



DEPARTAMENTO
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico II

Rutas en Internet

Teoría de las Comunicaciones

Integrante	LU	Correo electrónico
Fernández, Gonzalo	836/10	gpfernandezflorio@gmail.com
Aleman, Damián Eliel	377/10	damianealeman@gmail.com
Pizzagalli, Matías	257/12	matipizza@gmail.com

Instancia	Docente	Nota
Primera entrega		
Segunda entrega		



Facultad de Ciencias Exactas y Naturales

Universidad de Buenos Aires

Ciudad Universitaria - (Pabellón I/Planta Baja)

Intendente Güiraldes 2610 - C1428EGA

Ciudad Autónoma de Buenos Aires - Rep. Argentina

Tel/Fax: (++54 +11) 4576-3300

<http://www.exactas.uba.ar>

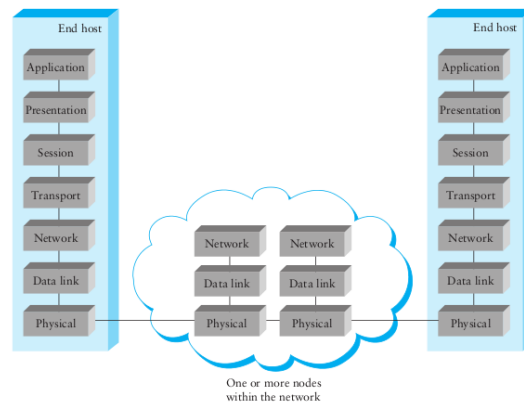
Índice

1. Introducción Teórica	2
1.1. Modelo OSI	2
1.2. Paquetes IP	2
1.3. Paquetes ICMP	2
1.4. Traceroute	2
1.5. RTT: Round Trip Time	3
2. Desarrollo	3
3. Resultados	5
3.1. Lomonosov Moscu State University	5
3.2. The University of Tokyo	6
3.3. The University of Sydney	7
4. Conclusiones	8
5. Apéndice	10

1. Introducción Teórica

1.1. Modelo OSI

El modelo OSI es un modelo que abstrae en 7 capas los protocolos involucrados en la comunicación entre dos nodos en una red.



1.2. Paquetes IP

Los paquetes IP¹ son el método principal de intercambio de mensajes entre nodos a nivel de red. Es decir, cuando los nodos pertenecen a distintas redes locales y no tienen acceso la dirección física del otro. El protocolo IP es *best-effort*, por lo tanto existe la posibilidad de que un mensaje nunca llegue a destino. Es más, los routers que implementan RED², están configurados para descartar paquetes periódicamente con alguna probabilidad, incluso antes de entrar en un estado de congestión.

1.3. Paquetes ICMP

Los paquetes ICMP³ son paquetes de control que no contienen datos, utilizados por los routers para reportar errores en el intercambio de mensajes de una conexión.

1.4. Traceroute

Traceroute es una herramienta que permite mostrar la ruta de una conexión entre dos nodos, identificando todos los nodos intermedios y sus respectivos tiempos de demora. Existen distintas implementaciones de Traceroute a diferentes niveles, que brindan ventajas o desventajas en función de ello. Todas se basan en enviar mensajes con el campo TTL (time to live) incrementándose de uno en uno de forma que, los paquetes sean rechazados por los sucesivos routers en la ruta, al haber finalizado su tiempo de vida. El emisor recoge esas respuestas de los routers y genera el camino virtual correspondiente a partir de las ips

¹RFC 791 (IP): <https://tools.ietf.org/html/rfc791>

²RFC 2309 (RED): <https://tools.ietf.org/html/rfc2309>

³RFC 792 (ICMP): <https://tools.ietf.org/html/rfc792>

de los emisores de estos mensajes. Notar que en el caso de los protocolos IP o UDP, donde no se establece una conexión (son orientados a datagramas, no a conexión) es posible que se produzca un cambio de ruta durante el procedimiento. En el momento en que el mensaje llega a destino, se obtiene una respuesta del host objetivo. Esto indica la finalización del Traceroute.

1.5. RTT: Round Trip Time

Se define el RTT como el tiempo que tarda un paquete de datos enviado desde un emisor en volver a este mismo emisor habiendo pasado por el receptor de destino. Si llamamos RTT_i al RTT medido para el salto i , se define $ZRTT_i$ como

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

Siendo \overline{RTT} y $SRTT$ el promedio y el desvío standard de los RTTs de la ruta, respectivamente. De esta manera, con el $ZRTT_i$ podemos ver a cuanto está de la media cada RTT_i de forma normalizada (debido a que lo dividimos por el desvío standard)

2. Desarrollo

En este trabajo implementaremos una versión de traceroute a través de mensajes ICMP mediante la herramienta Scapy de Python. Como estamos trabajando con paquetes IP, no tenemos asegurado que el paquete enviado llegue a destino, así como que la respuesta llegue de regreso. Debemos tener esto en cuenta al momento de hacer las mediciones.

Mediremos el tiempo de la recepción de una respuesta a un paquete enviado. Sobre estas mediciones utilizaremos la técnica de estimación de outliers propuesta por Cimbala para identificar posibles saltos transcontinentales y un método gráfico para corroborar esa discriminación.

La técnica de estimación de outliers sirve para identificar valores distantes en módulo a la media. Al utilizar esta técnica vamos a estar identificando valores muy por encima y muy por debajo de la media. Sin embargo, como el objetivo es identificar saltos intercontinentales, tendremos en cuenta sólo aquellos outliers por encima de la media, ya que estos presentan una gran distancia entre dos saltos consecutivos.

Al suponer que la carga de la red de una región depende del horario, proponemos como hipótesis que los tiempos totales medidos diferirán según el horario en que se envían debido a distintos niveles de carga en las redes utilizadas. También es posible que esta diferencia no se vea en conexiones lejanas ya que podrían balancearse las demoras entre las distintas regiones. Esto se debe a que tienen distintos usos horarios, luego la carga se distribuye en el tiempo de otra forma.

La implementación se encuentra en el archivo `traceroute.py` y se necesitan permisos de administrador para ejecutarlo. Toma como único parámetro opcional la dirección IP (o el nombre) del host destino. A continuación se presenta un pseudocódigo de la misma.

```
1 main(dest = 'www.dc.uba.ar'):
```

```

2
3  # Mediciones
4  rtts = []
5  for ttlive in [1..limit]:
6      deltas = []
7      for i in [1..tries]:
8          start = datetime.datetime.now()
9          pkt = sr(IP(dst=dest, ttl=ttlive) / ICMP(), timeout=to, verbose=False)
10         fin = datetime.datetime.now()
11         # RTT hasta el hop actual
12         deltas.append(fin-start)
13
14         # Si cambio de ruta, termino la ejecucion
15         if (cambio_de_ruta()):
16             print("Cambio_de_Ruta!")
17             sys.exit()
18         # Si ya llegue, dejo de iterar
19         if destino_alcanzado():
20             break
21     rtts.append(avg(deltas))
22
23     relatives = calcular_relativos(rtts)
24     calcular_outliers(relatives)

```

La instrucción principal es el llamado a la función `sr` de Scapy en la línea 9. Esta envía un paquete de control de tipo IP/ICMP con un determinado TTL y devuelve el paquete recibido por respuesta. El valor de TTL itera de uno hasta una constante `limit`. Al recibir cada respuesta, se obtiene un host intermedio (cuya distancia en saltos coincide con el valor de TTL utilizado) en la ruta que se construye. Esto se realiza una determinada cantidad `tries` de veces, para obtener un promedio más confiable entre todos estos intentos.

Como se mencionó anteriormente, el método basado en paquetes IP para implementar Traceroute es propenso a pérdida de paquetes y cambios de ruta. Si no se recibe una respuesta de ninguno de los `tries` paquetes, se considera un salto nulo (probablemente, un router programado para no enviar respuestas de tipo `Time-Exceeded`) y se pasa al siguiente nodo de la ruta (aumentando en uno el TTL). Si se detecta un cambio de ruta (dos emisores distintos en un mismo ciclo TTL) se finaliza la ejecución, ya que no va a ser posible determinar la ruta completa hasta el destino.

Si el emisor de la respuesta es el host al que intentábamos conectarnos, significa que ya tenemos la ruta completa, por lo tanto no hace falta seguir iterando el valor de TTL. Estimamos que no vamos a encontrar una ruta con más hosts intermedios que el valor máximo de TTL, es decir `limit`.

Finalmente se calculan los outliers usando el procedimiento de estimación de outliers mencionado anteriormente. Este toma un arreglo con los valores de RTT relativos de cada nodo no nulo de la ruta. Llamamos RTT relativo de un nodo al valor de RTT de dicho nodo, restándole el valor de RTT del nodo anterior. De esta forma, son los valores de RTT relativos muy altos los que queremos identificar como outliers, ya que estos se corresponderán con nodos detrás de un enlace intercontinental.

Adicionalmente, se imprimen por pantalla cada una de las direcciones IP obtenidas,

junto con el RTT estimado desde el origen, la diferencia respecto al RTT del nodo anterior y la ubicación geográfica del router obtenida a partir de <http://freegeoip.net/>. También se imprimen los outliers estimados, junto con su valor de RTT relativo. Esto es necesario ya que sólo nos interesan los outliers con valor de RTT relativo positivo.

3. Resultados

Para experimentar con las herramientas desarrolladas, realizamos traceroutes a IPs pertenecientes a sitios web de universidades en diferentes países alrededor del mundo. De todas las experimentaciones que hicimos nos quedamos con tres universidades:

- Lomonosov Moscu State University, situada en Moscu, Rusia, Europa. (www.msu.ru)
- The University of Tokyo, situada en Tokio, Japon, Asia. (www.u-tokyo.ac.jp)
- The University of Sydney, situada en Sydney, Australia, Oceania. (www.sydney.edu.au)

3.1. Lomonosov Moscu State University

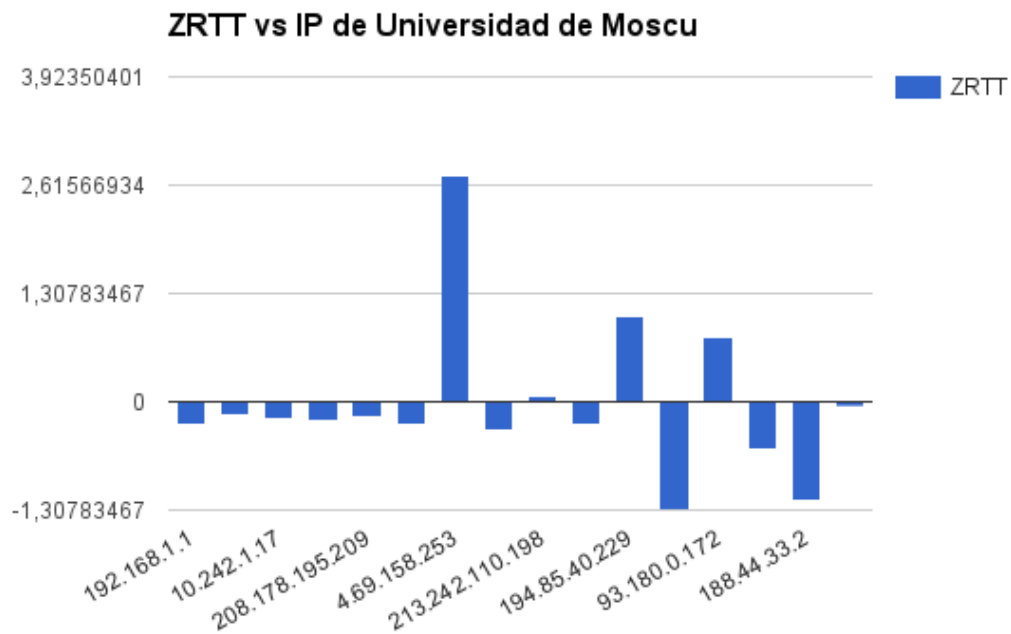
A continuación podemos observar los resultados que obtuvimos al probar nuestra herramienta de traceroute con destino la universidad situada en Moscu, es decir www.msu.ru.

HOP	RTT	RTT RELATIVO	Ubicación	ZRTT
192.168.1.1	66 ms	0	-	-0,2714373843
10.21.192.1	75 ms	9	-	-0,160394818
10.242.1.17	80 ms	5	-	-0,2097470697
208.178.195.210	84 ms	4	(Estados Unidos)	-0,2220851326
208.178.195.209	91 ms	7	(Estados Unidos)	-0,1850709439
*				
4.69.158.253	335 ms	244	Suecia	2,739049969
4.69.158.253	329 ms	-6	Suecia	-0,3454657619
213.242.110.198	356 ms	27	(Reino Unido)	0,06169031462
*				
194.85.40.229	462 ms	106	(Rusia)	1,036397286
194.190.254.118	378 ms	-84	(Rusia)	-1,30783467
93.180.0.172	464 ms	86	Moscu (Rusia)	0,7896360271
188.44.33.30	439 ms	-25	Moscu (Rusia)	-0,5798889574
188.44.33.2	365 ms	-74	Moscu (Rusia)	-1,184454041
188.44.50.103	383 ms	18	Moscu (Rusia)	-0,0493522517

Figura 1: Tabla generada por Traceroute a la Universidad de Moscu (188.44.50.103)

Además obtuvimos mediante la técnica de estimación de outliers el salto desde Estados Unidos (208.178.195.209) hacia Suecia (4.69.158.253). Efectivamente ese es un salto transcontinental. En el siguiente gráfico podemos observar las variaciones de ZRTT a lo largo de los saltos de la ruta:

Podemos observar en el gráfico que además del salto identificado mediante la técnica de Cimbala, sobresalen también el salto desde el Reino Unido hasta Rusia. Aquí se observa la ventaja de este método gráfico y la efectividad del método de Cimbala.

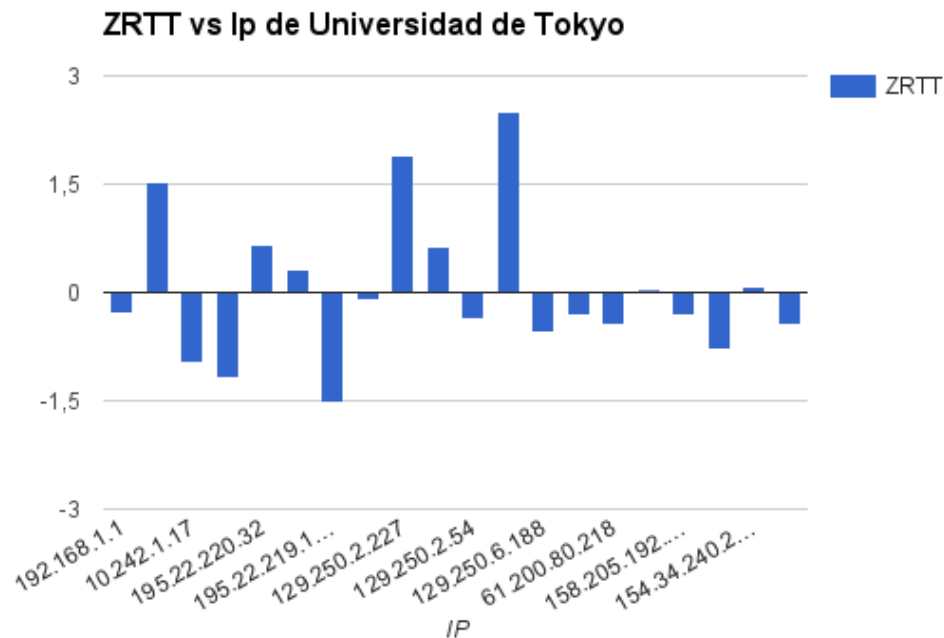


3.2. The University of Tokyo

A continuación mostramos los resultados obtenidos cuando tomamos como destino la Universidad de Tokio, es decir www.u-tokyo.ac.jp.

HOP	RTT	RTT RELATIVO	Ubicación	ZRTT
192.168.1.1	62 ms	0	-	-0,3018867925
10.21.192.1	159 ms	97	-	1,528301887
10.242.1.17	123 ms	-36	-	-0,9811320755
195.22.220.33	76 ms	-47	(Italia)	-1,188679245
195.22.220.32	127 ms	51	(Italia)	0,6603773585
195.22.219.145	160 ms	33	(Italia)	0,320754717
195.22.219.145	95 ms	-65	(Italia)	-1,528301887
149.3.181.65	106 ms	11	(Italia)	-0,09433962264
129.250.2.227	222 ms	116	Englewood (Estados Unidos)	1,886792453
129.250.4.13	272 ms	50	Englewood (Estados Unidos)	0,641509434
129.250.2.54	269 ms	-3	Englewood (Estados Unidos)	-0,358490566
129.250.3.86	418 ms	149	Englewood (Estados Unidos)	2,509433962
129.250.6.188	405 ms	-13	Englewood (Estados Unidos)	-0,5471698113
129.250.2.255	404 ms	-1	Englewood (Estados Unidos)	-0,320754717
61.200.80.218	396 ms	-8	(Japón)	-0,4528301887
158.205.192.173	414 ms	18	(Japón)	0,03773584906
158.205.192.86	413 ms	-1	(Japón)	-0,320754717
158.205.121.250	387 ms	-26	(Japón)	-0,7924528302
154.34.240.254	407 ms	20	(Japón)	0,07547169811
210.152.135.178	399 ms	-8	(Japón)	-0,4528301887

Figura 2: Tabla generada por Traceroute a la Universidad de Tokyo (210.152.135.178)



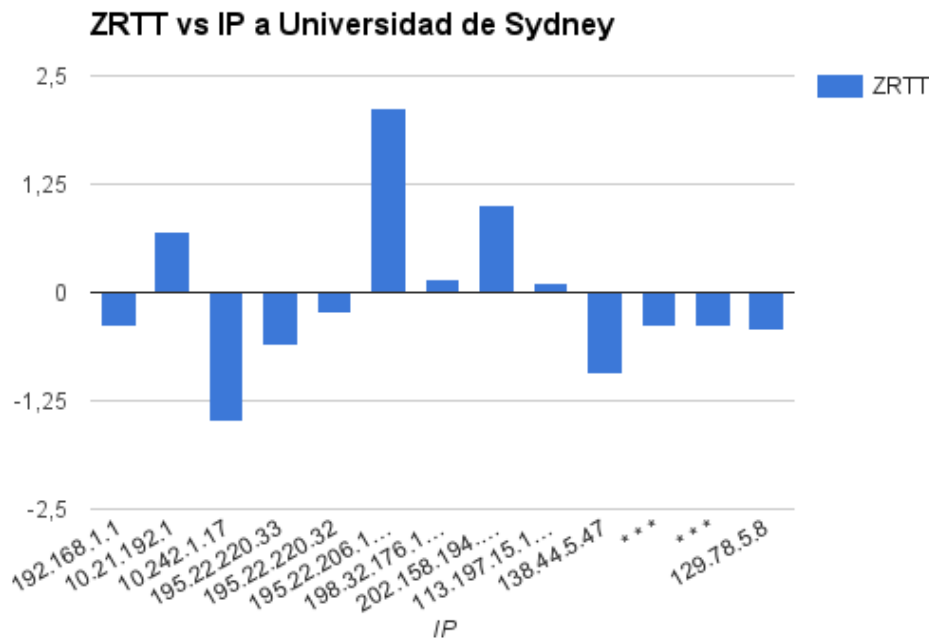
3.3. The University of Sydney

A continuacion podemos observar los resultados que obtuvimos al probar nuestra herramienta de traceroute con destino www.sydney.edu.au.

HOP	RTT	RTT RELATIVO	Ubicación	ZRTT
192.168.1.1	83 ms	0	Argentina	-0,3940627873
10.21.192.1	167 ms	84	Argentina	0,7093130172
10.242.1.17	83 ms	-84	Argentina	-1,497438592
195.22.220.33	67 ms	-16	Italia	-0,6042296073
195.22.220.32	78 ms	11	Italia	-0,2495730986
195.22.206.190	270 ms	192	Italia -	2,127939052
198.32.176.177	312 ms	42	Redwood City (Estados Unidos) -	0,1576251149
202.158.194.176	419 ms	107	Canberra (Australia) -	1,011427821
113.197.15.146	458 ms	39	Canberra (Australia) -	0,1182188362
138.44.5.47	416 ms	-42	Canberra (Australia) -	-0,9457506896
* * *			-	-0,3940627873
* * *			-	-0,3940627873
129.78.5.8	413 ms	-3	Sydney (Australia)	-0,4334690661

Figura 3: Tabla generada por Traceroute a la Universidad de Sydney (129.78.5.8)

Si bien tenemos la geolocalización del outlier en Italia, viendo el dominio de la dirección IP (obtenida a partir del traceroute implementado por Linux) **xe-1-2-0.paloalto2.pao.seabone.net** podemos suponer que en realidad ese nodo se encuentra en Palo Alto (California, Estados Unidos). Por lo cual no estaría mal que lo detecte como outlier, sin embargo no lo podemos saber con certeza.



4. Conclusiones

Si bien la tool diseñada y el método propuesto nos permiten obtener la ruta a un website detectando los posibles enlaces intercontinentales, este procedimiento está sujeto

a numerosas adversidades. Routers que no responden (aún con timeouts largos) o que asignan prioridad baja a los paquetes ICMP, geolocalizadores inexactos, congestión en una ruta o rutas distintas para un mismo website son mayormente lo que notamos que afecta considerablemente a los resultados obtenidos. Veamos algunas de estas problemáticas en detalle:

En los casos en los que no obtenemos una respuesta del router, no tenemos forma de conocer, con este método, esa parte de la ruta, aún sabiendo que allí debería haber un nodo. Esto afecta a la comparativa general ya que, en caso de tener numerosas no-respuestas sucesivas, el RTT relativo entre los extremos de esta secuencia podría distribuirse de diversos modos. Un caso posible consiste en una distribución equitativa de los RTTs entre los nodos de la secuencia significando que ninguno corresponde a un enlace submarino. A su vez podría suceder que la distribución sea desigual y exista un enlace intermedio de elevado RTT representando una conexión intercontinental.

Por otra parte, en los casos en donde obtenemos una respuesta, esta información no necesariamente basta. La estimación de la distancia entre hops mediante el RTT no resulta demasiado confiable debido a que el tiempo de ida y vuelta (de la forma calculada) no depende única y exclusivamente de la longitud del enlace sino también incluye el tiempo del paquete dentro del router que podría extenderse por congestión, prioridad u otros factores. Además la congestión a lo largo de la red puede no ser uniforme a lo largo de la ruta en un momento dado y cada router puede tener una asignación de prioridades diferente. De esta manera la comparación entre RTTs se ve afectada no sólo por el momento de la medición sino también por los nodos involucrados en la ruta elegida. Una forma posible de resolver la congestión en un horario podría ser tomar mediciones en distintos momentos del día, pudiendo así tener una idea de cómo afecta la congestión a nuestras mediciones.

A pesar de esto, encontramos casos en los que el método pudo ser llevado a cabo de forma efectiva.

5. Apéndice