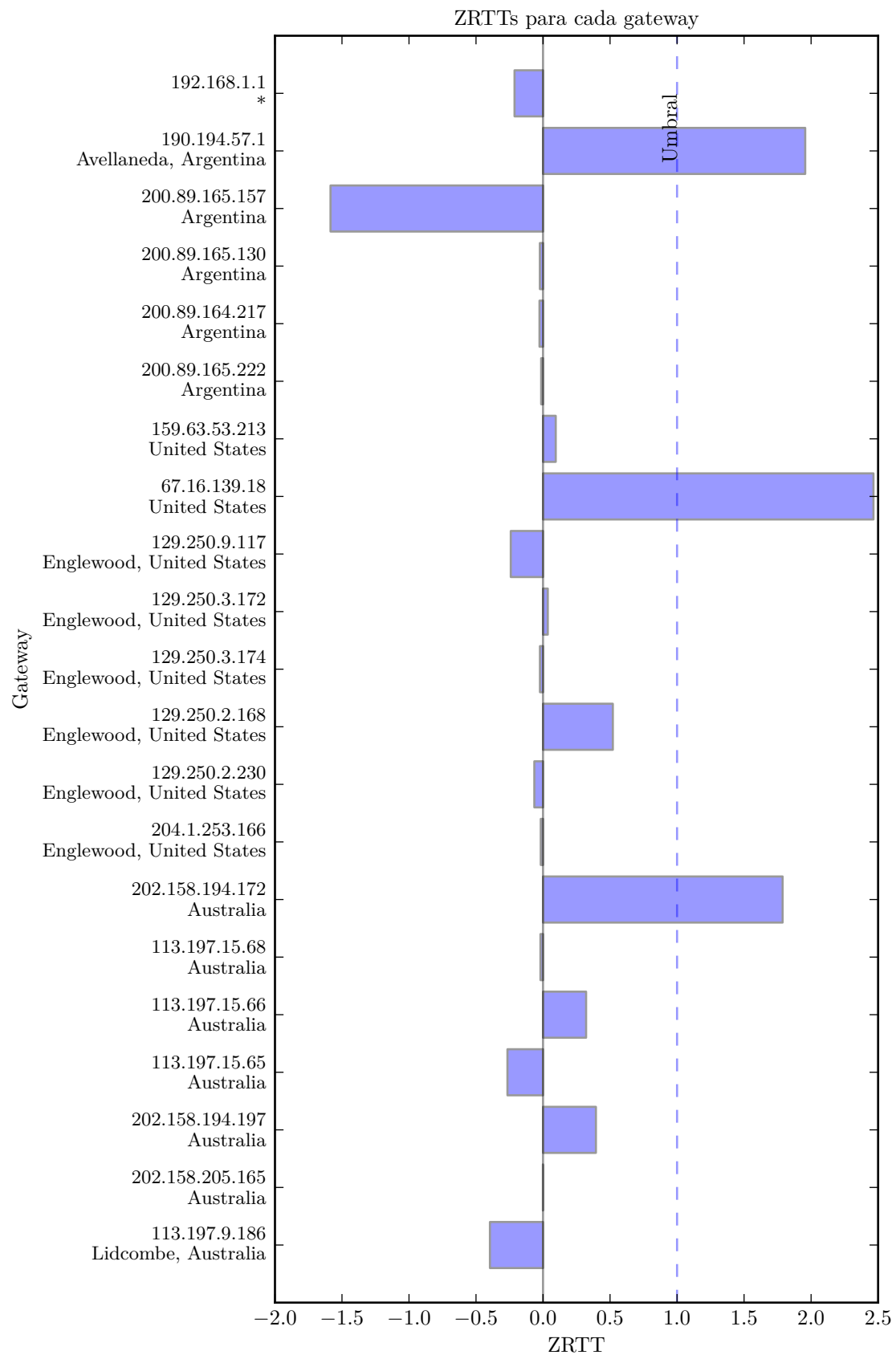


Figura 12: ZRTT de los gateways de la ruta hacia The University of Sydney

### 3.3. Malaysia University of Science and Technology

TTL	IP Addresses	Absolute RTT	Relative RTT	Relative ZRTT	Location
1	192.168.1.1	5.278 ms	5.278 ms	-0.134	*
2	181.28.111.1	121.930 ms	116.651 ms	2.043	Argentina
6	200.89.166.121	28.317 ms	-93.613 ms	-1.623	Argentina
7	200.89.165.86	28.037 ms	-0.280 ms	0.004	Argentina
8	64.214.130.253	45.763 ms	17.726 ms	0.318	United States
	208.178.245.21				United States
9	67.17.192.6	171.696 ms	125.933 ms	2.205	United States
10	203.208.172.189	174.447 ms	2.751 ms	0.057	Singapore
11	203.208.183.145	271.733 ms	97.286 ms	1.705	Singapore
	203.208.171.137				Singapore
	203.208.149.61				Singapore
	203.208.182.125				Singapore
	203.208.182.77				Singapore
	203.208.149.73				Singapore
	203.208.172.101				Singapore
	203.208.149.25				Singapore
	203.208.153.121				Singapore
	203.208.149.37				Singapore
	203.208.171.85				Singapore
	203.208.171.234				Singapore
	203.208.182.41				Singapore
12	203.208.151.117	348.933 ms	77.199 ms	1.355	Singapore
	203.208.152.222				Singapore
	203.208.151.113				Singapore
	203.208.153.166				Singapore
	203.208.151.98				Singapore
	203.208.171.9				Singapore
	203.208.151.229				Singapore
	203.208.149.225				Singapore
	203.208.152.226				Singapore
	203.208.151.85				Singapore
	203.208.154.45				Singapore
	203.208.151.221				Singapore
	203.208.182.45				Singapore
	203.208.171.189				Singapore
13	203.208.183.14	350.153 ms	1.220 ms	0.030	Singapore
	203.208.183.153				Singapore
	203.208.153.254				Singapore
	203.208.174.82				Singapore
14	203.208.153.166	352.471 ms	2.318 ms	0.050	Singapore
	203.208.151.98				Singapore
	124.158.224.45				Malaysia
	203.208.152.222				Singapore
	203.208.152.226				Singapore
	203.208.182.45				Singapore
15	61.11.210.1	354.032 ms	1.560 ms	0.036	Malaysia
	203.208.174.82				Singapore
16	61.11.211.175	349.901 ms	-4.131 ms	-0.063	Malaysia
	124.158.224.45				Malaysia
17	124.158.228.58	356.670 ms	6.769 ms	0.127	Malaysia
	61.11.210.1				Malaysia
18	110.4.44.250	350.958 ms	-5.711 ms	-0.090	Penang, Malaysia
	61.11.211.175				Malaysia
19	110.4.45.250	352.772 ms	1.814 ms	0.041	Penang, Malaysia
	124.158.228.58				Malaysia

Figura 13: Traza hacia Malaysia University of Science and Technology

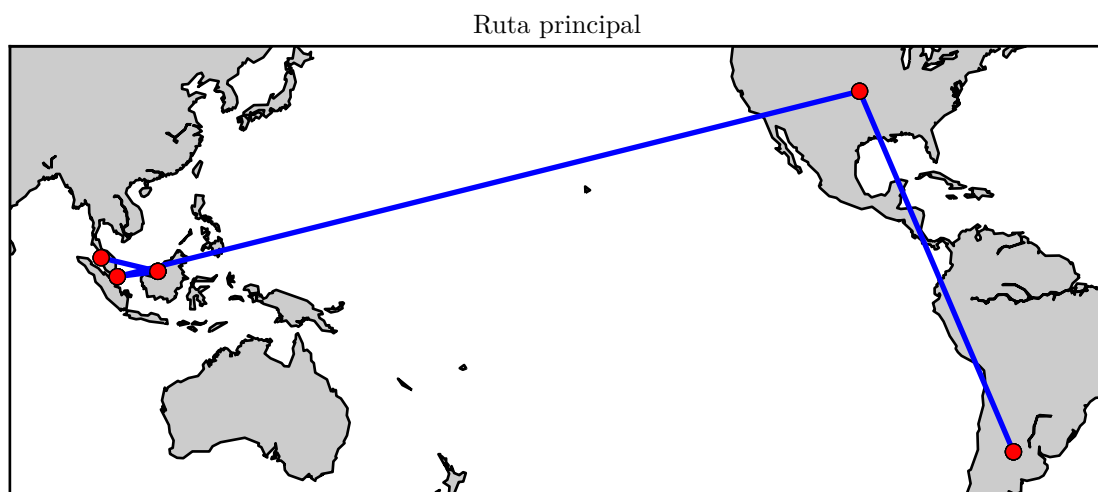


Figura 14: Ruta hacia Malaysia University of Science and Technology

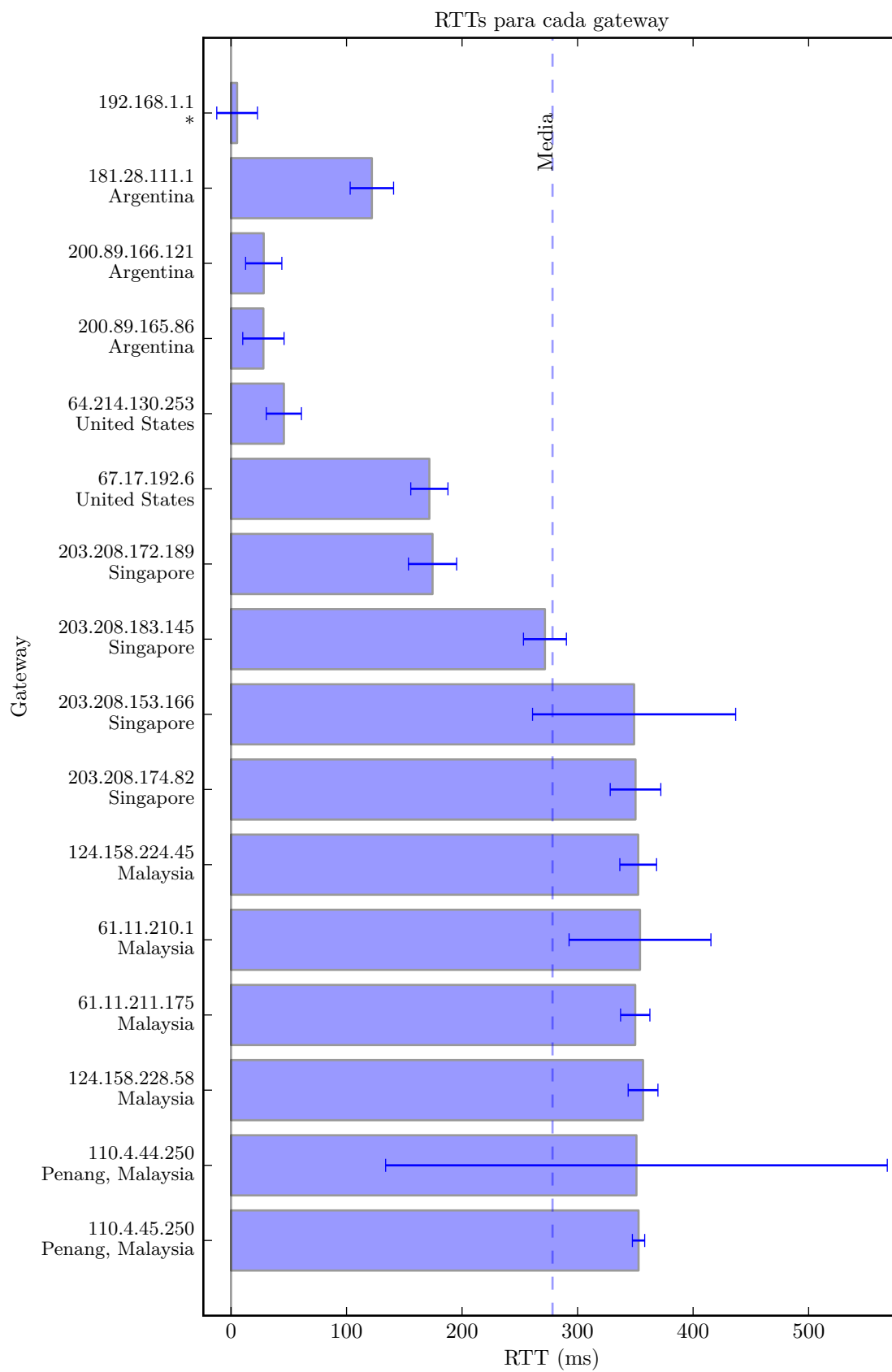


Figura 15: RTT de los gateways de la ruta hacia Malaysia University of Science and Technology

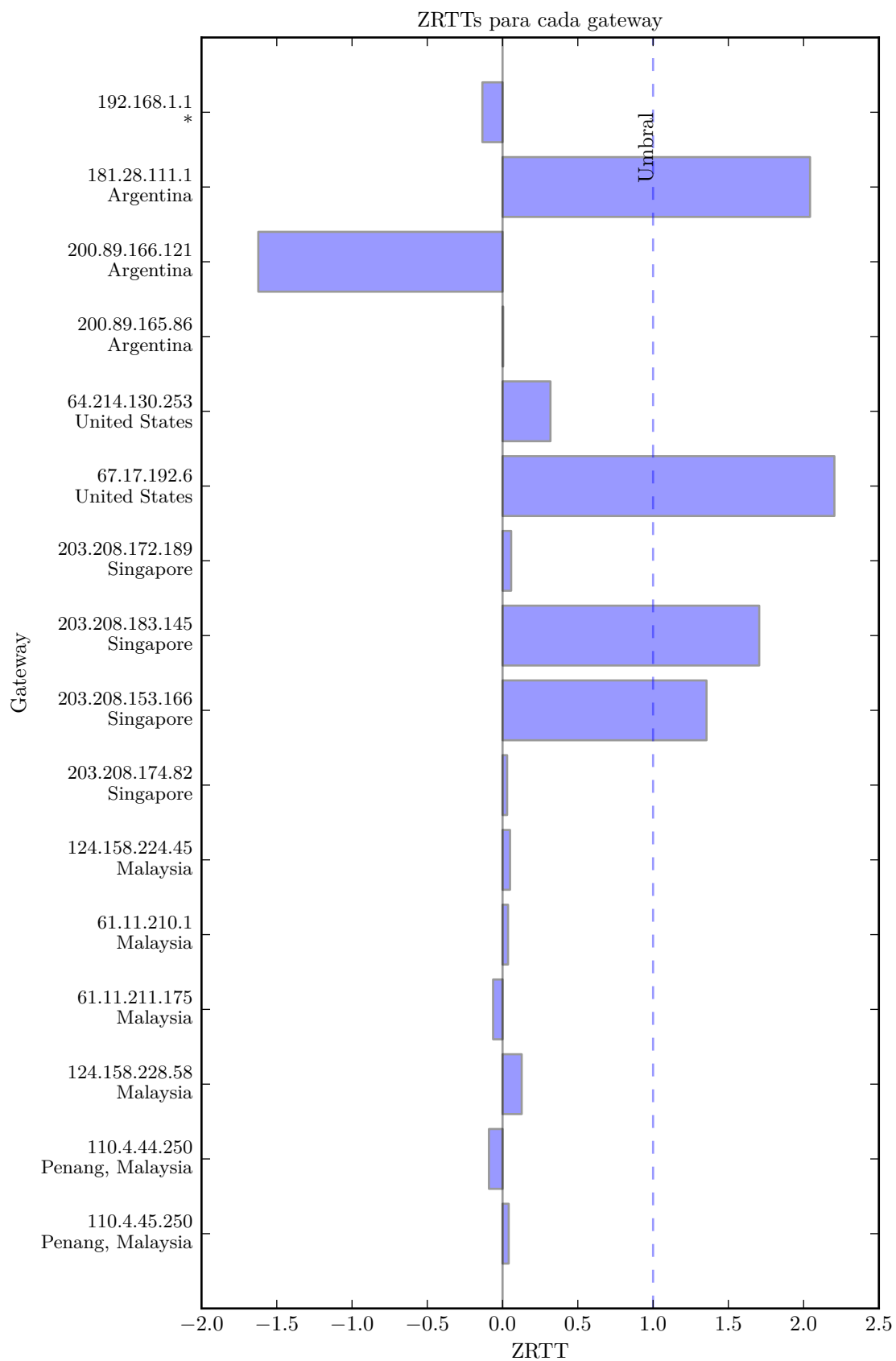


Figura 16: ZRTT de los gateways de la ruta hacia Malaysia University of Science and Technology

## 4. Discusión

Teniendo como referencia los resultados obtenidos, notamos que ocurrieron algunos fenómenos en común que creemos vale la pena mencionar.

### 4.1. Primer nodo externo

Podemos notar, en los resultados de todas las universidades analizadas, que el segundo nodo, el primer nodo que no es nuestro gateway, posee un RTT promedio alto en comparación a los nodos más próximos a éste. Podemos deducir que esto se debe a que este router tiene una prioridad baja para las respuestas a paquetes ICMP, haciendo que las respuestas tarden más de lo esperado.

### 4.2. Posible error de localización

Otro punto a tener en cuenta, también visible en los resultados de todas las universidades, es que la biblioteca elegida para la geolocalización sitúa muy probablemente la localización de los IP según la procedencia de la compañía que realice el enlace entre países. Pueden notarse en los resultados hops con bajo ZRTT relativo entre distintos países y luego el próximo nodo dentro del segundo país tiene un ZRTT relativo muy alto, indicando probablemente que se trata de un enlace de gran distancia.

### 4.3. Promedios de RTT

Un dato estadístico anómalo general es el de obtener, para un determinado nodo, un RTT absoluto menor al RTT absoluto del nodo anterior, lo que significaría que llegar a este nodo toma menos tiempo que llegar al anterior. Esta anomalía se debe a que los valores del RTT absolutos se calculan mediante el promedio de los RTT obtenidos para cada nodo, pudiendo el paquete ICMP haber tomado caminos diferentes y habiendo conseguido llegar de manera apenas más rápida en promedio.

### 4.4. Posibles enlaces submarinos

En la traza a la universidad de Oxford podemos observar en el gráfico del ZRTT relativo como la IP 67.16.134.218 asignado a Estados Unidos obtiene un ZRTT relativo alto estando rodeado por dos nodos cuyos ZRTT son bajos y su nodo anterior sufre del problema general de la geolocalización del cuál hablamos anteriormente (el nodo debería pertenecer a un router en Argentina), podemos decir que el IP mencionado pertenece al primer router luego de un enlace submarino.

Podemos observar también en el gráfico del ZRTT relativo de esta universidad como existen varios enlaces (4.69.138.123 y 4.69.202.65) de los cuales no es posible deducir con certeza la causa de sus altos valores, pero podemos especular de que, algún router posee una prioridad baja para contestar paquetes ICMP o que las IP sufren del problema de geolocalización indicado y estos saltos son entre Estados Unidos y algún país europeo y luego de el continente europeo a Reino Unido o posiblemente, una combinación de ambos (un salto a Reino unido y un router con prioridad de contestación baja). Esta deducción surge de que el análisis de los ZRTT relativos de los nodos siguientes muestra valores para los ZRTT muy bajos, incluso cuando la geolocalización muestra el cambio de países.

La ruta a The University of Sydney muestra un gráfico de ZRTT relativos satisfactorio en cuanto al análisis de saltos submarinos. Podemos notar la IP del router 67.16.139.18 que sufre del problema de geolocalización y que al obtener un ZRTT relativo alto en relación a sus nodos vecinos y al estar próximo de Argentina, es posible identificarlo como salto submarino. El próximo salto notable es el de Estado Unidos a Australia de IP 202.158.194.172, donde podemos ver que esta IP no sufre del problema de geolocalización y marca un ZRTT relativo alto entre nodos cercanos además del cambio de país. Los demás routers del recorrido, a excepción del caso general del segundo nodo en la conexión, muestran ZRTT relativos esperables y bajos al no ser saltos submarinos, dejando como distinguidos los IP mencionados.

Por último, la traza obtenida a Malaysia University of Science and Technology muestra en su gráfico de ZRTT relativos, además del caso general del segundo nodo con alto ZRTT, 3 IP, 67.17.192.6, 203.208.183.145 y 203.208.153.166 los cuales podemos tomar como saltos submarinos. La IP 67.17.192.6



cae en el caso de geolocalización errónea y correspondería al salto de Argentina a Estados Unidos y las IP 203.208.183.145 y 203.208.153.166 que también sufren de lo mismo y que estimamos que sus ZRTT relativos representan un salto de Estados Unidos a Singapore y de Singapore a Malasia respectivamente. Los demás IP tienen ZRTT relativos bajos, indicando comunicaciones entre nodos cercanos.

#### 4.5. Heurística para detección de enlaces submarino

Basándonos en el análisis realizado sobre la experimentación, proponemos como umbral en las mediciones de los ZRTT relativos para la detección de enlaces submarinos el valor 1. El umbral propuesto creemos que es suficiente para detectar grandes variaciones en relación al desvío estándar de RTT entre nodos.

Como lo planteamos anteriormente, los enlaces submarinos y los routers que asignan prioridad baja a las respuestas de paquetes ICMP muestran ambos un ZRTT alto, pero con la diferencia de que los routers que asignan una prioridad diferente hacen que el nodo siguiente tenga un ZRTT más bajo que el resto. Si bien se destacan del resto, usar únicamente un umbral positivo sobre los ZRTT presenta problemas a la hora de decidir si realmente pertenecen a un enlace submarino.

### 5. Conclusión

Podemos concluir en que la heurística basada en ZRTT's relativos funciona en casos donde es posible diferenciar un salto submarino de un router con prioridad baja de contestación de paquetes ICMP. En los casos donde el camino posee una variedad de routers que hacen diferencia en el tiempo de contestación, la identificación de los saltos puede volverse dificultosa y es probable que requiera de una base de geolocalización precisa para la resolución del problema.

Debido al problema de clasificación de nodos (nodo con prioridad baja para paquetes ICMP o enlace submarino) planteamos como mejora a futuro para la heurística, la utilización de un umbral negativo para las mediciones de los ZRTT relativos, el cual parece efectivo para descartar los casos en los que se obtengan routers con prioridad baja, en especial el del primer nodo externo.

### Referencias

- [1] *Scapy Project*. <http://www.secdev.org/projects/scapy>, Mayo de 2014.
- [2] *RFC 792: Internet Control Message Protocol*. <http://tools.ietf.org/html/rfc792>.
- [3] *Traceroute*. <http://en.wikipedia.org/wiki/Traceroute>, Mayo de 2014.
- [4] *Ping (network utility) (Artículo en Wikipedia)*. [http://en.wikipedia.org/wiki/Ping\\_\(networking\\_utility\)](http://en.wikipedia.org/wiki/Ping_(networking_utility)), Mayo de 2014.
- [5] *Internet Control Message Protocol (Artículo en Wikipedia)*. [http://en.wikipedia.org/wiki/Internet\\_Control\\_Message\\_Protocol](http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol), Mayo de 2014.